

# Command Line Interface Reference, Modes R - Z, StarOS Release 21.28

**First Published:** 2022-09-29

**Last Modified:** 2026-07-24

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

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

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

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

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

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

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022-2025 Cisco Systems, Inc. All rights reserved.



# CONTENTS


PREFACE

**About this Guide** xxxv

CLI Command Sections xxxvi

Conventions Used xxxvi

Supported Documents and Resources xxxviii

Related Documentation xxxviii

Contacting Customer Support xxxviii

CHAPTER 1

**Common Commands** 1

do show 1

end 1

exit 2

CHAPTER 2

**RAC Profile Configuration Mode Commands** 3

do show 3

end 4

exit 4

rac 4

CHAPTER 3

**Radio Congestion Policy Configuration Mode Commands** 7

congestion-level 7

correlation-method 9

data-loss threshold 10

do show 11

end 11

exit 12

reporting-interval 12

rtt-samples 13
rtt-variance 14
sampling-interval 14

CHAPTER 4 RANAP Cause Code Group Configuration Mode 17
cause 17
do show 18
end 19
exit 19

CHAPTER 5 Remote Address List Configuration Mode Commands 21
address 21
do show 22
end 23
exit 23

CHAPTER 6 Remote Server List Configuration Mode Commands 25
address 25
do show 26
end 26
exit 27

CHAPTER 7 Remote Secret List Configuration Mode Commands 29
do show 29
end 30
exit 30
remote-id 30

CHAPTER 8 RLF Template Configuration Mode Commands 33
delay-tolerance 33
do show 34
end 35
exit 35

msg-rate 35
threshold 36

CHAPTER 9 RNC Configuration Mode Commands 39
associate-gtpu-bind-address 40
description 41
direct-tunnel 41
do show 42
dual-address-pdp 43
enb-data-forward 44
enb-direct-data-forward 45
end 45
exit 46
lac 46
mbms 47
overload-action disable 47
paging-non-searching-indication 49
pointcode 50
pooled 51
rab-asymmetry-indicator 51
rab-modify-procedure 52
ranap arp-ie 54
ranap bidirectional-always 54
ranap eutran-service-handover-ie 55
ranap global-cn-id 57
ranap paging-area-id 58
ranap paging-cause-ie 59
ranap rab-arsp-ue-radio-lost 61
ranap rab-release-with-radiolost 62
ranap rfsp-id-ie 63
ranap signalling-indication-ie 63
ranap ue-ambr-ie 64
ran-information-management 65
release-compliance 66

reset-resource 68

CHAPTER 10 RoHC Profile Common Options Configuration Mode Commands 71

delay-release-hc-context-timer 71

do show 72

end 73

exit 73

inactive-traffic-release-hc-context-timer 73

CHAPTER 11 RoHC Profile Compression Configuration Mode Commands 75

context-timeout 76

do show 77

end 77

exit 77

ipid-history-size 78

max-jitter-cd 78

max-sliding-window 79

multiple-ts-stride 80

new-context-blocking-time 80

num-pkts-ts 81

num-pkts-u-mode 82

num-updates-ir 83

optimistic-repeats 83

rtp-sn-p 84

rtp-sn-p-override 85

rtp-time-stride 86

rtp-ts-deviation 87

rtp-ts-stride 87

sliding-window-ts 88

total-jitter-ipv4 89

total-jitter-ipv6 90

unimode-timeout-to-fo-state 90

unimode-timeout-to-ir-state 91

use-calculated-rtp-time-stride 92

use-calculated-rtp-ts-stride 92
use-ipid-override 93
use-optimized-talkspurt 94
use-optimized-transience 95
use-timer-based-compression 95
use-uncomp-profile 96

CHAPTER 12 RoHC Profile Configuration Mode Commands 99
common-options 99
compression-options 100
decompression-options 101
do show 102
end 102
exit 102

CHAPTER 13 RoHC Profile Decompression Configuration Mode Commands 103
accept-delayed-pkts 104
context-timeout 104
crc-errors-fo 105
crc-errors-so 106
do show 107
end 108
exit 108
max-jitter-cd 108
nack-limit 109
optimistic-mode-ack 110
optimistic-mode-ack-limit 111
piggyback-wait-time 111
preferred-feedback-mode 112
rtp-sn-p 113
rtp-sn-p-override 114
rtp-time-stride 115
rtp-ts-stride 116
sliding-window-ts 116

total-jitter-ipv4 117
total-jitter-ipv6 118
use-clock-option 119
use-crc-option 119
use-feedback 120
use-jitter-option 121
use-reject-option 122
use-sn-not-valid-option 122
use-sn-option 123

CHAPTER 14 Route-map Configuration Mode Commands 125
do show 126
end 126
exit 126
match as-path 127
match community 127
match extcommunity 128
match interface 129
match ip address 130
match ip next-hop 131
match ipv6 address 131
match ipv6 next-hop 132
match metric 133
match origin 134
match route-type external 135
match tag 135
set as-path 136
set community 137
set extcommunity rt 138
set ip next-hop 139
set ipv6 next-hop 139
set local-preference 140
set metric 141
set metric-type 142

set origin 142
set tag 143
set weight 144

CHAPTER 15 RS-232 Port Configuration Mode Commands 145
do show 145
end 146
exit 146
preferred slot 146
snmp trap link-status 147
terminal 148

CHAPTER 16 S102 Pool Area Configuration Mode Commands 151
cell-id 151
do show 152
end 153
exit 153
hash-value 153
msc-id 154
plmnid 155

CHAPTER 17 S102 Service Configuration Mode Commands 157
1xrtt 157
bind 158
do show 159
end 160
exit 160
ip 160
msc 161
non-pool-area 162
pool-area 163

CHAPTER 18 S102 MSC Configuration Mode Commands 165
do show 165

end 166
exit 166
ipv4-address 166

CHAPTER 19 S1AP Cause Code Configuration Mode Commands 169
class 169
do show 170
end 171
exit 171

CHAPTER 20 S1-U Relay Configuration Mode Commands 173
associate 173
do show 174
end 175
exit 175
ip 175

CHAPTER 21 SAEGW Service Configuration Mode Commands 179
associate 179
do show 181
gtpc handle-collision upc nrupc 181
end 182
exit 182
sxa-tunnel-del-at-dsr-on-sgw-change 182

CHAPTER 22 SaMOG Service Configuration Mode Commands 185
associate 185
do show 187
end 188
exit 188
max-sessions 188
reporting-action 189
timeout 190

CHAPTER 23 SBc Service Configuration Mode Commands 193

associate 193

bind 194

cbc-associations 195

do show 196

end 196

exit 197

ip 197

sbc-mme 198

send 199

CHAPTER 24 SCCP Network Configuration Mode Commands 201

associate 201

description 202

destination 203

do show 205

end 205

exit 206

global-title-translation 206

hop-count 207

self-point-code 208

timeout 209

CHAPTER 25 SCTP Parameter Template Configuration Mode Commands 213

do show 214

end 214

exit 214

sctp-alpha 215

sctp-alt-accept-flag 215

sctp-beta 216

sctp-checksum-type 217

sctp-cookie-life 218

sctp-max-assoc-retx 218

sctp-max-in-strms 219
sctp-max-init-retx 220
sctp-max-mtu-size 220
sctp-max-out-strms 221
sctp-max-path-retx 222
sctp-min-mtu-size 223
sctp-rto-initial 224
sctp-rto-max 224
sctp-rto-min 225
sctp-sack-frequency 226
sctp-sack-period 226
sctp-start-mtu-size 227
timeout 228

CHAPTER 26 Security Configuration Mode Commands 231
category 231
end 232
exit 232
server 232

CHAPTER 27 Service Chain Configuration Mode Commands 235
end 235
exit 235
nsh-format 236

CHAPTER 28 Service Redundancy Protocol Configuration Mode Commands 237
advertise-routes-in-standby-state 238
audit 239
bfd-mon-ignore-dead-interval 241
bind 241
chassis-mode 242
checkpoint session 243
configuration-interval 245
dead-interval 245

delay-interval 246
delta-route-modifier 247
do show 248
dscp-marking 248
end 249
exit 250
guard-timer 250
handle-interim-resource-msg 251
hello-interval 252
internal-switchover-retry-interval 253
monitor authentication-probe 254
monitor bfd 255
monitor bgp 256
monitor diameter 257
monitor hsrp 259
monitor sx 260
monitor system 261
num-internal-switchover-retry 262
peer-ip-address 263
priority 264
retain-complete-sess-info 265
route-modifier 265
standby database-recovery 266
switchover allow-all-data-traffic 267
switchover allow-early-active-transition 268
switchover allow-volte-data-traffic 269
switchover control-outage-optimization 269

CHAPTER 29 Session Event Module Configuration Mode Commands 271
do show 271
end 272
event 272
exit 275
file 276

CHAPTER 30 Session Priority Profile Configuration Mode Commands 281
priority 281

CHAPTER 31 Session Trace Template Configuration Mode Commands 283
archive 283
disk-limit 284
do show 285
end 286
exit 286
interface 286
target-interface 289
target-ne 291
trace-extension 293

CHAPTER 32 SGSN ASP Configuration Mode Commands 295
do show 295
end 296
end-point 296
exit 298

CHAPTER 33 SGSN Congestion Action Profile Configuration Mode 299
active-call-policy 300
do show 301
end 301
exit 302
new-call-policy 302
sm-messages 303

CHAPTER 34 SGSN Congestion Control Configuration Mode 307
congestion-action-profile 307
do show 308
end 309

exit 309

CHAPTER 35 SGSN Global Configuration Mode Commands 311

aggregate-ipc-msg 312

apn-resolve-dns-query snaptr 314

bssgp-message dl-unitdata 315

bssgp-message ms-flow-control-from-unknown-ms 316

bssgp-message ptp-bvc-reset 317

bssgp-timer 318

bvc-unblock 319

canonical-node-name 320

common-ra-paging 320

congestion-control 321

do show 322

dscp-template 322

dual-address-pdp 324

ec-gsm 325

eir-profile 325

end 326

exit 326

gmm-message 327

gmm-sm-statistics 327

gprs-mocn 328

interface-management 328

ipms-suppress 329

imsi-range 330

location-services 332

map-message 333

max-pending-attaches 334

msisdn-group 335

msisdn-range 336

old-tlli invalidate tlli 337

old-tlli hold-time 338

pdp-deactivation-rate 339

qos-arp-rp-map-profile 340
ranap excess-len ignore 341
ran-information-management 342
target-offloading 342
tlli-cb-audit 343
umts-aka-r99 344

CHAPTER 36 SGSN Interface Management Configuration Mode 347
do show 347
end 348
exit 348
interface 348
lock-interface 350
paging-rlf-template 351

CHAPTER 37 SGSN Pool Area Configuration Mode Commands 353
do show 353
end 354
exit 354
hash-value 354
lac 356

CHAPTER 38 SGSN PSP Configuration Mode Commands 357
associate 358
do show 360
end 360
end-point 360
exchange-mode 361
exit 362
psp-mode 363
routing-context 364
sctp-alpha 365
sctp-beta 366
sctp-checksum-type 367

sctp-cookie-life 368
sctp-init-rwnd 369
sctp-max-assoc-retx 370
sctp-max-data-chunks 371
sctp-max-in-strms 372
sctp-max-init-retx 372
sctp-max-mtu size 373
sctp-max-out-strms 374
sctp-max-path-retx 375
sctp-parameter 376
sctp-rto-initial 377
sctp-rto-max 378
sctp-rto-min 379
sctp-sack-frequency 380
sctp-sack-period 381
sctp-suppress-alarm 382
shutdown 383
timeout 384

CHAPTER 39 SGSN Service Configuration Mode Commands 387
accounting 388
admin-disconnect-behavior 389
associate 391
cc profile 394
check-imei 396
check-imei-timeout-action 397
core-network 397
disable/enable super-charger 397
dns israu-mcc-mnc-encoding 398
dns mcc-mnc-encoding 399
do show 400
end 400
exit 401
gmm 401

gs-service 406
lac 407
max-pdp-contexts 408
mobile-application-part 409
network-sharing cs-ps-coordination 410
nri length 411
override-lac-li 413
LI-specific 413
override-rac-li 414
Li-specific 414
qos-modification 415
rac 416
LI-specific 416
ran-protocol 417
reporting-action event-record 417
s4-overcharge-protection 418
sgsn-number 419
sgtp-service 420
sm 421

CHAPTER 40 SGTP Service Configuration Mode Commands 425
direct-tunnel-disabled-ggsn 425
disable-remote-restart-counter-verification 427
do show 428
end 428
exit 429
ggsn-fail-retry-timer 429
gn-delay-monitoring 430
gtpc 431
gtpu 436
ignore-remote-restart-counter-change 438
max-remote-restart-counter-change 438
mbms 439
path-failure 440

pool 440

CHAPTER 41 S-GW Access Peer Profile Configuration Mode Commands 443

description 443

do show 444

end 445

exit 445

ntsr 445

CHAPTER 42 S-GW Paging Profile Configuration Mode Commands 447

do show 447

end 448

exit 448

ipv4 | ipv6 448

CHAPTER 43 S-GW Service Configuration Mode Commands 451

accounting context 452

accounting mode 453

accounting stop-trigger 454

associate 454

cc 457

cc profile 458

ddn failure-action 459

ddn isr-sequential-paging 460

ddn success-action no-user-connect ddn-retry-timer 461

ddn temp-ho-rejection mbr-guard-timer 462

ddn throttle 463

do show 466

egtp idft-support 466

egtp 467

egtp-service 468

end 469

exit 469

gtpc handle-collision upc nrupc 469

gtpu-error-ind 470
mag-service 471
ntsr session-hold timeout 472
page-ue 473
paging-policy-differentiation 474
path-failure 475
pgw-fteid-in-relocation-cs-rsp 477
plmn 477
reporting-action 478
timeout idle 479

CHAPTER 44 SLs Service Configuration Mode Commands 483
bind 483
do show 485
end 485
esmlc 485
exit 487
ip 487
max-retransmissions 488
t-3x01 488
t-3x02 489

CHAPTER 45 SMS Service Configuration Mode Commands 491
cp-data 491
do show 492
end 493
exit 493
mo-message-forwarding-destination 493
smsc-address-restiction-list 494
smsc-address-restiction-type 495
smsc-address-selection-prioritization 496
smsc-routing 497
timeout 498

CHAPTER 46 SS7 Routing Domain Configuration Mode Commands 501

asp 501

description 502

do show 503

end 504

exit 504

inbound-asp-identifier validate 504

linkset 505

MTU-size 506

peer-server 506

route 507

routing-context 508

ssf 509

CHAPTER 47 SSHD Configuration Mode Commands 511

allowusers add 512

authorized-key 513

challenge-response-authentication 514

ciphers 515

client-alive-countmax 517

client-alive-interval 518

do show 519

end 519

exit 520

listen 520

macs 521

max servers 522

subsystem 523

CHAPTER 48 SSH Client Configuration Mode Commands 525

ciphers 525

do show 527

end 527

exit 527
preferredauthentications 528
ssh 528

CHAPTER 49 Stats Profile Configuration Mode Commands 531
do show 531
end 532
exit 532
packet-drop 532
qci 533
rat-type 534

CHAPTER 50 Subscriber Configuration Mode Commands 537
aaa 540
access-link ip-fragmentation 542
accounting-mode 543
active-charging bandwidth-policy 544
active-charging link-monitor tcp 545
active-charging radio-congestion 546
active-charging rulebase 547
always-on 548
asn-header-compression-rohc 549
asn nspid 550
asn-pdfid 551
asn-policy 552
associate accounting-policy 554
authorized-flow-profile-id 555
content-filtering category 556
credit-control-client 557
credit-control-group 558
credit-control-service 559
data-tunneling ignore df-bit 560
dcca peer-select 560
default 561

description 564
dhcp dhcpv6 565
dhcp options 566
dhcp parameter-request-list-option 566
dhcp service 567
dns 568
do show 569
eap 569
encrypted password 571
end 571
exit 571
external-inline-server 572
firewall policy 572
fw-and-nat policy 573
gtpp 574
idle-timeout-activity 575
ikev2 tsr 576
ims application-manager 577
ims-auth-service 578
inter-pdsn-handoff 579
ip access-group 579
ip address 580
ip address alloc-method 581
ip address pool 583
ip address secondary-pool 584
ip allowed-dscp 585
ip context-name 588
ip header-compression 589
ip hide-service-address 591
ip local-address 592
ip multicast discard 593
ip qos-dscp 593
ip route 595
ip source-validation 596

ip user-datagram-tos copy 596
ip vlan 598
ipv6 access-group 599
ipv6 address 599
ipv6 dns 600
ipv6 dns-proxy 601
ipv6 egress-address-filtering 602
ipv6 initial-router-advt 603
ipv6 interface-id 604
ipv6 minimum-link-mtu 605
ipv6 secondary-address 606
l2tp send accounting-correlation-info 607
l3-to-l2-tunnel address-policy 608
loadbalance-tunnel-peers 609
long-duration-action 610
max-pdn-connections 611
mediation-device 612
mobile-ip 613
mobile-ip ha 616
mobile-ip reg-lifetime-override 617
mobile-ip send access-technology 618
mobile-ip send accounting-correlation-info 619
mobile-ip send bsid 620
mobile-ip send pcf-address 621
mobile-ip send service-option 622
mobile-ip send subnet-id 623
mobile-ipv6 623
nai-construction-domain 625
nbns 625
nexthop-forwarding-address 626
npu qos 627
nw-reachability-server 628
outbound 629
overload-disconnect 630

password 631
pdif mobile-ip 633
permission 634
policy ipv6 tunnel 634
policy-group 635
ppp 636
prepaid 3gpp2 639
prepaid custom 641
prepaid unclassify 642
prepaid voice-push 643
prepaid wimax 643
proxy-dns intercept list-name 643
proxy-mip 644
qos apn-ambr 645
qos rate-limit 646
qos traffic-police 653
qos traffic-shape 655
radius accounting 658
radius group 660
radius returned-framed-ip-address 661
radius rulebase-format 662
rohc-profile-name 664
secondary ip pool 664
send-destination-pgw 665
service-option 666
simultaneous 667
timeout absolute 668
timeout idle 668
timeout long-duration 670
tpo policy 671
tunnel address-policy 671
tunnel gre 672
tunnel ipip 673
tunnel ipsec 674

tunnel l2tp 675
w-apn 677

CHAPTER 51 Sx Service Configuration Mode Commands 679
bind 679
instance-type 680
sx-protocol association release-timeout 681
sx-protocol heartbeat 681
sx-protocol pdi-optimization 683
sx-protocol supported-features 684
sx-service exclude-user-plane 685
sxa 686
sxab 686
sxb 687

CHAPTER 52 TACACS+ Configuration Mode Commands 689
accounting 690
authorization 691
do show 692
end 692
exit 692
idle-session threshold 693
max-sessions 694
on-authen-fail 694
on-network-error 695
on-unknown-user 696
priv-lvl 697
rem_addr client-ip 698
server 699
user-id 702

CHAPTER 53 TAC Profile Configuration Mode Commands 703
do show 703
end 704

exit 704

tac 704

CHAPTER 54 Telnet Configuration Mode Commands 707

do show 707

end 708

exit 708

max servers 708

CHAPTER 55 TFTP Configuration Mode Commands 711

do show 711

end 712

exit 712

max servers 712

CHAPTER 56 Throttling Override Policy Configuration Mode Commands 715

do show 715

egress bypass-rlf 716

end 718

exit 718

CHAPTER 57 Traffic Optimization Policy Confiugration 721

bandwidth-mgmt 721

curbing-control 722

do show 723

end 724

exit 724

heavy-session 724

link-profile 725

session-params 726

CHAPTER 58 Traffic Optimization Profile Configuration Mode Commands 729

data-record 729

efd-flow-cleanup-interval 730
end 731
exit 731
heavy-session detection-threshold 731
mode 732
stats-interval 733
stats-options 733

CHAPTER 59 Traffic Policy-Map Configuration Mode Commands 735
3gpp2 data-over-signaling 736
access-control 736
accounting suppress 737
accounting trigger 738
class-map 740
description 741
do show 741
end 742
exit 742
flow-tp-trigger 742
ip header-compression 743
qos encaps-header 744
qos traffic-police 745
qos user-datagram dscp-marking 747
sess-tp-trigger 748
type 749

CHAPTER 60 Traffic Policy Group Configuration Mode Commands 753
3gpp2 data-over-signaling 754
access-control 754
accounting suppress 755
accounting trigger 756
class-map 758
description 759
do show 759

end 760
exit 760
flow-tp-trigger 760
ip header-compression 761
qos encaps-header 762
qos traffic-police 763
qos user-datagram dscp-marking 765
sess-tp-trigger 766
type 767

CHAPTER 61 Traffic Steering Configuration Mode Commands 771
appliance-group 771
do show 772
end 772
exit 772
service-chain 773

CHAPTER 62 Traffic Steering Appliance Group Configuration Mode Commands 775
do show 775
end 776
exit 776
ip 776
nsh-format 777

CHAPTER 63 Traffic Steering Service Chain Configuration Mode Commands 779
do show 779
end 780
exit 780
load-balancing 780
sfp 781

CHAPTER 64 TSI Server Configuration Mode Commands 783
do show 783
end 784

exit 784
ip 784
logging 785
sftp 786
update-time 787

CHAPTER 65 Tunnel Interface Configuration Mode Commands 789
description 790
end 790
exit 790
ip address 791
ip ospf authentication-key 792
ip ospf authentication-type 792
ip ospf bfd 793
ip ospf cost 794
ip ospf dead-interval 794
ip ospf hello-interval 795
ip ospf message-digest-key 796
ip ospf network 796
ip ospf priority 797
ip ospf retransmit-interval 798
ip ospf transmit-delay 799
ip vrf 799
ipv6 address 800
tunnel-mode 801

CHAPTER 66 TWAN Profile Configuration Mode Commands 803
access-type 803
dictionary 805
do show 805
end 806
exit 806
radius 806
session-trigger 809

ue-address 810

CHAPTER 67 UDR Format Configuration Mode Commands 813

attribute 813

do show 818

end 819

event-label 819

exit 820

rule-variable 820

CHAPTER 68 UDR Module Configuration Mode Commands 823

cdr 823

do show 828

end 828

exit 829

file 829

CHAPTER 69 UIDH Server Configuration Mode Commands 837

end 837

exit 837

refresh-interval 838

remote-address 839

response-timeout 840

CHAPTER 70 Unnumbered Interface Configuration Mode Commands 841

description 841

end 842

exit 842

CHAPTER 71 UPF Load Control Profile Configuration Mode Commands 843

inclusion-frequency 843

end 844

CHAPTER 72 UPF Overload Control Profile Configuration Mode Commands 845
overload-threshold 845
inclusion-frequency 847
validity-period 848
end 848

CHAPTER 73 User Plane Group Configuration Mode Commands 849
peer-node-id 849

CHAPTER 74 User Plane Profile Configuration Mode 851
do show 851
end 852
endpoint 852
exit 853

CHAPTER 75 User Plane Service Configuration Mode Commands 855
associate 855
associate ise-server-profile name 857
end 857
exit 858

CHAPTER 76 UUT Profile Configuration Mode Commands 859
do show 859
end 860
exit 860
uut 860

CHAPTER 77 Video Group Configuration Mode 863
do show 863
end 864
exit 864
keepalive-server 864

local-address 866
server 867

CHAPTER 78 VLAN Configuration Mode Commands 869
bind interface 869
do show 870
end 871
exit 871
ingress-mode 871
priority 872
shutdown 873
vlan-map 874

CHAPTER 79 WSG Lookup Priority List Configuration Mode Commands 875
do show 875
end 876
exit 876
priority 876

CHAPTER 80 WSG Service Configuration Mode Commands 879
associate subscriber-map 880
bind address 880
deployment-mode 881
dhcp 882
dns-server 883
do show 884
duplicate-session-detection 884
end 885
exit 885
initiator-mode-duration 885
ip 886
ipv6 887
peer-list 888
pre_fragment mtu 889

responder-mode-duration 890

Server dhcp 891

CHAPTER 81 X2-GW Service Configuration Mode Commands 893

bind 893

do show 894

end 895

exit 895

x2-c 895



# About this Guide

**Note** Control and User Plane Separation (CUPS) represents a significant architectural change in the way StarOS-based products are deployed in the 3G, 4G, and 5G networks. Unless otherwise specified, it should not be assumed that any constructs (including, but not limited to, commands, statistics, attributes, MIB objects, alarms, logs, services) referenced in this document imply functional parity between legacy/non-CUPS and CUPS products. Please contact your Cisco Account or Support representative for any questions about parity between these products.

**Note** The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

**Note** The ASR 5000 hardware platform has reached end of life and is not supported in this release. Any references to the ASR 5000 (specific or implied) or its components in this document are coincidental. Full details on the ASR 5000 hardware platform end of life are available at: https://www.cisco.com/c/en/us/products/collateral/wireless/asr-5000-series/eos-eol-notice-c51-735573.html.

**Note** The HA, HSGW, PDSN, and SecGW products have reached end of life and are not supported in this release. Any references to these products (specific or implied) their components or functions including CLI commands and parameters in this document are coincidental and are not supported. Full details on the end of life for these products are available at: https://www.cisco.com/c/en/us/products/collateral/wireless/asr-5000-series/eos-eol-notice-c51-740422.html.

This preface describes the *Command Line Interface Reference* and its document conventions.

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


- CLI Command Sections, on page xxxvi
- Conventions Used, on page xxxvi
- Supported Documents and Resources, on page xxxviii
- Contacting Customer Support, on page xxxviii


# CLI Command Sections

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

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

# Conventions Used

The following tables describe the conventions used throughout this documentation.

| Notice Type | Description |
|---|---|
| Information Note | Provides information about important features or instructions. |

| Notice Type | Description |
|---|---|
| Caution | Alerts you of potential damage to a program, device, or system. |
| Warning | Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards. |

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

| Command Syntax Conventions | Description |
|---|---|
| **{ keyword** or *variable* **}** | Required keyword options and variables are those components that are required to be entered as part of the command syntax.<br>Required keyword options and variables are surrounded by grouped braces { }. For example:<br>**sctp-max-data-chunks { limit** *max_chunks* **\| mtu-limit }**<br>If a keyword or variable is not enclosed in braces or brackets, it is mandatory. For example:<br>**snmp trap link-status** |
| **[ keyword** or *variable* **]** | Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by brackets. |

| Command Syntax Conventions | Description |
|---|---|
| \| | Some commands support multiple options. These are documented within braces or brackets by separating each option with a vertical bar.<br>These options can be used in conjunction with required or optional keywords or variables. For example:<br>**action activate-flow-detection { intitiation \| termination }**<br>or<br>**ip address [ count** *number_of_packets* **\| size** *number_of_bytes* **]** |

# Supported Documents and Resources

## Related Documentation

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

The following related product documents are also available:

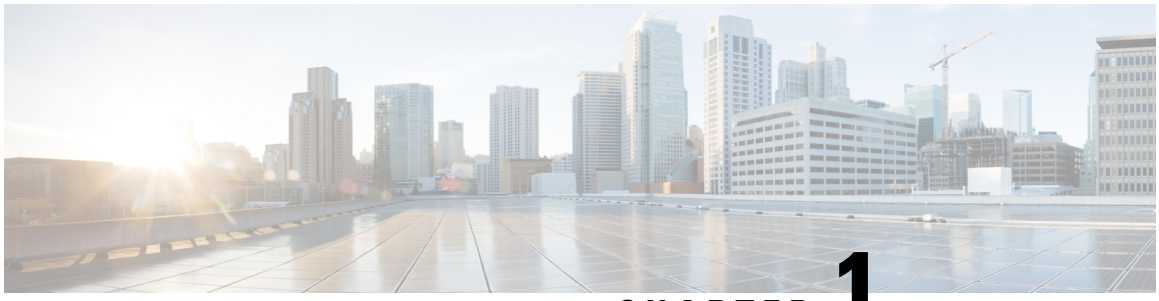
- *AAA Interface Administration and Reference*
- *GTPP Interface Administration and Reference*
- *IPSec Reference*
- Platform-specific System Administration Guides
- Product-specific Administration Guides
- *Release Change Reference*
- *SNMP MIB Reference*
- *Statistics and Counters Reference*
- *Statistics and Counters Reference - Bulk Statistics Descriptions*
- *Thresholding Configuration Guide*

# Contacting Customer Support

Use the information in this section to contact customer support.

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

About this Guide



CHAPTER 1

# Common Commands

This chapter describes the common commands available in each CLI configuration mode.


- do show, on page 1
- end, on page 1
- exit, on page 2


## do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution**

There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

## end

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

**Product**

All

**Privilege** Security Administrator, Administrator

**Syntax Description** `end`

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

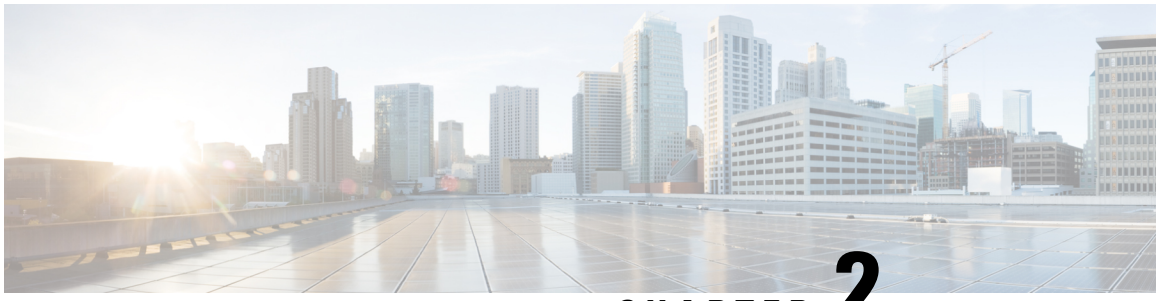
Exits the current mode and returns to the parent configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `exit`

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



CHAPTER 2

# RAC Profile Configuration Mode Commands

The Routing Area Code (RAC) Profile Configuration Mode is used to configure RAC profiles on a per-context basis. This mode enables to select a Virtual APN (vAPN) based on RAC range and discrete values, and thereby a specific UP group and/or IP pool associated with vAPN.

**Command Modes**

Exec > Global Configuration > Context Configuration > RAC Profile Configuration

**configure > context** *context_name* **> rac-profile** *profile_name*

`[context_name]host_name(config-rac-profile)#`

**Important** Available commands or keywords/variables vary based on platform type, product version, and installed license(s).


- do show, on page 3
- end, on page 4
- exit, on page 4
- rac, on page 4


# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**do show**

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# rac

Configures Routing Area Code (RAC) profile with discrete values and range.

**Product** SAEGW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > RAC Profile Configuration

**configure > context** *context_name* **> rac-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rac-profile)#
```

## Syntax Description

**[ no ] rac { range** *start_range* **to** *end_range* **|** *value* **}**

### no

Including **no** with the command disables the specified configuration.

### range *start_range* to *end_range*

Specifies the RAC start and end range of discrete integer value ranging from 0 to 255.

### *value*

The number of discrete RAC values supported per CLI command is 16.

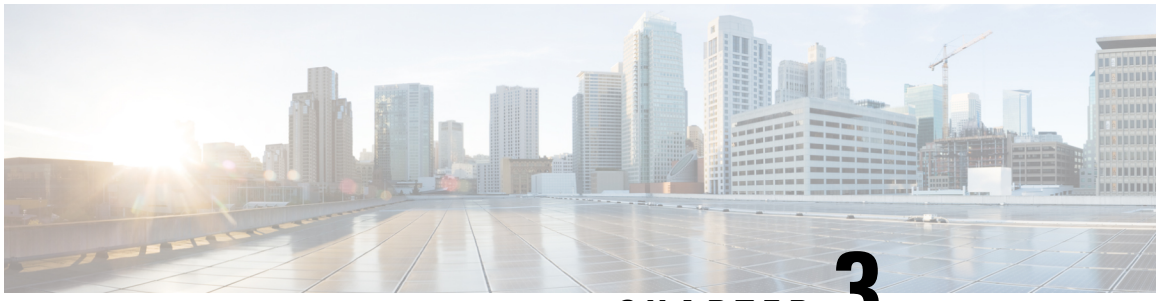
## Usage Guidelines

Use this command to configure RAC profiles per context. The maximum number of RAC discrete values supported in a profile are 100. Memory usage is fixed per profile. RAC range or discrete values can overlap between profiles to support maintenance activities like split existing profile or others. Multiple profiles can be associated with an APN.

### Example

The following command configures RAC range of 1 to 10:

```
rac range 1 to 10
```



CHAPTER 3

# Radio Congestion Policy Configuration Mode Commands

The Radio Congestion Policy Configuration Mode provides the commands to configure the parameters to interpret the congestion indications per TCP flow, the congestion sampling time and reporting frequency.

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

**Command Modes**

Exec > ACS Configuration > Radio Congestion Policy Configuration

**active-charging service** *service_name* **> radio-congestion policy** *policy_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-radio-congestion-policy)#
```

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


- congestion-level, on page 7
- correlation-method, on page 9
- data-loss threshold, on page 10
- do show, on page 11
- end, on page 11
- exit, on page 12
- reporting-interval, on page 12
- rtt-samples, on page 13
- rtt-variance, on page 14
- sampling-interval, on page 14


# congestion-level

Configures the congestion values for each congestion level — None, Low, Medium, High, and Extreme.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec > ACS Configuration > Radio Congestion Policy Configuration

**active-charging service** *service_name* **> radio-congestion policy** *policy_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-radio-congestion-policy)#
```

**Syntax Description**

**congestion-level low** *low_value* **medium** *medium_value* **high** *high_value* **extreme** *extreme_value*
**default congestion-level**

**default**

Configures this command with its default setting.

**low *low_value***

Specifies the congestion range for low congestion.

*low_value* must be a number from 1 to 100.

Default: 20

**medium *medium_value***

Specifies the congestion range for medium congestion.

*medium_value* must be a number from 1 to 100.

Default: 40

**high *high_value***

Specifies the congestion range for high congestion.

*high_value* must be a number from 1 to 100.

Default: 60

**extreme *extreme_value***

Specifies the congestion range for extreme congestion.

*extreme_value* must be a number from 1 to 100.

Default: 80

**Usage Guidelines**

Use this command to configure the congestion values for each congestion level — None, Low, Medium, High, and Extreme. The congestion level values will be reported to the CAE in order to select a video optimization mechanism suitable for subscriber-side network congestion condition. The congestion level range for NO congestion must be less than 10.

### Example

The following command configures the values — *10*, *20*, *30* and *40* for Low, Medium, High and Extreme congestion respectively:

```
congestion-level low 10 medium 20 high 30 extreme 40
```

# correlation-method

Configures the correlation method used to correlate multiple flows of a subscriber to calculate the congestion level of a subscriber.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec > ACS Configuration > Radio Congestion Policy Configuration

**active-charging service** *service_name* **> radio-congestion policy** *policy_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-radio-congestion-policy)#
```

**Syntax Description**

```
correlation-method { mean | optimistic | pessimistic }
default correlation-method
```

#### default

Configures this command with its default setting.

Default: **mean**

#### mean

Configures the mean correlation method. The congestion level is the average across all concurrent TCP flows.

#### optimistic

Configures the optimistic correlation method. The congestion level is the lowest value indicated across all the concurrent flows.

#### pessimistic

Configures the pessimistic correlation method. The congestion level is the highest value indicated across all concurrent flows.

**Usage Guidelines**

Use this command to configure the method used to correlate multiple flows of a subscriber to calculate the congestion level of a subscriber. Each flow will have a congestion level and at the end of each reporting interval, the correlation method will be used to correlate all these flows to arrive at a congestion level for the subscriber.

### Example

The following command configures the **optimistic** correlation method:

```
correlation-method optimistic
```

# data-loss threshold

Configures the acceptable data loss percentage in the network.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec > ACS Configuration > Radio Congestion Policy Configuration

**active-charging service** *service_name* **> radio-congestion policy** *policy_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-radio-congestion-policy)#
```

**Syntax Description**

**data-loss threshold** *threshold_value* **weightage** *weightage_value*
**default data-loss**

#### default

Configures this command with its default setting.

#### threshold *threshold_value*

Configures the percentage of packet loss considered as acceptable in the network. This is used to determine the congestion level to be reported.

*threshold_value* must be a number from 1 to 99.

Default: 1%

#### weightage *weightage_value*

Configures the data loss weightage to be given to packet loss while calculating the congestion level for a subscriber.

*weightage_value* must be a number from 0 to 100.

Default: 50

**Usage Guidelines**

Use this command to configure the acceptable percentage of packet-loss in the network, and the data loss weightage to be given to packet loss while calculating the congestion level for a subscriber. Currently, the minimum value allowed to be configured is 1%. This is required to offset the effects of parameters other than the airlink congestion. The congestion primarily occurs at the airlink, but it is also possible at other places in the flow path. The link monitor cannot distinguish between airlink and congestion at any other point. For example, if 1% packet loss is considered normal in some network and if some flow of a subscriber experiences

a packet loss of 2%, then it will be considered as a sign of congestion. If some flow of a subscriber has a packet loss of 1% or less, then it is not considered as congestion, as it is in the normal range for that network.

### Example

The following command sets the packet loss percentage to *1* and the data loss weightage to *50*:

```
data-loss threshold 1 weightage 50
```

# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
end
```

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**exit**

**Usage Guidelines**

Use this command to return to the parent configuration mode.

# reporting-interval

Configures the reporting interval in terms of the number of sampling intervals.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec > ACS Configuration > Radio Congestion Policy Configuration

**active-charging service** *service_name* **> radio-congestion policy** *policy_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-radio-congestion-policy)#`

**Syntax Description**

**reporting-interval** *interval_value* **min-samples-required** *num_samples*
**default reporting-interval**

**default**

Configures this command with its default setting.

**reporting-interval *interval_value***

Specifies the reporting interval in seconds.

*interval_value* must be a number from 1 to 60.

Default: 5 seconds

**min-samples-required *num_samples***

Specifies the minimum number of samples required for reporting.

*num_samples* must be a number from 1 to 60.

Default: 5

**Usage Guidelines** Use this command to configure the reporting interval in terms of the number of sampling intervals. This indicates after how many sampling intervals, the report must be generated and reported to external entities like PCRF if required.

#### Example

The following command configures the reporting interval as *10* seconds and *5* samples for a subscriber:

```
reporting-interval 10 min-samples-required 5
```

# rtt-samples

Configures RTT (Round Trip Time) samples for base RTT.

**Product** All

**Privilege** Security Administrator, Administrator, Operator, Inspector

**Command Modes** Exec > ACS Configuration > Radio Congestion Policy Configuration

**active-charging service** *service_name* **> radio-congestion policy** *policy_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-radio-congestion-policy)#
```

**Syntax Description**

```
rtt-samples min_samples
default rtt-samples
```

#### default

Configures this command with its default setting.

Default:

#### *min_samples*

Specifies the minimum number of RTT samples for base RTT.

*min_samples* must be a number from 1 to 20.

**Usage Guidelines** Use this command to configure the minimum number of RTT samples for base RTT.

#### Example

The following command configures *10* RTT samples:

```
rtt-samples 10
```

# rtt-variance

Configures the RTT (Round Trip Time) variance.

**Product**

MVG

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec > ACS Configuration > Radio Congestion Policy Configuration

**active-charging service** *service_name* **> radio-congestion policy** *policy_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-radio-congestion-policy)#
```

**Syntax Description**

**rtt-variance threshold** *variance_percent* **weightage** *rtt_weightage*
**default rtt-variance**

**default**

Configures this command with its default setting.

**rtt-variance threshold *variance_percent***

Specifies the RTT acceptable variance percentage.

*variance_percent* must be a number from 50 to 500.

Default: 100

**weightage *rtt_weightage***

Specifies the weightage to be given to RTT variance while calculating the congestion level of a subscriber.

*rtt_weightage* must be a number from 0 to 100.

Default: 50

**Usage Guidelines**

Use this command to configure the RTT variance.

**Example**

The following command sets the RTT variance threshold to *60*% and weightage to *80*:

```
rtt-variance threshold 60 weightage 80
```

# sampling-interval

Configures the sampling interval.

**Product**

All

## Privilege

Security Administrator, Administrator, Operator, Inspector

## Command Modes

Exec > ACS Configuration > Radio Congestion Policy Configuration

**active-charging service** *service_name* **> radio-congestion policy** *policy_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-radio-congestion-policy)#
```

## Syntax Description

**sampling-interval** *sampling_interval*
**default sampling-interval**

### default

Configures this command with its default setting.

Default: 5 seconds

### *sampling_interval*

Specifies the sampling interval, in seconds.

*sampling_interval* must be a number from 2 to 60.

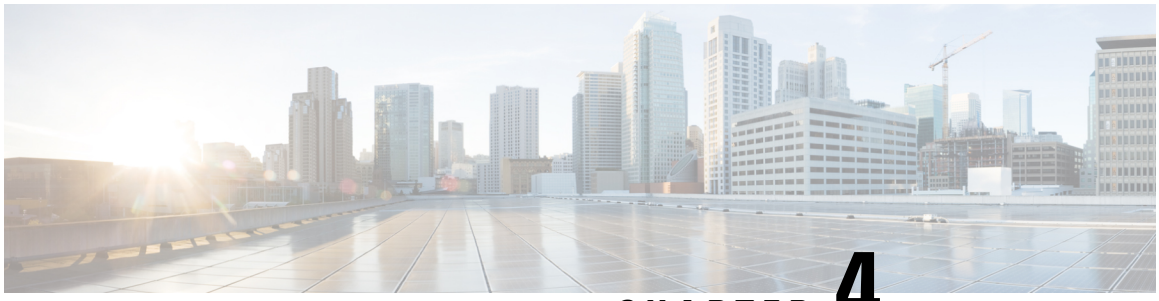
## Usage Guidelines

Use this command to configure the sampling interval. This indicates the interval in seconds at which various TCP parameters are captured to determine the congestion level.

### Example

The following command specifies a sampling interval of *20* seconds:

```
sampling-interval 20
```



CHAPTER 4

# RANAP Cause Code Group Configuration Mode

Commands in this mode enable the operator to define multiple cause codes for the 3G service.

**Command Modes**

Exec > Global Configuration > LTE Policy Configuration > RANAP Cause Code Configuration

**configure > lte-policy > cause-code-group** *group_name* **protocol ranap**

Entering the above command sequence results in the following prompt:

```
[local] host_name(ranap-cause-code)
```

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


- cause, on page 17
- do show, on page 18
- end, on page 19
- exit, on page 19


# cause

Enables the operator to specify one or more cause codes for the 3G service.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > LTE Policy Configuration > RANAP Cause Code Configuration

**configure > lte-policy > cause-code-group** *group_name* **protocol ranap**

Entering the above command sequence results in the following prompt:

```
[local] host_name(ranap-cause-code)
```

**Syntax Description**

**cause** *cause_code*
**no cause** *cause_code*

**no**

When included with the command, the specified cause code is deleted from the group. If all cause codes are deleted from the group then the group is automatically deleted.

***cause_code***

Enter an integer from 1 to 512 to identify a cause code. Valid options are listed in 3GPP TS 25.413 v11.5.0 (or later version), subsection on *Cause* in section for *Radio Network Layer Related IEs*.

**Usage Guidelines**

A maximum of 16 RANAP protocol cause codes can be defined per group. Note that under each cause code group the maximum number of cause codes (ranap+bssgp+s1ap) that can be supported is 16.

Benefit of using the cause code group for 3G service is

- ***if*** the RANAP cause code configured by the operator matches with the cause received in the Iu-Release Request message, and
- ***if*** the Subscriber Overcharging Protection feature is enabled for 3G service in the SGSN-Service configuration,
- ***then*** the S4-SGSN includes ARRL (i.e., Abnormal Release of Radio Link) bit in Release Access Bearer Request message initiated on Iu-Release.

**Example**

Repeat the command to define multiple cause codes for the group.

```
cause 27
cause 121
cause 200
```

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`end`**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

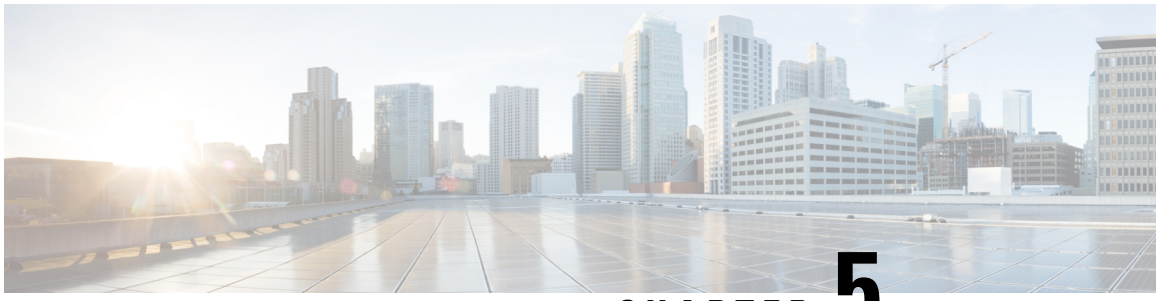
**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`exit`**

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

**exit**



CHAPTER 5

# Remote Address List Configuration Mode Commands

The Remote Address List Configuration Mode is used to configure address lists for the Remote Address-based Accounting feature on a per-context basis.

**Command Modes**

Exec > Global Configuration > Context Configuration > Remote Address List Configuration

**configure > context** *context_name* **> radius accounting ip remote-address list** *list_number*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-remaddr-list)#`

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


- address, on page 21
- do show, on page 22
- end, on page 23
- exit, on page 23


# address

Configures addresses within a Remote Address List.

**Product**

PDSN

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Remote Address List Configuration

**configure > context** *context_name* **> radius accounting ip remote-address list** *list_number*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-remaddr-list)#`

**Syntax Description** **[ no ] address** *ip_address* **netmask** *subnet*

**no**

Removes a previously configured address.

***ip_address***

Specifies the IP address of the remote device.

*ip_address* is entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**netmask *subnet***

Specifies the subnet mask of the remote device.

*subnet* is the netmask expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Usage Guidelines** Use this command to configure remote address lists for use with the Remote Address-based accounting feature. A maximum of 10 address can be configured per list.

**Example**

The following command adds an IP address of *192.168.100.1* with a subnet mask of *255.255.255.224* to the list:

```
address 192.168.100.1 netmask 255.255.255.224
```

# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **do show**

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `end`

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

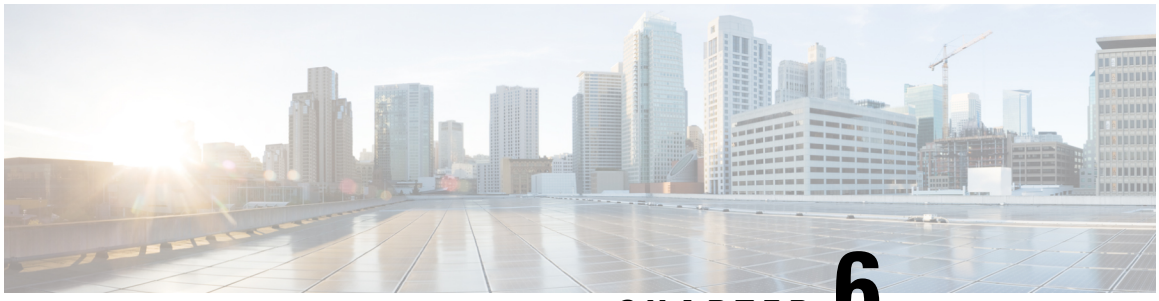
**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `exit`

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

exit



CHAPTER 6

# Remote Server List Configuration Mode Commands

**Command Modes**

The Remote Server List Configuration Mode manages the list of server addresses to which a context has access.

Exec > Global Configuration > Remote Server List Configuration

**configure > context** *context_name* **> remote-server-list name** *list_name*

`[context_name]host_name(config-remote-server-list)#`

**Important** Available commands or keywords/variables vary based on platform type, product version, and installed license(s).


- address, on page 25
- do show, on page 26
- end, on page 26
- exit, on page 27


# address

Configures or removes an IP address to a remote server.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Remote Server List Configuration

**configure > context** *context_name* **> remote-server-list name** *list_name*

`[context_name]host_name(config-remote-server-list)#`

**Syntax Description**

**address** *remote-ip-address* **netmask** *ip_netmask*
**no address** *remote-ip-address* **netmask** *ip_netmask*

**no**

Removes the specified IP address from the Remote Server List.

***remote-ip-address*** **netmask** ***ip_netmask***

Specifies the IP address and netmask of the remote server in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Usage Guidelines** Use this command to create and maintain a list of remote servers accessible by this context.

**Example**

```
address 193.154.78.9 netmask 255.255.255.0
```

# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
end
```

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

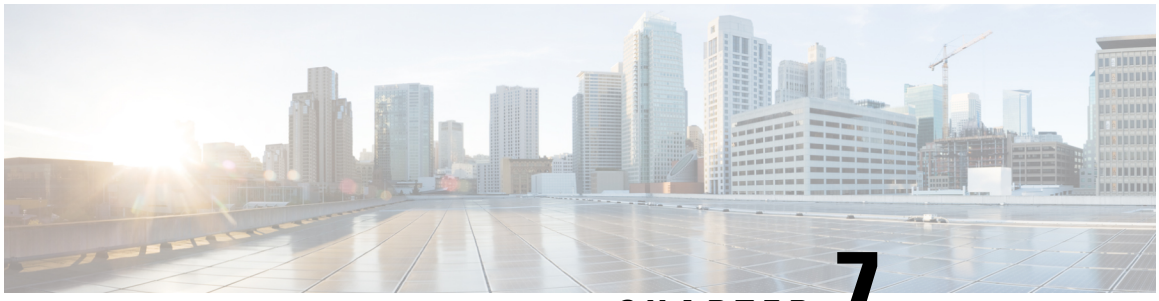
**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `exit`

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

exit



CHAPTER 7

# Remote Secret List Configuration Mode Commands

**Command Modes**

The Remote Secret List Configuration Mode manages the list of for storing remote secrets based on ID type.

Exec > Global Configuration > Remote Secret List Configuration

**> crypto remote-secret-list** *listname*

`[local_context]host_name(config-remote-server-list)#`


- do show, on page 29
- end, on page 30
- exit, on page 30
- remote-id, on page 30


# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**do show**

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution**

There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
end
```

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
exit
```

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

# remote-id

Configures the remote pre-shared key based on the ID type.

**Product** WSG

**Privilege** Security Administrator

**Command Modes** Exec > Global Configuration > Remote Secret List Configuration

**> crypto remote-secret-list** *listname*

```
[local_context]host_name(config-remote-server-list)#
```

**Syntax Description**

```
remote-id id-type { der-asn1-dn | fqdn | ip-addr | key-id | rfc822-addr
} id id_value secret [ encrypted ]  key key_value
no remote-id id-type { der-asn1-dn | fqdn | ip-addr | key-id | rfc822-addr
 } id id_value
```

**no**

Removes the specified ID from the remote secret list.

**id-type { der-asn1-dn | fqdn | ip-addr | key-id | rfc822-addr }**

Configures the NAI IDr type parameter. If no id-type is specified, then **rfc822-addr** is assumed.

- **der-asn1-dn**: configures NAI Type DER_ASN1_DN (Distinguished Encoding Rules, ASN.1 encoding, Distinguished Name)
- **fqdn**: configures NAI Type ID_FQDN (Internet Fully Qualified Domain Name).
- **ip-addr**: configures NAI Type ID_IP_ADDR (IP Address).
- **key-id**: configures NAI Type ID_KEY_ID (opaque octet string).
- **rfc822-addr**: configures NAI Type ID_RFC822_ADDR (RFC 822 email address).

**secret [ encrypted ] key *key_value***

Specifies the use of an encrypted or plain text secret key. *key_value* is an alphanumeric string of 1 through 255 bytes or a hexadecimal string of 16 to 444 bytes.

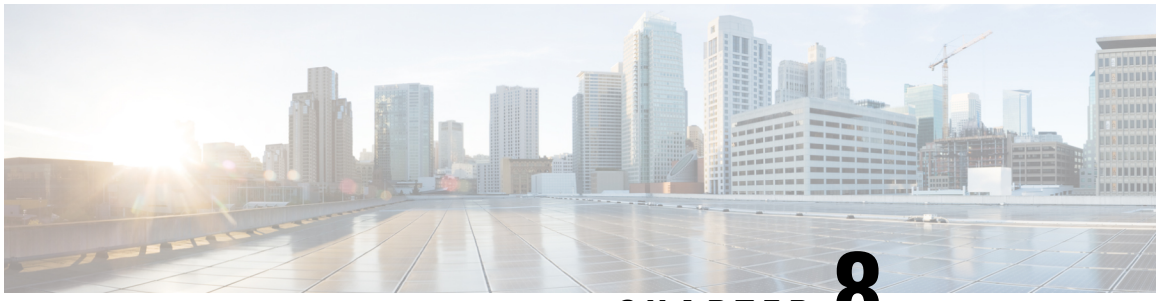
## Usage Guidelines

Use this command to enter up to 1000 entries in the remote secret list. Each entry is designated by ID type and ID value. Repeat the command sequence to add entries to the list.

### Example

The following command enters an ip address in the remote secret list:

```
remote-id id-type ip-addr id 10.1.1.1
```



CHAPTER 8

# RLF Template Configuration Mode Commands

Rate Limiting Function (RLF) Template Configuration Mode is accessed from the Global Configuration Mode. This mode allows an operator to configure the RLF template that can be associated with Diameter and other applications for throttling and rate controlling of messages sent to external network interfaces.

**Important** Rate Limiting Function (RLF) is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

**Command Modes**

Exec > Global Configuration > RLF Template Configuration

**configure > rlf-template** *rlf_template_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-rlf-template)#
```

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


- delay-tolerance, on page 33
- do show, on page 34
- end, on page 35
- exit, on page 35
- msg-rate, on page 35
- threshold, on page 36


# delay-tolerance

Defines the maximum number of seconds a control plane signaling message can be queued before being processed. After exceeding this delay, the message is dropped.

**Product**

GGSN

P-GW

SaMOG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > RLF Template Configuration

**configure > rlf-template** *rlf_template_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-rlf-template)#
```

**Syntax Description**

**delay-tolerance** *tolerance_value* **[ -noconfirm ]**
**default delay-tolerance**

**default**

Removes the configuration associated with the RLF template. Default value is 2.

***tolerance_value***

Specifies the maximum number of seconds a message can be queued in the RLF module. The message must be sent after expiry of "delay-tolerance" seconds.

*tolerance_value* must be an integer from 0 through 10. Default value is 2.

**[ -noconfirm ]**

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

**Usage Guidelines**

Use this command to define the maximum number of seconds a message can be queued in the RLF module before being processed. After exceeding this delay, the message is dropped.

**Example**

The following command sets the value of delay tolerance to 4 seconds:

**delay-tolerance 4**

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**do show**

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`end`**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`exit`**

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

# msg-rate

Sets the maximum number of messages that can be processed per second.

**Product** GGSN

P-GW

SaMOG

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > RLF Template Configuration

**configure > rlf-template** *rlf_template_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-rlf-template)#
```

**Syntax Description**

**msg-rate** *tps_value* **burst-size** *size* **[ -noconfirm ]**

***tps_value***

Specifies the number of messages that can be processed per second. This is the maximum number of allowed transactions per second (TPS) for an external interface.



**Important** The TPS value (configured per external interface) is at a chassis-level and is distributed appropriately to all session managers, AAA manager, Diamproxy, or any other applications that use RLF. RLF employs the Token Bucket Algorithm to achieve the rate limiting.

*tps_value* must be an integer from 1 through 100000.

**burst_size *size***

Defines the maximum number of messages (burst) that can be sent out together at any instant of time. If this setting is not configured, the default value is the current message rate.

Burst size is used to derive the shaping interval in such a way that it splits the 1000 ms in N slots, where N can be 1, 2, 4, 5, 10, 20, 50, and 100.

*size* must be an integer from 1 through 100000.

**[ -noconfirm ]**

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

**Usage Guidelines**

Use this command to define the number of messages that can be processed per second. This is the maximum number of allowed transactions per second (TPS) for an external interface. The RLF ensures that the maximum configured TPS rate is not exceeded on the interface.

If burst-size is not configured. the messages are sent without delay when they arrive in RLF. For example, if the CLI command **msg-rate 1000 burst-size 100** is configured, then all 1,000 messages are sent to an external interface in bursts of 100 messages (burst-size). If the burst size is not configured, then all 1,000 messages are sent as they arrive in RLF (regardless of TPS).

**Example**

The following command sets the value of message rate to 20:

```
msg-rate 20
```

# threshold

Configures the threshold for rate-limiting the outgoing messages.

**Product**

GGSN

P-GW

SaMOG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > RLF Template Configuration

**configure > rlf-template** *rlf_template_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-rlf-template)#
```

**Syntax Description**

**threshold { lower** *lowerThreshold_value* **| upper** *upperThreshold_value* **} [ -noconfirm ]**
**default threshold**

#### default

Returns the command to its default settings.

#### lower *lowerThreshold_value*

This threshold indicates that the application has message-rate control enabled.

Default is 30%. If the number of outstanding messages in the RLF queue drops below 30% of msg-rate, RLF will transition to READY state.

#### upper *upperThreshold_value*

This threshold indicates that action will be taken when the message-rate reaches the maximum limit.

Default is 80%. If the number of outstanding messages in the RLF queue exceeds 80% of msg-rate, RLF will transition to OVER_THRESHOLD state.

**Usage Guidelines**

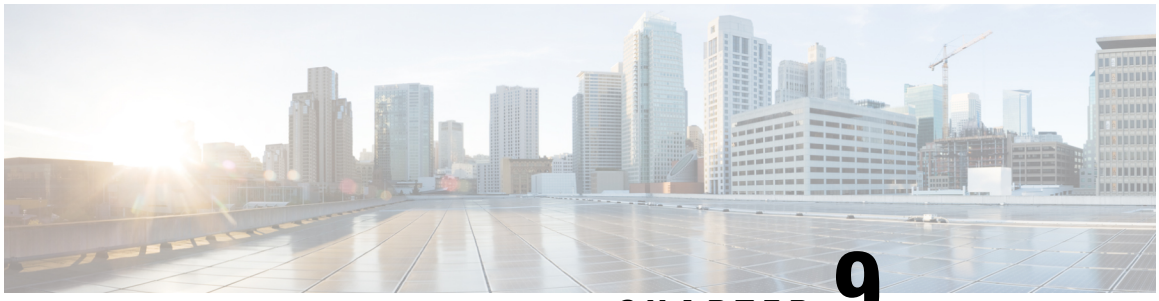
Use this command to configure the desired threshold value for rate limiting the outgoing messages.

The configurable threshold value of TPS for an interface is used to notify applications of corrective actions when the threshold criteria is met.

#### Example

The following command configures the upper threshold to 80 and the lower threshold to 60 for throttling and rate control:

```
threshold upper 80 lower 60
```



CHAPTER 9

# RNC Configuration Mode Commands

## Command Modes

The RNC (radio network controller) configuration mode defines the parameters related to the SGSN connection with an RNC.

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure > context** *context_name* **> iups-service** *service_name* **> rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-iups-service-rnc)#`

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

**Note** From R15.0 onwards, License Control is implemented on all Network Sharing related commands.


- associate-gtpu-bind-address, on page 40
- description, on page 41
- direct-tunnel, on page 41
- do show, on page 42
- dual-address-pdp, on page 43
- enb-data-forward, on page 44
- enb-direct-data-forward, on page 45
- end, on page 45
- exit, on page 46
- lac, on page 46
- mbms, on page 47
- overload-action disable, on page 47
- paging-non-searching-indication, on page 49
- pointcode, on page 50
- pooled, on page 51
- rab-asymmetry-indicator, on page 51
- rab-modify-procedure, on page 52

- ranap arp-ie, on page 54
- ranap bidirectional-always, on page 54
- ranap eutran-service-handover-ie, on page 55
- ranap global-cn-id, on page 57
- ranap paging-area-id, on page 58
- ranap paging-cause-ie, on page 59
- ranap rab-arsp-ue-radio-lost, on page 61
- ranap rab-release-with-radiolost, on page 62
- ranap rfsp-id-ie, on page 63
- ranap signalling-indication-ie, on page 63
- ranap ue-ambr-ie, on page 64
- ran-information-management, on page 65
- release-compliance, on page 66
- reset-resource, on page 68


# associate-gtpu-bind-address

This command defines the GTP-U loopback address and associates (binds) this address with a particular interface (non-loopback) address.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure > context** *context_name* **> iups-service** *service_name* **> rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax Description**

**`[ no ] associate-gtpu-bind-address`** *`ip_address`* **`to-interface-address`** *`ip_address`*

**no**

Removes the loopback address definition and interface association from the current RNC configuration.

***ip_address***

*ip_address:* Must be specified using the standard IPv4 dotted decimal notation.

**Usage Guidelines**

Use this command to setup associations between loopback GTP-U addresses and a non-loopback addresses.

**Example**

Bind the GTP-U loopback address of *123.1.1.1* to interface address *222.1.1.1*:

```
associate-gtpu-bind-address 123.1.1.1 to-interface-address 222.1.1.1
```

# description

This command defines an alphanumeric string that is intended to provide descriptive information about the radio network controller (RNC). This is used for operator reference only.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure > context** *context_name* **> iups-service** *service_name* **> rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-iups-service-rnc)#`

**Syntax Description**

**`description`** *`string`*
**`no description`**

**no**

Removes the description string from the current RNC configuration.

***string***

Specifies the alphanumeric string that is stored. must be from 1 through 255 alphanumeric characters. Strings with spaces must be enclosed in double-quotes. See the example below.

**Usage Guidelines**

Use this command to set a description for reference by operators.

**Example**

The following command sets the description to identify a particular RNC and carrier in Uganda *"RNC1 Carrier2 Uganda"*:

**`description "RNC1 Carrier2 Uganda"`**

# direct-tunnel

This command enables/disables the direct tunnel feature through the interface to the radio network controller (RNC).

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure > context** *context_name* **> iups-service** *service_name* **> rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax Description**

```
direct-tunnel not-permitted-by-rnc
default direct-tunnel
```

**default**

Sets the direct tunnel support on RNC to default mode; i.e. enabling direct tunnel.

**not-permitted-by-rnc**

Default: enabled

Disables the direct-tunnel support on radio network controller (RNC).

**Usage Guidelines**

Use this command to disable/enable the direct-tunnel function through the interface to the RNC.

**Example**

Following command disables the direct tunnel support to the RNC:

```
direct-tunnel not-permitted-by-rnc
```

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# dual-address-pdp

This command enables the SGSN to work with an RNC with functioning dual address (IPv4v6) bearer support capability. By default, it is assumed that the RNC does not support dual PDP-type addressing.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure > context** *context_name* **> iups-service** *service_name* **> rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax Description**

```
dual-address-pdp { not-supported | supported }
default dual-address-pdp
```

**default**

Resets the SGSN to function with an RNC that is not supporting dual PDP addressing.

**not-supported**

Default

Enables the SGSN to work with an RNC that does not support dual PDP-type addressing. It allows a single address bearer PDP-type to be activated with a configured PDP-type.

**supported**

Enables the SGSN to work with an RNC that does support dual PDP-type addressing.

**Usage Guidelines**

This command enables the SGSN to support dual PDP-type addressing (IPv4v6) per RNC.

For a dual PDP context to be activated, the RNC should support the PDP-type IPv4v6 in the RAB assignment request. For an RNC that does support the dual PDP-type addressing, use this command to change the default configuration and to configure the SGSN to work with the RNC's dual address bearer support capability.

If the RNC does not support this functionality, then the **default** form of this command should be configured to enable the SGSN to activate a single-address bearer PDP context even if (1) the UE requests PDP type IPv4v6 and if (2) the subscription allows this PDP type. The single address bearer PDP type will be activated with a configured PDP type.

When a UE moves from an RNC that supports dual PDP-type addressing to another RNC that does not support dual PDP-type addressing, then the SGSN will deactivate the PDP context. This is done because, even if we preserve the PDP contexts, the UE would be unaware of the preserved PDP context. This would lead to non-synchronized behavior in the network. So the SGSN deactivates the PDP context with cause code "reactivation-required" to ensure the UE, RNC, SGSN, and GGSN are in synch. As well, this gives the UE the opportunity to activate a PDP context again without dual bearers.

The **sgsn-rnc-no-dual-pdp-init-pdp-deact** disconnect reason is used to indicate that a PDP context has been deactivated because of roaming into an RNC that does not support this feature.

**Important** For this configuration to function, support for dual PDP-type addressing must be enabled at the global level (the default). To confirm the functionality is enabled, issue the **show sgsn-mode** command from the Exec mode. If the PDP-type addressing is not enabled, then refer to the instructions for the **dual-address-pdp** command in the *SGSN Global Configuration Mode Commands* section.

### Example

Use the following command to enable dual PDP-type addressing with a supporting RNC:

```
dual-address-pdp supported
```

# enb-data-forward

Use this command to enable forwarding of data from this RNC to eNodeB.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure** > **context** *context_name* > **iups-service** *service_name* > **rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax Description**

```
[no] enb-data-forward
```

**[ no ]**

Disables the forwarding of data from this RNC to eNodeB.

**enb-data-forward**

Enables the forwarding of data from this RNC to eNodeB.

**Usage Guidelines**

Use this command to configure forwarding of data from the RNC to eNodeB

### Example

Use the following command to enable forwarding of data from this RNC to eNodeB.

```
enb-data-forward
```

# enb-direct-data-forward

Selects the setup of indirect data forwarding tunnels (IDFT) between the eNodeB and the RNC via the SGW during SRNS relocation, or, selects the use of direct data forwarding.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure > context** *context_name* **> iups-service** *service_name* **> rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax Description**

**[no] enb-direct-data-forward**

**[ no ]**

Disables direct data forwarding and enables the setup of indirect data forwarding tunnels between the eNodeB and the RNC via the SGW during SRNS relocation. This allows the S4-SGSN to support connected mode handovers between the UTRAN and E-UTRAN networks across the S3 interface. This is the default setting.

**enb-direct-data-forward**

Enables the use of direct data forwarding between the eNodeB and the RNC via the SGW. If this setting is configured and the SGSN receives a Relocation Required message from this RNC for a subscriber with target node as an eNodeB, then the SGSN will set the indication->DFI (direct forwarding indicator) flag in the Forward Relocation Request message sent across the S3 interface. Use of this command disables the setup of indirect data forwarding tunnels.

**Usage Guidelines**

Use this command to enable the setup of direct data forwarding tunnels between the eNodeB and the RNC during inter RAT connected mode handover. Enabling direct data forwarding tunnels allows the S4-SGSN to support connected mode handovers between the UTRAN and E-UTRAN networks across the S3 interface without the use of indirect data forwarding tunnels through SGW. Once direct data forwarding is enabled, indirect data forwarding is automatically disabled.

**Example**

Enable the setup of indirect data forwarding tunnels between the eNodeB and RNC via the SGW during SRNS relocation. This command also disables direct data forwarding.

**no enb-direct-data-forward**

# end

Exits the configuration mode and returns to the Exec mode.

**Product**

SGSN

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Change the mode to the Exec mode.

# exit

Exits the current configuration mode and returns to the IuPS Service configuration mode.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

**Usage Guidelines** Return to the previous configuration mode.

# lac

This command identifies a Local Area Concentrator (LAC) and a Remote Area Concentrator (RAC) and associates them with this RNC definition.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure > context** *context_name* **> iups-service** *service_name* **> rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-iups-service-rnc)#`

**Syntax Description** `[ no ] lac lac_id rac rac_id`

**no**

Deletes the LAC and RAC information from the system configuration.

***lac_id***

A unique numeric identifier for the LAC associated with the RNC.

*lac_id* must be an integer between 1 and 65535.

***rac_id***

A unique numeric identifier for the RLAC associated with the RNC.

*rac_id* must be an integer between 1 and 255.

**Usage Guidelines** Creates an association with a specific LAC and RAC.

### Example

Associate LAC *545* and RAC *23* with this RNC:

```
lac 545 rac 23
```

# mbms

Configures RNC options for multimedia broadcast multicast service.

**Important** This feature and command are currently under development and are not supported.

**Product** SGSN

# overload-action disable

This command maps an action to be taken if traffic reaches or exceeds defined levels.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure** > **context** *context_name* > **iups-service** *service_name* > **rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax Description**

```
overload-action disable { activate | attach | auth-challenge |
modify-request | paging-downlink-data | ptmsi-reallocation |
service-request-data | sms | srns } traffic-level traffic-level
[ no | default ] overload-action disable { activate | attach |
auth-challenge | modify-request | paging-downlink-data | ptmsi-reallocation
 | service-request-data | sms | srns }
```

### no

Removes the defined overload action from configuration.

### default

Resets the traffic level to the default level for the associated overload action.

**activate traffic-level *traffic-level***

The system rejects new requests to activate PDP contexts if the defined traffic-level is exceeded.

*traffic-level*: An integer 1 to 15.

Default: 14

**attach traffic-level *traffic-level***

The system rejects new requests for GPRS attach if the defined traffic-level is exceeded.

*traffic-level*: An integer 1 to 15.

Default: 15

**auth-challenge traffic-level *traffic-level***

The system skips performing authentication challenges if the defined traffic-level is exceeded.

*traffic-level*: An integer 1 to 15.

Default: 4

**modify-request *traffic-level***

The system rejects requests to modify a PDP context if the defined traffic-level is exceeded.

*traffic-level*: An integer 1 to 15.

Default: 12

**paging-downlink-data traffic-level *traffic-level***

If the defined traffic-level is exceeded, then paging is not performed for data during downlinks if RABs are not available.

*traffic-level*: An integer 1 to 15.

Default: 11

**ptmsi-reallocation traffic-level *traffic-level***

The system skips performing ptmsi-reallocation if the defined traffic-level is reached or exceeded.

*traffic-level*: An integer from 1 to 15.

Default: 4

**service-request-data traffic-level *traffic-level***

The system rejects service requests to accept data and establish new RABs if the defined traffic-level is reached or exceeded.

*traffic-level*: An integer from 1 to 15.

Default: 10

**sms traffic-level *traffic-level***

The system rejects SMS signaling if the defined traffic-level is reached or exceeded.

*traffic-level*: An integer 1 to 15.

Default: 8

**srns traffic-level *traffic-level***

The SGSN rejects/disables SRNS if the target RNC is in overload at the specified traffic level. This keyword setting is effective for both Inter-SGSN SRNS and Intra-SGSN SRNS.

*traffic-level*: An integer 1 to 15.

Default: 15

**Usage Guidelines**

This command defines traffic levels and the actions to take if traffic exceeds the defined levels. The command can be re-entered multiple times to create individual definitions for each type of traffic level and action.

**Example**

Use the following to instruct the system to reject service requests to establish new RABs if the traffic level reaches *3*:

```
overload-action disable service-request-data traffic-level 3
```

# paging-non-searching-indication

This command instructs the SGSN to include the non-searching indicator flag in the page-request message.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure > context** *context_name* **> iups-service** *service_name* **> rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax Description**

```
paging-non-searching-indication { non-searching | searching }
[ no | default ] paging-non-searching-indication
```

**no | default**

This is the default. Entering no or default with this command disables the inclusion of the flag.

**non-searching**

Set the non-searching-indication to non-searching in the page-request message.

**searching**

Set the non-searching-indication to searching in the page-request message.

**Usage Guidelines** Use this command to determine which type of search indicator flag will be included in the page-request message.

### Example

Use this command to include the non-searching flag in page-request messages:

```
paging-non-searching-indication non-searching
```

# pointcode

Configures the point code of the RNC.

The access protocol that is part of the IuPS Service configuration mode must be configured prior to defining the RNC's point code.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure > context** *context_name* **> iups-service** *service_name* **> rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax Description**

```
pointcode pt_code
no pointcode
```

#### no

Deletes the RNC's point code information from the system configuration.

#### *pt_code*

Point code in dotted-decimal format :

- ITU Range 0.0.1 to 7.255.7
- ANSI Range 0.0.1 to 255.255.255
- TTC Range 0.0.1 to 15.31.255
- string of 1 to 11 characters

**Usage Guidelines** Use this command to identify the point code of the associated RNC.

### Example

Identify the pointcode for this RNC as *1.234.2*:

```
pointcode 1.234.2
```

# pooled

Configure an RNC as either 'pooled' or 'non-pooled'.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure > context** *context_name* **> iups-service** *service_name* **> rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax Description**

```
pooled
[ default | no ] pooled
```

**default | no**

Entering either **default** or **no** returns the RNC configuration to the default 'non-pooled' state.

**Usage Guidelines**

Each RNC, one-at-a-time, can be identified as 'pooled' -- as participating within an SGSN pool -- or 'non-pooled'. Pooled RNCs can co-exist with non-pooled RNCs.

**Example**

Identify this RNC as being part of an SGSN pool:

```
pooled
```

# rab-asymmetry-indicator

Configures the SGSN to force "Asymmetric-Bidirecitonal" as the RAB Asymmetry Indicator when uplink/downlink bitrates are equal.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure > context** *context_name* **> iups-service** *service_name* **> rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax Description**

```
rab-asymmetry-indicator symmetric-bidirectional
force-asymmetric-bidirectional
no rab-asymmetry-indicator symmetric-bidirectional
```

```
force-asymmetric-bidirectional
default rab-asymmetry-indicator
```

**default | no**

Disables the override and sets the indicator based on the symmetry of the bitrates as described for the Default Functionality below.

**Usage Guidelines**

This command defines an override that uses "Asymmetric-Bidirecitonal" as the RAB Asymmetry Indicator when uplink/downlink bitrates are equal (default functionality item #1). This overrides the default functionality (see below) for the RAB indicator in the RAB Assignment Request.

As a result of using this override command, two sets of bitrates, one for downlink and one for uplink, will be included in RAB Assignment Requests for establish or modify per 3GPP TS 25.413.

**Default Functionality:** The SGSN sets the value of the RAB Asymmetry Indicator based on symmetry of negotiated maximum bitrates in the following manner:

- If the uplink and downlink bitrates are equal, then it is set to "Symmetric-Bidirectional".
- If uplink bitrate is set to 0 kbps, then it is set to "Asymmetric-Unidirectional-Downlink".
- If downlink bitrate is set to 0 kbps, then it is set to "Asymmetric-Unidirectional-Uplink".
- If the uplink and downlink bitrates are non-zero and different, then it is set to "Asymmetric-Bidirectional".

**Example**

Override the use of the "Symmetric-Bidirectional" RAB Asymmetry Indicator for equal up/downlink bitrates with the following command:

```
rab-asymmetry-indicator symmetric-bidirectional
force-asymmetric-bidirectional
```

Disable the override with the following command:

```
no rab-asymmetry-indicator symmetric-bidirectional
force-asymmetric-bidirectional
```

# rab-modify-procedure

This command configures how the RAB (radio access bearer) assignment procedure will be modified.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure** > **context** *context_name* > **iups-service** *service_name* > **rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax Description**

```
rab-modify-procedure { normal-modify [ data-vol-report-ind-ie |
pdp-type-info-ie ] | release-and-establish }
```

```
default rab-modify-procedure
no rab-modify-procedure normal-modify [ data-vol-report-ind-ie |
pdp-type-info-ie ]
```

### default

Resets the configuration to use 'release-and-establish', the SGSN's default RAB Assignment modification procedure.

### normal-modify

Selects the normal modification procedure for RAB assignment. Either one of two IE options can be included:

- **data-vol-report-ind-ie** sends the "Data Volume Reporting Indication IE" as part of the modification request of the RAB Assignment Request procedure.
- **pdp-type-info-ie** sends the "PDP Type Information IE" as part of the modification request of the RAB Assignment Request procedure.

### release-and-establish

Instructs the system to release and establish the RAB procedure.

In the case of S4-SGSN, SGSN does not send the Release Access Bearer Request to the S-GW as the RAB is immediately re-established after the release of RAB in direct tunnel.

## Usage Guidelines

Set the type of modification procedure to be used to establish the radio access bearer (RAB) assignment.

The command can be issued multiple times to configure either or both IEs for 'normal-modify' procedure.

The effect of adding the **no** prefix to the command depends on the keyword options included with the command:

- **no rab-modify-procedure normal-modify** disables a previously configured normal modify procedure and sets the configuration to use the default RAB Assignment modification procedure (**release-and-establish**).
- **no rab-modify-procedure normal-modify data-vol-report-ind-ie** changes the configuration to disable sending "Data Volume Reporting Indication IE" in the RAB Assignment request for modification. NOTE: This command does not change the use of the normal RAB modification procedure (**normal-modify**).
- **no rab-modify-procedure normal-modify pdp-type-info-ie** changes the configuration to disable sending "PDP Type Information IE" in the RAB Assignment request for modification. NOTE: This command does not change the use of the normal RAB modification procedure (**normal-modify**).

Use either of the following commands to verify the current configuration for type of RAB Assignment modification procedure, and if optional IEs are to be used:

- **show configuration verbose**
- **show iups-service**

### Example

Use the following command to enable 'normal-modify' as the modification procedure to be used for RAB Assignment:

```
rab-modify-procedure normal-modify
```

Use the following command to configure 'release-establish' as the modification procedure to be used by the SGSN for RAB Assignments:

**default rab-modify-procedure**

Use the following command to enable the "Data Volume Reporting Indication IE" as part of the normal modification request of the RAB Assignment Request procedure.

**rab-modify-procedure normal-modify data-vol-report-ind-ie**

# ranap arp-ie

This command enables or disables the inclusion of ARP-IE in RAB assignment / Relocation request RANAP messages per RNC.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure > context** *context_name* **> iups-service** *service_name* **> rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-iups-service-rnc)#`

**Syntax Description**

**ranap arp-ie**
**[ default | no ] ranap arp-ie**

**default**

Returns the configuration to the default setting, the inclusion of ARP-IE in RAB assignment / Relocation request RANAP messages is disabled.

**no**

Disables the inclusion of ARP-IE in RAB assignment / Relocation request RANAP messages per RNC.

# ranap bidirectional-always

Enables or disables sending of extended bitrates bi-directionally. When this command is enabled, the specified extended bitrates (MBR or GBR) are included bi-directionally (uplink and downlink directions) in the RAB Assignment Request even if the negotiated birate indicates that extended birates should be included in one direction.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure > context** *context_name* **> iups-service** *service_name* **> rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax Description**

```
ranap bidirectional-always ext-mbr-ie [ext-gbr-ie]
no ranap bidirectional-always
```

**no**

Disables sending of both extended MBR and GBR bi-directionally.

**ranap bidirectional-always ext-mbr-ie**

When this command is configured, if the maximum bitrate for either uplink or downlink directions indicates that extended bitrates should be included (that is, the maximum bitrate negotiated value exceeds "16"Mbps in either uplink or downlink direction), then the maximum bitrate extended IE is included in both uplink and downlink directions. If in one direction (uplink or downlink) the negotiated value does not exceed "16" Mbps then extended maximum bitrate is sent as "16000001".

**ext-gbr-ie**

Enables sending of Extended Guaranteed Bitrates IE.

**Usage Guidelines**

Configure this command to include the extended bitrates in both directions when it is present in one direction.

**Example**

Use the following command to include extended MBR bitrates bi-directionally in the RAB Assignment Request:

```
ranap bidirectional-always ext-mbr-ie
```

# ranap eutran-service-handover-ie

Enables/disables the inclusion of the E-UTRAN Service Handover Information Element in RAB Assignment Request messages (during the PDP activation phase) and Relocation Request RANAP messages (during the SRNS relocation phase). This ensures that an SRNS relocation handover to E-UTRAN is not allowed for E-UTRAN capable UEs that have only a UTRAN/GERAN roaming agreement in place.

**Product**

SGSN

**Privilege**

Administrator, Security Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure > context** *context_name* **> iups-service** *service_name* **> rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax Description**

```
ranap eutran-service-handover-ie
[ default | no ] ranap eutran-service-handover-ie
```

### ranap eutran-service-handover-ie

Enables the inclusion of the E-UTRAN Service Handover Information Element in RAB Assignment Request (during the PDP activation phase) and Relocation Request RANAP messages (during the SRNS relocation phase). The IE in the RAB Assignment Request during the PDP activation phase informs the RNC not to handover the subscriber to E-UTRAN. The IE in Relocation Request is sent when there is an intra- SGSN SRNS or inter-SGSN SRNS relocation within the UTRAN itself so that the target RNC knows that it shall not handover the subscriber to E-UTRAN.

### no ranap eutran-service-handover-ie

Specifies that the SGSN will not include the E-UTRAN Service Handover IE in RAB Assignment Request and Relocation Request RANAP messages.

### default

Returns the configuration to the default setting, The inclusion of the E-UTRAN Service Handover Information Element in RAB Assignment Request and Relocation Request RANAP messages is disabled.

### no

Disables the inclusion of the E-UTRAN Service Handover Information Element in RAB Assignment Request and Relocation Request RANAP messages is disabled.

## Usage Guidelines

Use this feature to prevent handovers to E-UTRAN in the following scenarios:

1. A UE is E-UTRAN capable, the PLMN is E-UTRAN capable, but the UE has not subscribed to EPS services (no 4G subscription available).
2. The VPLMN is E-UTRAN-capable, and the UE of an inbound roamer is E-UTRAN capable, but the UE has only a UTRAN/GERAN roaming agreement in place.

Enabling this parameter helps ensure that an SRNS relocation handover to E-UTRAN is not allowed for E-UTRAN capable UEs that have only a UTRAN/GERAN roaming agreement. This results in an elimination of potential service denial or disruption issues, and unnecessary signaling.

The following commands and features must be executed before enabling the **ranap eutran-service-handover-ie** setting:

- The SRNS relocation feature must be configured in *Call Control Profile Configuration Mode* via the **srns-inter** and/or **srns-intra** commands.
- The **eutran-not-allowed** flag must be enabled in the access-restriction-data command in *Call Control Profile Configuration Mode*.
- The call-control-profile must then be associated with an operator policy via the **associate** command in *Operator Policy Configuration Mode*.

### Example

This example enables the inclusion of the E-UTRAN Service Handover IE in RAB Assignment Request and Relocation Request RANAP messages.

```
ranap eutran-service-handover-ie
```

# ranap global-cn-id

This command configures the SGSN to use include the Global Core Network ID IE in the various messages.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure > context** *context_name* **> iups-service** *service_name* **> rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax Description**

**ranap global-cn-id { paging-request | relocation-request | reset-procedure | reset-resource-procedure } [ network-sharing selected-plmn ]**
**[ default | no ] ranap global-cn-id { paging-request | relocation-request }**

**default**

Returns the configuration to the default setting and sends the common-plmn in the Global CN ID IE.

**no**

Disables sending the Global CN ID IE.

**paging-request**

Instructs the SGSN to send the Global CN ID IE in the Paging Request message.

**relocation-request**

Instructs the SGSN to send the Global CN ID IE in the Relocation Request message.

**reset-procedure**

Instructs the SGSN to send the Global CN ID IE in the Reset/Ack message.

**reset-resource-procedure**

Instructs the SGSN to send the Global CN ID IE in the Reset-Resource/Ack message.

**network-sharing selected-plmn**

Instructs the SGSN to send the selected-plmn in the Global CN ID IE ***if*** network sharing has been enabled.

**Usage Guidelines**

Use this command to configure the SGSN to use 'selected-plmn' in the Global Core Network ID IE in various messages when network sharing is enabled.

### Example

Use the following command to include the global-cn-id IE in a Paging Request with the common PLMN when network sharing is enabled :

```
default ranap global-cn-id paging-request
```

Use the following command to include global-cn-id IE in Relocation Request with the selected-plmn (assumes network sharing has been enabled):

```
ranap global-cn-id relocation-request network-sharing selected-plmn
```

# ranap paging-area-id

This command configures the SGSN to use include the Paging Area ID IE in the Paging Request message.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure > context** *context_name* **> iups-service** *service_name* **> rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax Description**

```
ranap paging-area-id paging-request [ network-sharing selected-plmn ]
[ default | no ] ranap paging-area-id paging-request [ network-sharing
selected-plmn ]
```

#### default

Returns the configuration to the default setting and sends the common-plmn in the Paging Area ID IE.

#### no

Disables sending the Paging Area ID IE.

#### paging-request

Instructs the SGSN to send the Paging Area ID IE in the Paging Request message.

#### network-sharing selected-plmn

Instructs the SGSN to send the selected-plmn in the Paging Area ID IE ***if*** network sharing has been enabled.

**Usage Guidelines**

Use this command to configure the SGSN to use 'selected-plmn' in the Paging Area ID IE in the Paging Request message when network sharing is enabled.

### Example

Use the following command to include the paging-area-id IE in a Paging Request with the common PLMN when network sharing is enabled :

```
default ranap paging-area-id paging-request
```

Use the following command to include global-cn-id IE in Paging Request with the selected-plmn (assumes network sharing has been enabled):

```
ranap global-cn-id paging-request network-sharing selected-plmn
```

# ranap paging-cause-ie

This command sets the paging cause value and either includes or suppresses the Paging Cause IE in responses to Paging Requests due to various sources. This command is available in releases 8.1 and higher.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure** > **context** *context_name* > **iups-service** *service_name* > **rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax Description**

```
ranap { paging-cause-ie { all | background-data [ value ] |
conversational-data [ value ] | gmm-signalling [ value ] | gs-signalling [
 value ] | interactive-data [ value ] | mme-signalling [ value ] |
sm-signalling [ value ] | sms-signalling [ value ] | streaming-data [ value
 ] }
[ default | no ] ranap { paging-cause-ie { all | background-data |
conversational-data | gmm-signalling | gs-signalling | interactive-data
|  mme-signalling | sm-signalling | sms-signalling | streaming-data }
```

#### default

Resets the specific parameters value to default.

#### no

Suppresses the Paging Cause IE so that it is not included in responses to Paging Requests from respective sources.

#### all

Using **all** sets the action for the Paging Cause IE value for all paging due to all sources.

**background-data [ *value* ]**

Default: 3 (terminating background call)

Set the Paging Cause IE value for paging due to background data.

*value* : Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

**conversational-data [ *value* ]**

Default: 5 (terminating high priority signaling)

Set the Paging Cause IE value for paging due to conversational data.

*value* : Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

**gmm-signalling [ *value* ]**

Default: 5 (terminating high priority signaling)

Set the Paging Cause IE value for paging due to gmm-signaling.

*value* : Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

**gs-signalling [ *value* ]**

Default: 5 (terminating high priority signaling)

Set the Paging Cause IE value for paging due to VLR Paging Request.

*value* : Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

**interactive-data [ *value* ]**

Default: 2 (terminating interactive call)

Set the Paging Cause IE value for paging due to interactive data.

*value* : Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

**mme-signalling [ *value* ]**

Default: 5 (terminating high priority signaling)

Sets the Paging Cause IE value for paging from MME due to Circuit Switch Fallback (CSFB).

*value* : Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

**sm-signalling [ *value* ]**

Default: 5 (terminating high priority signaling)

Set the Paging Cause IE value for paging due to SM signaling.

*value* : Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

**sms-signalling [ *value* ]**

Default: 4 (terminating low priority signaling)

Set the Paging Cause IE value for paging due to SMS signaling.

*value* : Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

**streaming-data [ *value* ]**

Default: 5 (terminating high priority signaling)

Set the Paging Cause IE value for paging due to streaming data.

*value* : Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

**Usage Guidelines**

This command can be used to set the value (meaning) of the Paging Cause IE included in responses to Paging Requests or it can be used to suppress the inclusion of the Paging Cause IE in the responses. These actions can be configured for paging for all sources or for a specified source.

The following values are applicable to all Paging Cause IEs:

- **0** - Terminating conversational call
- **1** - Terminating streaming call
- **2** - Terminating interactive call
- **3** - Terminating background call
- **4** - Terminating low priority signaling
- **5** - Terminating high priority signaling

**Example**

Use the following command to set Paging Cause value to *3* for paging due to GMM signaling without affecting cause values for other sources:

```
ranap paging-cause-ie gmm-signalling 3
```

Use the following command to suppress the Paging Cause IE from all Paging Requests to the RNC:

```
no ranap paging-cause-ie all
```

Either of the following commands will cause the Paging Cause IE to be included in Paging Requests with the default value for SM signaling without affecting the cause for other sources:

```
ranap paging-cause-ie sm-signalling
default ranap paging-cause-ie sm-signalling
```

# ranap rab-arsp-ue-radio-lost

This command configures the Iu Release Command when SGSN receives the RAB Assignment Response with cause 46 "Radio Connection with UE Lost".

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure** > **context** *context_name* > **iups-service** *service_name* > **rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax Description**

**[ no ] ranap rab-arsp-ue-radio-lost**

**no**

When **no ranap rab-arsp-ue-radio-lost** is configured, SGSN will send the RAB Assignment Request with cause RAB Release to RNC.

**Usage Guidelines**

Use this command to enable or disable handling of the RAB Assignment Response with cause 46 "Radio Connection With UE Lost". SGSN sends the Iu Release Command with normal cause to RNC when it receives the RAB Assignment Response with cause 46.

This command is disabled by default.

**Note** This command applies to Gn-SGSN only.

# ranap rab-release-with-radiolost

This command configures the Iu Release Command when SGSN receives the RAB Release Request with cause 46 "Radio Connection with UE Lost".

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure** > **context** *context_name* > **iups-service** *service_name* > **rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax Description**

**[ no ] ranap rab-release-with-radiolost**

**no**

When **no ranap rab-release-with-radiolost** is configured, SGSN will send the RAB Assignment Request with cause RAB Release to RNC.

**Usage Guidelines**

Use this command to enable or disable handling of the RAB Release Request with cause 46 "Radio Connection With UE Lost". SGSN sends the Iu Release Command to RNC when it receives the RAB Release Request with cause 46.

This command is disabled by default.

**Note** This command applies to Gn-SGSN only.

# ranap rfsp-id-ie

Configure this command to enable or disable the inclusion of the Subscriber Profile ID for RAT/Frequency priority IE in RANAP Direct transfer Extension and Common Id. Extension messages.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure > context** *context_name* **> iups-service** *service_name* **> rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-iups-service-rnc)#`

**Syntax Description**

```
ranap rfsp-id-ie
no ranap rfsp-id-ie
```

**no**

Instructs the SGSN to exclude the Subscriber Profile ID for RAT/Frequency priority IE in RANAP Direct transfer Extension and Common Id Extension messages.

**rfsp-id-ie**

This keyword enables the Subscriber Profile ID for RAT/Frequency priority IE to be inserted in outbound RANAP Direct transfer Extension and Common Id Extension messages.

**Usage Guidelines**

Inclusion of RFSP ID IE is disabled by default in RANAP Direct transfer extension and Common ID Extension. Configure the keyword **rfsp-id-ie** to include Subscriber Profile ID for RAT/Frequency priority IE in RANAP Direct transfer Extension and Common Id Extension messages.

**Example**

Use the following command to include Subscriber Profile ID for RAT/Frequency priority IE in outbound RANAP Direct transfer Extension and Common Id Extension messages.

```
ranap rfsp-id-ie
```

# ranap signalling-indication-ie

This command enables/disables the inclusion of the Signaling Indication IE in either or both the RAB Assignment Request and/or the Relocation Request RANAP messages.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure > context** *context_name* **> iups-service** *service_name* **> rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax Description**

```
ranap signalling-indication-ie { rab-assignment-request [
relocation-request ] | relocation-request [ rab-assignment-request ] }
no ranap signalling-indication-ie
default ranap signalling-indication-ie
```

**no**

Sets the configuration so that the SGSN never includes the IE.

**default**

Resets the configuration to the default - the SGSN includes the IE in the messages if preconditions are met (see Usage section).

**rab-assignment-request | relocation-request**

Including one or both of these keywords configures what type of RANAP message will include the IE.

**Usage Guidelines** The command enables the operator to determine whether the signalling indication information element is included in either or both the RAB Assignment Request and Relocation Request messages during the PDP context setup procedure.

For this command configuration to work so that the IE is included, two preconditions must be met:

- Received QoS traffic class for the context must be interactive
- Received QoS has a signalling indication value as optimized

When an RNC receives this IE, the RNC assumes that the customer is using IMS signaling and allocates massive amounts of bandwidth, potentially causing cell congestion. This command enables the operator to determine the usage of this IE which provides the operator with additional session management control.

**Example**

Use the following command to include the signalling indication IE in the RAB Assignment Request:

```
ranap signalling-indication-ie rab-assignment-request
```

# ranap ue-ambr-ie

Enables the SGSN to include UE AMBR IE when sending RANAP messages.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure > context** *context_name* **> iups-service** *service_name* **> rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-iups-service-rnc)#`

**Syntax Description** **`[ no ] ranap ue-ambr-ie`**

**no**

Returns to the default functionality by disabling the sending of the UE AMBR IE.

**Usage Guidelines** This command allows the operator to determine if the UE AMBR IE is to be included when the SGSN sends RANAP messages of the type RAB Assignment Request and Relocation Request. This functionality can be enabled per RNC basis.

**Example**

If configuration for this functionality has been enabled, using the following command disables the sending of UE AMBR IE in RANAP messages.

**`no ranap ue-ambr-ie`**

# ran-information-management

Use this command to inform the SGSN which RNC are capable of handling RAN information management (RIM) messages.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure > context** *context_name* **> iups-service** *service_name* **> rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-iups-service-rnc)#`

**Syntax Description** **`[ default | no ] ran-information-management`**

**default**

Resets the default so RIM is disabled.

**no**

Disables the RIM support in the configuration file.

**Usage Guidelines**

By default, handling of RAN information management (RIM) messages is disabled. This command informs the SGSN which RNC are capable of handling RIM messages. This configuration only becomes 'operational' if the **ran-information-management** command is enabled in the SGSN global configuration mode.

When RIM support is enabled on both the SGSN and the destination node, then all RIM PDUs are forwarded to the BSC/RNC. If RIM message handling is not enabled on both nodes, then the RIM PDUs are dropped silently.

**Example**

Use the following command to enable RIM support:

```
ran-information-management
```

Use the following command to disable RIM support that has been added to the configuration:

```
no ran-information-management
```

# release-compliance

This command allows the SGSN to set support based on the RNC's 3GPP release compliance and to define per RNC QoS overrides.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure** > **context** *context_name* > **iups-service** *service_name* > **rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax Description**

**release-compliance { pre-release-7 | release-7 } [ gbr-down** *gbr_dn_val* **| gbr-up** *gbr_up_val* **| mbr-down** *mbr_dn_val* **| mbr-up** *mbr_up_val* **] +**
**default release-compliance**

**default**

Returns the configuration to the default value, **release-7**.

**pre-release-7**

Enables support for an RNC with capabilities compliant with releases prior to Release 7, such as HSPA in R6.

**release-7**

Enables support for RNC with capabilities compliant with 3GPP Release 7 or later, such as HSPA+ available in R7.

**gbr-down *gbr_dn_val***

Defines a guaranteed kbps bit rate for downlink direction,

- options for **pre-release-7** include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000. Default cap is 16000.
- options for **release-7** include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000, 21000, 28000, 42000. See default cap information below.

**gbr-up *gbr_up_val***

Defines a guaranteed kbps bit rate for uplink direction,

- options for **pre-release-7** include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000. Default cap is 16000.
- options for **release-7** include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000, 21000, 28000, 42000. See default cap information below.

**mbr-down *mbr_dn_val***

Defines a maximum kbps bit rate for downlink direction,

- options for **pre-release-7** include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000. Default cap is 16000.
- options for **release-7** include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000, 21000, 28000, 42000. See default cap information below.

**mbr-up *mbr_up_val***

Defines a maximum kbps bit rate for uplink direction,

- options for **pre-release-7** include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000. Default cap is 16000.
- options for **release-7** include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000, 21000, 28000, 42000. See default cap information below.

## Usage Guidelines

Use this command to match the 3GPP release support by the RNC. As the 3GPP releases each support differing data rate options - R6 supports HSPA and R7 supports HSPA+ - then selecting the compliance is a method of preforming data rate management on a per RNC basis.

Also use this command to set QoS capping overrides for each RNC separately. Default caps for Release 7 RNC will vary depending upon which overrides are set.

**Important** Once caps are set for an RNC, if the RNC release level changes the capping remains the same until the QoS override values are changed for that RNC. Values do not automatically change to the default values appropriate for that release .

### Example

Enable HSPA fallback to R6 compliance:

```
release-compliance pre-release-7
```

# reset-resource

This command enables the operator to control message length by configuring the number of IuConIDs sent in each RANAP Reset Resource messages.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

**configure > context** *context_name* **> iups-service** *service_name* **> rnc id** *rnc_id*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax Description**

```
reset-resource max-iuconid-per-msg number
default reset-resource max-iuconid-per-msg
```

#### default

Resets the number of Iu connection Ids included in the Reset Resource messages. Default is 250.

#### max-iuconid-per-msg *number*

Sets the number of Iu connection Ids to be included in the Reset Resource messages.

*number*: Integer from 1 to 250.

Default: 250

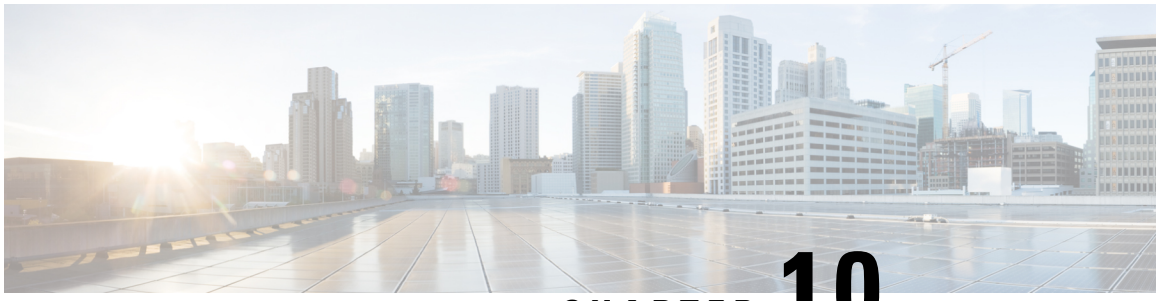
**Usage Guidelines**

Id numbers for each Iu connection are included in the RANAP Reset Resource messages. Including this potentially long stream of numbers can make the message very long. With this command, the operator can control the size of the messages by controlling the number of Id messages included in the messages.

### Example

Limit the number of Iu connection IDs to *30*:

```
reset-resource max-iuconid-per-msg 30
```



CHAPTER 10

# RoHC Profile Common Options Configuration Mode Commands

The RoHC Profile Common Options Configuration Mode is used to set timers that, upon expiration, release robust header compression contexts.

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Common Options Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-common)#`

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


- delay-release-hc-context-timer, on page 71
- do show, on page 72
- end, on page 73
- exit, on page 73
- inactive-traffic-release-hc-context-timer, on page 73


# delay-release-hc-context-timer

Sets a delay in releasing Robust Header Compression (RoHC) contexts allowing for context continuation during intra-gateway handoffs.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Common Options Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-common)#
```

**Syntax Description**

**delay-release-hc-context-timer** *seconds*
**no delay-release-hc-context-timer**

**no**

Removes previously configured value for this command. No value disables the feature.

***seconds***

Specifies the number of seconds the system delays before releasing the header compression context as an integer from 0 to 65535.

**Usage Guidelines**

Use this command to set a delay in releasing a header compression context. THis command is necessary when employing RoHC and mobility. Typically, when an RP connection is released, the header compression context is also released immediately. However, in mobility situations, such as intra-PDSN handoffs, the header compression context should be preserved. Adding a delay to cover the handoff time allows the context to be maintained.

A header compression context contains the compression/decompression configuration and statistics for the session.

**Example**

The following command sets the header compression release delay to 20 seconds:

```
delay-release-hc-context-timer 20
```

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**do show**

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# inactive-traffic-release-hc-context-timer

Sets an inactivity timer that is checked when inactivity is detected on an SO67 A10 bearer connection with negotiated RoHC parameters. When this timer expires, the header compression context is released.

**Product** HSGW

PDSN

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Common Options Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-common)#
```

## Syntax Description

**inactive-traffic-release-hc-context-timer** *seconds*
**no inactive-traffic-release-hc-context-timer**

### no

Removes previously configured value for this command. No value disables the feature.

### *seconds*

Specifies the time, in seconds, the system waits for activity on the bearer channel before releasing the header compression context as an integer from 1 through 65535.

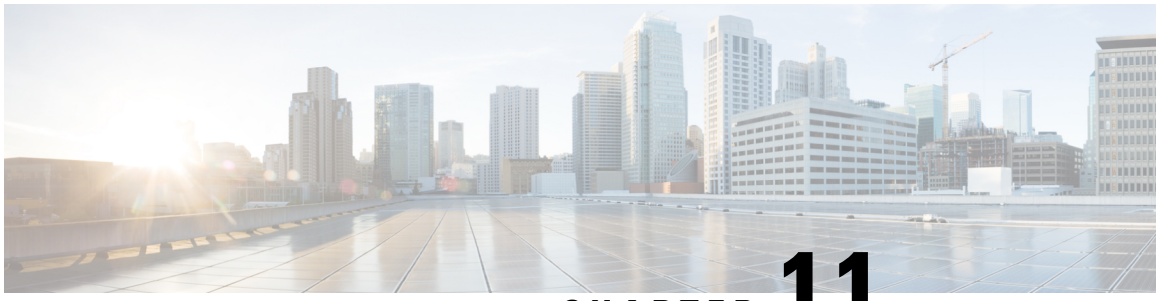
## Usage Guidelines

Use this command to set a timer that is started upon detecting inactivity on the bearer channel. Upon expiry, the header compression context is released. Enable this feature for more efficient memory utilization.

### Example

The following command sets the bearer channel inactivity timer to 60 seconds:

```
inactive-traffic-release-hc-context-timer 60
```



CHAPTER 11

# RoHC Profile Compression Configuration Mode Commands

The RoHC Profile Compression Configuration Mode is used to configure RoHC (Robust Header Compression) Compressor parameters. RoHC is not supported on GGSN.

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Important** The availability of commands, keywords and variables in this mode are dependent on platform type, product version, and installed license(s).


- context-timeout, on page 76
- do show, on page 77
- end, on page 77
- exit, on page 77
- ipid-history-size, on page 78
- max-jitter-cd, on page 78
- max-sliding-window, on page 79
- multiple-ts-stride, on page 80
- new-context-blocking-time, on page 80
- num-pkts-ts, on page 81
- num-pkts-u-mode, on page 82
- num-updates-ir, on page 83
- optimistic-repeats, on page 83
- rtp-sn-p, on page 84
- rtp-sn-p-override, on page 85
- rtp-time-stride, on page 86
- rtp-ts-deviation, on page 87
- rtp-ts-stride, on page 87
- sliding-window-ts, on page 88

- total-jitter-ipv4, on page 89
- total-jitter-ipv6, on page 90
- unimode-timeout-to-fo-state, on page 90
- unimode-timeout-to-ir-state, on page 91
- use-calculated-rtp-time-stride, on page 92
- use-calculated-rtp-ts-stride, on page 92
- use-ipid-override, on page 93
- use-optimized-talkspurt, on page 94
- use-optimized-transience, on page 95
- use-timer-based-compression, on page 95
- use-uncomp-profile, on page 96


# context-timeout

Context timeout in seconds.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Syntax Description**

**`context-timeout`** *`seconds`*
**`default context-timeout`**

**default**

Returns the command to its default value.

***seconds***

Specifies the context timeout value (in seconds) as an integer from 0 through 100.

Default: 20

**Usage Guidelines**

Use this command to set the context timeout.

**Example**

The following command sets the context timeout to 10 seconds:

**`context-timeout-period 10`**

# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `do show`

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `end`

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `exit`

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

# ipid-history-size

Specifies the number of IP-IDs of previously sent packets to store. An IP ID is a 16-bit header field that stores IPv4 Identification information.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Syntax Description**

**ipid-history-size** *number*
**default ipid-history-size**

**default**

Returns the command to its default value.

***number***

Specifies the number of IP IDs to store as an integer from 1 through 32.

Default: 8

**Usage Guidelines**

Use this command to set the number of IP IDs to store in the history.

**Example**

The following command sets the history size to 24 IP-IDs:

**ipid-history-size 24**

# max-jitter-cd

Specifies the upper boundary of jitter expected on the communication channel between the compressor and decompressor.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Syntax Description**

**max-jitter-cd** *num_ms*
**default max-jitter-cd**

**default**

Returns the command to its default value.

***num_ms***

Specifies the number of milliseconds for the maximum jitter setting as an integer from 0 through 999999999.

Default: 150

**Usage Guidelines**

Use this command to set the maximum amount of jitter allowed on the communication channel between compressor and decompressor.

**Example**

The following command sets the jitter limit to 1000 ms (1 second):

**max-jitter-cd 1000**

# max-sliding-window

Specifies the width of the sliding window for W-LSB (Windows-based Least Significant Bits) encoded values.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Syntax Description**

**max-sliding-window** *size*
**default max-sliding-window**

**default**

Returns the command to its default value.

***size***

Specifies the size of the sliding window as an integer from 1 through 1000.

Default: 6

**Usage Guidelines** Use this command to set the size of the sliding window used to compute jitter for W-LSB encoded values.

**Example**

The following command sets the sliding window size to 500:

```
max-sliding-window 500
```

# multiple-ts-stride

Enables or disables the use of repeated transmission of RTS_STRIDE for timer-based compression.

**Product** HSGW

PDSN

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-comp)#
```

**Syntax Description** **[ no ] multiple-ts-stride**

**no**

Disables the use of repeated transmission of RTS_STRIDE for time-based compression.

**Usage Guidelines** Use this command to enable or disable a gateway's ability to repeatedly transmit RTS_STRIDE for timer-based compression.

# new-context-blocking-time

Specifies the time period in seconds for blocking the establishment of new contexts after the compressor has received a feedback reject.

**Product** HSGW

PDSN

**Privilege** Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Syntax Description**

**new-context-blocking-time** *seconds*
**default context-timeout**

**default**

Returns the command to its default value.

***seconds***

Specifies the context blocking time (in seconds) as an integer from 0 through 100.

Default: 20

**Usage Guidelines**

Use this command to set the context blocking time after the compressor has received a feedback reject.

**Example**

The following command sets the context blocking time to 10 seconds:

```
new-context-blocking-time 10
```

# num-pkts-ts

Specifies the number packets per RTP timestamp (TS).

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Syntax Description**

**num-pkts-ts** *num_pkts*
**default num-pkts-ts**

**default**

Returns the command to its default value.

***num_pkts***

Specifies the number of packets for the timestamp as an integer from 0 through 999.

Default: 6

**Usage Guidelines**

Use this command to set the number of packets for each RTP timestamp (TS).

**Example**

The following command sets the number of packets per timestamp to 50:

```
num-pkts-ts 50
```

# num-pkts-u-mode

Specifies the number of packets sent when operating in U-Mode (unidirectional mode).

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-comp)#
```

**Syntax Description**

**num-pkts-u-mode** *num_pkts*
**default num-pkts-u-mode**

**default**

Returns the command to its default value.

***num_pkts***

Specifies the number of packets sent in U-Mode as an integer from 0 through 999.

Default: 1

**Usage Guidelines**

Use this command to set the number of packets sent when in U-Mode.

**Example**

The following command sets the number of packets for U-Mode to 50:

```
num-pkts-u-mode 50
```

# num-updates-ir

Configures the number of IR (Initiation and Refresh state) updates.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-comp)#
```

**Syntax Description**

**num-updates-ir** *num_pkts*
**default num-updates-ir**

**default**

Returns the command to its default value of 4.

***num_pkts***

Specifies the number of IR updates as an integer from 0 through 999.

Default: 4

**Usage Guidelines**

Use this command to set the number of IR updates.

**Example**

The following command sets the number of IR updates to 30:

```
num-updates-ir 30
```

# optimistic-repeats

Specifies the number of repeated packets to send to the decompressor. For transition from the FO (First Order) to the SO (Second Order) state, the compressor should be confident that the decompressor has all the parameters needed to decompress according to a fixed pattern.The compressor obtains its confidence about decompressor status by sending several packets with the same information according to the lower compression state. If the decompressor receives any of these packets, it is in sync with the compressor.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Syntax Description**

**optimistic-repeats** *num_pkts*
**default optimistic-repeats**

**default**

Returns the command to its default value.

***num_pkts***

Specifies the number of packets to repeat with the same information to assure synchronization with the decompressor.

*num_pkts* must be an integer from 0 through 10.

Default: 6

**Usage Guidelines**

Use this command to set the number of packets to repeat to the decompressor to assure synchronization before transition states.

**Example**

The following command sets the number of repeated packets to 5:

**optimistic-repeats 5**

# rtp-sn-p

Specifies the value of p in RTP SN (RTP Sequence Number) calculation. Least Significant Bits (LSB) encoding is used for header fields whose values are usually subject to small changes. With LSB encoding, the k least significant bits of the field value are transmitted instead of the original field value, where k is a positive integer. After receiving k bits, the decompressor derives the original value using a previously received value as reference (v_ref). The scheme is guaranteed to be correct if the compressor and the decompressor each use interpretation intervals as follows:

- In which the original value resides
- And in which the original value is the only value that has the exact same k least significant bits as those transmitted.

The interpretation interval can be described as a function:

f(v_ref, k). Let f(v_ref, k) = [v_ref - p, v_ref + (2^k - 1) - p]

Where p is an integer.

**Product**
HSGW
PDSN

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration
**configure > rohc-profile profile-name** *profile_name* **> compression-options**
Entering the above command sequence results in the following prompt:
`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Syntax Description**
**`rtp-sn-p`** *`p_value`*
**`default rtp-sn-p`**

**default**
Returns the command to its default value.

***p_value***
Specifies the value of p in the RTP SN calculation as an integer from 0 through 999.
Default: 6

**Usage Guidelines**
Use this command to set the value for p when performing the RTP SN calculation.

**Example**
The following command sets the value of p to 100:
**`rtp-sn-p 100`**

# rtp-sn-p-override

Enables an override of p in the RTP SN calculation. This is disabled by default.

**Product**
HSGW
PDSN

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration
**configure > rohc-profile profile-name** *profile_name* **> compression-options**
Entering the above command sequence results in the following prompt:
`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Syntax Description**
**`[ default | no ] rtp-sn-p-override`**

**default**

Returns the command to its default value of disabled.

**no**

Disables overriding p in RTP SN calculation.

**Usage Guidelines**

Use this command to enable an override of p in RTP SN calculation.

**Example**

The following command enables the override of p in the RTP SN calculation:

```
rtp-sn-p-override
```

# rtp-time-stride

Sets the time interval used for one TS (RTP Time Stamp) stride. This interval is used when timer-based encoding is enabled.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-comp)#
```

**Syntax Description**

**rtp-time-stride** *num_ms*
**default rtp-time-stride**

**default**

Returns the command to its default value.

***num_ms***

Specifies the number of milliseconds to use for TS_STRIDE as an integer from 0 through 999999999.

Default: 20

**Usage Guidelines**

Use this command to set the length of the TS_STRIDE in milliseconds.

**Example**

The following command sets TS_STRIDE to 100ms:

```
rtp-time-stride 100
```

# rtp-ts-deviation

Sets the maximum percentage of deviation allowed for input RTP packets for timer-based compression.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Syntax Description**

**rtp-ts-deviation** *percentage*
**default rtp-ts-deviation**

**default**

Returns the command to its default value of 25.

***percentage***

Specifies the maximum percentage of deviation allowed for input RTP packets for timer-based compression as an integer value from 0 through 100.

Default: 25

**Usage Guidelines**

Use this command to set the maximum percentage of deviation allowed for input RTP packets for timer-based compression.

**Example**

The following command sets the percentage to 30:

```
rtp-ts-deviation 30
```

# rtp-ts-stride

Specifies the amount by which TS (RTP time stamp) is incremented. This value is used for Scaled RTP TS encoding.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Syntax Description**

**rtp-ts-stride** *num_ms*
**default rtp-ts-stride**

**default**

Returns the command to its default value of 160.

***num_ms***

Specifies the number of milliseconds to use incrementing TS as an integer from 0 through 999999999.

Default: 160

**Usage Guidelines**

Use this command to set the amount by which TS is incremented for Scaled RTP TS encoding.

**Example**

The following command sets amount by which TS is incremented to 100ms:

**rtp-ts-stride 100**

# sliding-window-ts

Sets the sliding window used to compute jitter.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Syntax Description**

**sliding-window-ts** *size*
**default sliding-window-ts**

**default**

Returns the window to its default value of 4.

***size***

Specifies the size of the sliding window as an integer from 1 through 1000.

Default: 4

**Usage Guidelines** Use this command to set the size of the sliding window used to compute jitter for the current RoHC profile.

**Example**

The following command sets the sliding window size to 500:

```
sliding-window-ts 500
```

# total-jitter-ipv4

Specifies the total jitter allowed after compression for IPv4.

**Product** HSGW

PDSN

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-comp)#
```

**Syntax Description**

```
total-jitter-ipv4 time
default total-jitter-ipv4
```

**default**

Returns the command to its default value of 270.

***time***

Specifies the time interval to use (in milliseconds) as an integer from 0 through 999999999.

Default: 270

**Usage Guidelines** Use this command to set the jitter limit after compression.

**Example**

The following command sets the jitter after compression limit to 900 ms:

```
total-jitter-ipv4 900
```

# total-jitter-ipv6

Specifies the total jitter allowed after compression for IPv6.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Syntax Description**

**total-jitter-ipv6** *time*
**default total-jitter-ipv6**

**default**

Returns the command to its default value 580.

***time***

Specifies the total jitter interval allowed (in milliseconds) as an integer from 0 through 999999999.

Default: 580

**Usage Guidelines**

Use this command to set the jitter limit after compression.

**Example**

The following command sets the jitter after compression limit to 900 ms:

**total-jitter-ipv6 900**

# unimode-timeout-to-fo-state

Specifies the time period in seconds before falling back to the FO (First Order) state.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Syntax Description**

**unimode-timeout-to-fo-state** *num_ms*
**default unimode-timeout-to-fo-state**

**default**

Returns the command to its default value of 3.

***num_ms***

Specifies the timeout period (in seconds) as an integer from 0 through 10.

Default: 3

**Usage Guidelines**

Use this command to set the timeout before falling back to the FO state when in Unimode.

**Example**

The following command sets the fall back timeout to 2 seconds:

**unimode-timeout-to-fo-state 2**

# unimode-timeout-to-ir-state

Specifies the time period in seconds before falling back to the IR (Initiation and Refresh) state.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Syntax Description**

**unimode-timeout-to-ir-state** *num_ms*
**default unimode-timeout-to-ir-state**

**default**

Returns the command to its default value of 5.

***num_ms***

Specifies the timeout period in seconds as an integer from 0 through 20.

Default: 5

**Usage Guidelines** Use this command to set the timeout before falling back to the IR state when in Unimode.

### Example

The following command sets the fall back timeout to 3 seconds:

```
unimode-timeout-to-ir-state 3
```

# use-calculated-rtp-time-stride

Overrides the configured value of rtp-time-stride with a calculated value.

**Product** HSGW

PDSN

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-comp)#
```

**Syntax Description** **[ default | no ] use-calculated-rtp-time-stride**

### default

Returns the command to its default value of enabled.

### no

Disables the use of calculated RTP time stride override.

**Usage Guidelines** This command overrides the configured value of rtp-time-stride with a calculated value.

### Example

The following command overrides the configured value of rtp-time-stride.

```
use-calculated-rtp-time-stride
```

# use-calculated-rtp-ts-stride

Overrides the configured value of rtp-ts-stride with a calculated value.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Syntax Description**

**`[ default | no ] use-calculated-rtp-ts-stride`**

**default**

Returns the command to its default value of enabled.

**no**

Disables the use of calculated RTP TS time stride override.

**Usage Guidelines**

This command overrides the configured value of rtp-ts-stride with a calculated value.

**Example**

The following command overrides the configured value of rtp-ts-stride.

**`use-calculated-rtp-ts-stride`**

# use-ipid-override

Enables or disables overriding the IP-ID (IPv4 Identification header field).

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Syntax Description**

**`[ default | no ] use-ipid-override`**

**default**

Returns the command to its default value of disabled.

**no**

Disables the IP-ID override.

**Usage Guidelines** Use this command to enable overriding of the IP-ID.

**Example**

The following command enables the IP-ID override feature:

**use-ipid-override**

The following command disables the IP-ID override feature:

**no use-ipid-override**

The following command also disables the IP-ID override feature:

**default use-ipid-override**

# use-optimized-talkspurt

Enables or disables the use of optimized talkspurt.

**Product** HSGW

PDSN

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Syntax Description** **[ default | no ] use-optimized-talkspurt**

**default**

Returns the command to its default value of enabled.

**no**

Disables the use of optimized talkspurt.

**Usage Guidelines** Use this command to enable and disable the use of optimized talkspurt

**Example**

The following command enables the use of optimized talkspurt:

**use-optimized-talkspurt**

The following command disables the use of optimized talkspurt:

**no use-optimized-talkspurt**

# use-optimized-transience

Enables or disables the use of optimized transience.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Syntax Description**

**[ default | no ] use-optimized-transience**

**default**

Returns the command to its default value of enabled.

**no**

Disables the use of optimized transience.

**Usage Guidelines**

Use this command to enable or disable the use of optimized transience.

**Example**

The following command enables the use of optimized transience.

**use-optimized-transience**

The following command disables the use of optimized transience.

**no use-optimized-transience**

# use-timer-based-compression

Enables or disables timer-based compression of the RTP time stamp (TS) at the compressor.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Syntax Description**

**`[ default | no ] use-timer-based-compression`**

**default**

Returns the command to its default value of enabled.

**no**

Disables the use of timer-based compression.

**Usage Guidelines**

Use this command to enable or disable the use of timer-based compression.

**Example**

The following command enables the use of timer-based compression.

**`use-timer-based-compression`**

The following command disables the use of timer-based compression.

**`no use-timer-based-compression`**

# use-uncomp-profile

Enables or disables the use of the Uncompressed Profile (0x0000) if required at the compressor.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

**configure > rohc-profile profile-name** *profile_name* **> compression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Syntax Description**

**`[default | no ] useS-uncomp-profile`**

**default**

Returns the command to its default value of disabled.

**no**

Disables the use of the Uncompressed Profile.

## Usage Guidelines

Use this command to enable or disable the use of the Uncompressed Profile.

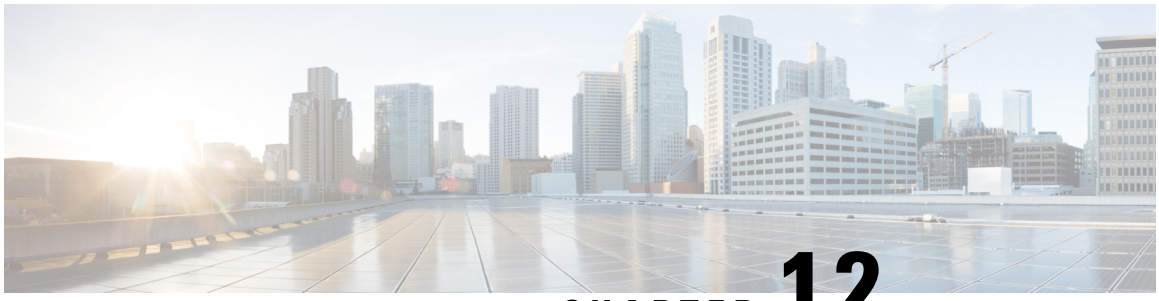
### Example

The following command enables the use of the Uncompressed Profile.

```
use-uncomp-profile
```

The following command disables the use of the Uncompressed Profile.

```
no use-uncomp-profile
```



CHAPTER 12

# RoHC Profile Configuration Mode Commands

The RoHC Profile Configuration Mode is used to configure RoHC (Robust Header Compression) Compressor and Decompressor parameters. The profiles can then be assigned to specific subscriber sessions when RoHC header compression is configured. RoHC is not supported on GGSN.

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration

**configure > rohc-profile profile-name** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name)#
```

**Important** The availability of commands, keywords and variables in this mode is dependent on platform type, product version, and installed license(s).


- common-options, on page 99
- compression-options, on page 100
- decompression-options, on page 101
- do show, on page 102
- end, on page 102
- exit, on page 102


# common-options

Enters the RoHC Profile Common Options Configuration Mode where inactivity and delay timers are set to support dynamic header compression contexts and context preservation during handoffs.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration

**configure > rohc-profile profile-name** *profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name)#`

**Syntax Description**

**`[ default ] common-options`**

**default**

Reset all parameters in the RoHC Profile Common Options Configuration Mode to default values.

**Usage Guidelines**

Use this command to enter the RoHC Profile Common Options Configuration Mode where parameters for maintaining header compression contexts and inactivity timers can be configured.

Entering this command results in the following prompt:

[*context_name*]*host*(config-rohcprofile-<*profile_name*>-common)#

RoHC Profile Common Options Configuration Mode commands are defined in the RoHC Profile Common Options Configuration Mode Commands chapter.

# compression-options

Enters the RoHC Profile Compression Options Configuration Mode allowing configuration of options applied during RoHC compression for the current RoHC profile.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration

**configure > rohc-profile profile-name** *profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name)#`

**Syntax Description**

**`[ default ] compression-options`**

**default**

Reset all options in the RoHC Profile Compression Configuration Mode to their default values.

**Usage Guidelines**

Use this command to enter RoHC Profile Compression Configuration Mode to set the compression options that are used for subscriber sessions using the current RoHC profile.

Entering this command results in the following prompt:

[*context_name*]*host*(config-rohcprofile-<*profile_name*>-comp)#

RoHC Profile Compression Options Configuration Mode commands are defined in the RoHC Profile Compression Configuration Mode Commands chapter.

### Example

The following command enters RoHC Profile Compression Options Configuration Mode:

**compression-options**

The following command sets all compression options to their default values:

**default compression-options**

# decompression-options

Enters the RoHC Profile Decompression Options Configuration Mode allowing configuration of options applied during RoHC decompression for the current RoHC profile.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration

**configure > rohc-profile profile-name** *profile_name*

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(config-rohcprofile-*profile_name*)#

**Syntax Description**

**[default ] decompression-options**

#### default

Reset all options in the RoHC Profile Decompression Options Configuration Mode to their default values.

**Usage Guidelines**

Use this command to enter RoHC Profile Decompression Options Configuration Mode to set the decompression options used for subscriber sessions using the current RoHC profile.

Entering this command results in the following prompt:

[*context_name*]*host*(config-rohcprofile-<*profile_name*>-decomp)#

RoHC Profile Decompression Options Configuration Mode commands are defined in the RoHC Profile Decompression Configuration Mode Commands chapter.

### Example

The following command enters RoHC Profile Decompression Options Configuration Mode:

**decompression-options**

The following command sets all decompression options to their default values:

**default decompression-options**

# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
end
```

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

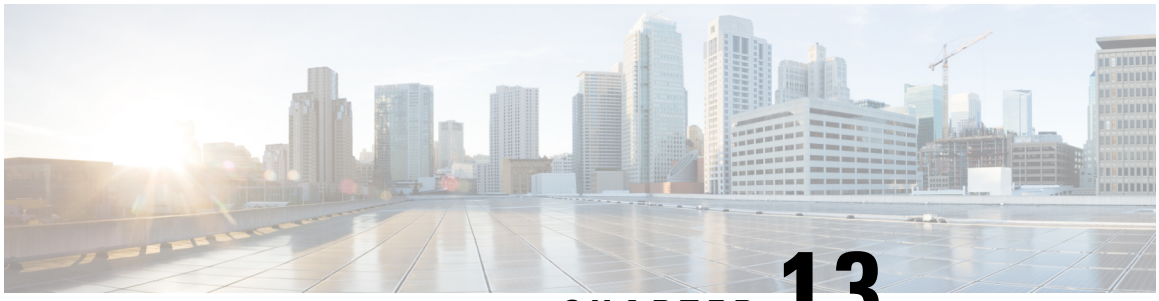
**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
exit
```

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



CHAPTER 13

# RoHC Profile Decompression Configuration Mode Commands

The RoHC Profile Decompression Configuration Mode is used to configure RoHC (Robust Header Compression) Decompressor parameters.

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-decomp)#`

**Important** The availability of commands, keywords and variables in this mode are dependent on platform type, product version, and installed license(s).


- accept-delayed-pkts, on page 104
- context-timeout, on page 104
- crc-errors-fo, on page 105
- crc-errors-so, on page 106
- do show, on page 107
- end, on page 108
- exit, on page 108
- max-jitter-cd, on page 108
- nack-limit, on page 109
- optimistic-mode-ack, on page 110
- optimistic-mode-ack-limit, on page 111
- piggyback-wait-time, on page 111
- preferred-feedback-mode, on page 112
- rtp-sn-p, on page 113
- rtp-sn-p-override, on page 114
- rtp-time-stride, on page 115
- rtp-ts-stride, on page 116
- sliding-window-ts, on page 116
- total-jitter-ipv4, on page 117

- total-jitter-ipv6, on page 118
- use-clock-option, on page 119
- use-crc-option, on page 119
- use-feedback, on page 120
- use-jitter-option, on page 121
- use-reject-option, on page 122
- use-sn-not-valid-option, on page 122
- use-sn-option, on page 123


# accept-delayed-pkts

Accepts delayed packets

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-decomp)#`

**Syntax Description**

**`[ default ] accept-delayed-pkts`**

**default**

Returns the command to its default value of disabled.

**Usage Guidelines**

This command helps reduce packet loss during context repair.

**Example**

Use the following command to enable the system to accept delayed packets:

**`accept-delayed-pkts`**

# context-timeout

Ensures that no expired contexts are used for data compression.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-decomp)#`

**Syntax Description**

**context-timeout** *seconds*
**default context-timeout**

**default**

Returns the command to its default value.

***seconds***

Specifies the context timeout value (in seconds) as an integer from 0 through 100.

Default: 20

**Usage Guidelines**

The RoHC stack should periodically clean up expired contexts and release memory in case there is no data activity for the call on this context. The context cleanup period is internally calculated to be set to half of the value of the context-timeout value. This will ensure that no expired contexts are used for data compression.

**Example**

The following command sets the context-timeout parameter to 30 seconds:

**context-timeout 30**

# crc-errors-fo

Sets the limits for when a NACK message is sent while in the FO (First Order) state. A NACK is sent whenever CRC errors are detected within a specified number of packets.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-decomp)#`

**Syntax Description**

**crc-errors-fo-k** *num_errors*
**crc-errors-fo-n** *num_packts*
**default crc-errors-fo-k**
**default crc-errors-fo-n**

**default**

Returns the command to its default value.

**crc-errors-fo-k *num_errors***

Specifies the number of received packets that trigger the sending of a NACK as an integer from 1 through 10.

Default: 1

**Important** *num_errors* must be less than or equal to the value specified with the **crc-errors-fo-n** command.

**crc-errors-fo-n *num_packts***

Specifies the number of packets to check for CRC errors as an integer from 1 through 10.

Default: 1

**Usage Guidelines** Use this command to set the parameters that trigger sending a NACK message when in the FO state.

**Example**

To configure a NACK to be sent when 4 out of the last 10 packets have CRC errors when in the FO state, use the following commands:

```
crc-errors-fo-k 4
crc-errors-fo-n 10
```

# crc-errors-so

Sets the limits for when a NACK message is sent while in the SO (Second Order) state. A NACK is sent whenever CRC errors are detected within a specified number of packets.

**Product** HSGW

PDSN

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-decomp)#
```

**Syntax Description**

```
crc-errors-so-k num_errors
crc-errors-so-n num_packets
```

```
default crc-errors-so-k
default crc-errors-so-n
```

**default**

Returns the command to its default value.

**crc-errors-so-k *num_errors***

Specifies the number of received packets that trigger the sending of a NACK as an integer from 0 through 10.

Default: 1

**Important** *num_errors* must be less than or equal to the value specified with the **crc-errors-so-n** command.

**crc-errors-so-n *num_packets***

Specifies the number of packets to check for CRC errors as an integer from 1 through 10.

Default: 1

**Usage Guidelines** Use this command to set the parameters that trigger sending a NACK message when in the SO state.

**Example**

To configure a NACK to be sent when 4 out of the last 10 packets have CRC errors when in the SO state, use the following commands:

```
crc-errors-so-k 4
crc-errors-so-n 10
```

# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# max-jitter-cd

Sets the upper boundary of jitter expected on the communication channel between the RoHC compressor and decompressor. The value is in milliseconds.

**Product** PDSN

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-decomp)#
```

**Syntax Description**

**max-jitter-cd** *no_ms*
**default max-jitter-cd**

**default**

Returns the command to its default value.

***no_ms***

Specifies the upper boundary jitter value (in milliseconds) as an integer from 0 through 999999999.

Default: 150

**Usage Guidelines**

Use this command to specify the maximum amount of jitter to expect on the channel between the RoHC compressor and decompressor.

**Example**

The following command sets the maximum jitter value to 100 ms:

**max-jitter-cd 100**

# nack-limit

Sets the number of unsuccessful decompressions allowed before a NACK is sent.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-decomp)#
```

**Syntax Description**

**nack-limit** *limit*
**default nack-limit**

**default**

Returns the command to its default value.

***limit***

Specifies the number of unsuccessful decompressions allowed as an integer from 0 through 20.

Default: 0

**Usage Guidelines** Use this command to set the maximum number of unsuccessful decompressions before a NACK message is sent.

### Example

The following command sets the number of unsuccessful decompressions allowed to 10:

```
nack-limit 10
```

# optimistic-mode-ack

When this command is enabled and a type 2 IR-DYN packet is successfully decompressed, an optional ACK is sent in U-mode.

**Product** HSGW

PDSN

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-decomp)#
```

**Syntax Description** **[ default | no ] optimistic-mode-ack**

### default

Returns the command to its default value of enabled.

### no

Disables the sending of the optional ACK.

**Usage Guidelines** Use this command to enable and disable the sending of an optional ACK in U-mode when a type 2 IR-DYN packet is successfully decompressed.

### Example

To enable the sending of the optional ACK, enter the following command:

```
optimistic-mode-ack
```

To disable the sending of the optional ACK, enter the following command:

```
no optimistic-mode-ack
```

# optimistic-mode-ack-limit

Sets the number of packets for which to send ACKs.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-decomp)#`

**Syntax Description**

**optimistic-mode-ack-limit** *num_pkts*
**default optimistic-mode-ack-limit**

**default**

Returns the command to its default value.

***num_pkts***

Specifies the number of packets for which to send ACKs as an integer from 0 through 20.

Default: 3

**Usage Guidelines**

Use this command to set the number of packets to send the optional ACK for when a type 2 IR-DYN packet is successfully decompressed.

**Example**

Enter the following command to set the number of packets to send and ACK for to 6:

**optimistic-mode-ack-limit 6**

Use the following command to set the number of packets to send an ACK for back to the default of 3:

**default optimistic-mode-ack-limit**

# piggyback-wait-time

Specifies the time in milliseconds to wait for a feedback packet to be picked up as piggybacked feedback by the associated compressor.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-decomp)#`

**Syntax Description**

**piggyback-wait-time** *m_secs*
**default piggyback-wait-time**

**default**

Returns the command to its default value.

***m_secs***

Specifies the time (in milliseconds) to wait for a feedback packet to be picked up as an integer value from 0 through 1000.

Default: 80

**Usage Guidelines**

Use this command to set the time in milliseconds to wait for a feedback packet to be picked up as piggybacked feedback by the associated compressor.

**Example**

The following command sets the wait time to 120 ms:

**piggyback-wait-time 120**

# preferred-feedback-mode

Specifies the preferred feedback mode to use between the compressor and the decompressor

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-decomp)#`

**Syntax Description**

**preferred-feedback-mode { bidirectional-optimistic | bidirectional-reliable | unidirectional }**
**default preferred-feedback-mode**

#### default

Returns the command to its default setting of bidirectional-optimistic.

#### bidirectional-optimistic

This mode is similar to the Unidirectional mode, with the exception of a feedback channel used to send error recovery requests from the decompressor to compressor.

This is the default mode.

#### bidirectional-reliable

Reliable mode makes extensive use of a feedback channel to avoid packet loss from context invalidation. A secure reference model is used instead of the optimistic approach used in the other modes. With the secure reference model, the confidence of the compressor depends on acknowledgements from the decompressor for every context updating packet.

Periodically the compressor sends context updating packets repeatedly until an acknowledgement is received from the decompressor.

#### unidirectional

Packets are sent in only one direction, from the compressor to the decompressor.

### Usage Guidelines

Use this command to specify the preferred feedback method to use between the compressor and the decompressor for the current RoHC profile.

#### Example

Use the following command to set the preferred feedback mode to bidirectional-reliable:

```
preferred-feedback-mode bidirectional-reliable
```

# rtp-sn-p

Specifies the value of p in RTP SN (RTP Sequence Number) calculation. Least Significant Bits (LSB) encoding is used for header fields whose values are usually subject to small changes. With LSB encoding, the k least significant bits of the field value are transmitted instead of the original field value, where k is a positive integer. After receiving k bits, the decompressor derives the original value using a previously received value as reference (v_ref). The scheme is guaranteed to be correct if the compressor and the decompressor each use interpretation intervals as follows:

- In which the original value resides
- And in which the original value is the only value that has the exact same k least significant bits as those transmitted.

The interpretation interval can be described as a function:

f(v_ref, k). Let f(v_ref, k) = [v_ref - p, v_ref + (2^k - 1) - p]

Where p is an integer.

**Product** HSGW

PDSN

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-decomp)#`

**Syntax Description** **`rtp-sn-p`** *`value`*
**`default rtp-sn-p`**

**default**

Returns the command to its default value.

***value***

Specifies the number the value of p in the RTP SN calculation as an integer from 0 through 999.

**Usage Guidelines** Use this command to set the value to use for p when performing the RTP SN calculation.

**Example**

The following command sets the RTP Sequence Number integer "p" value to 100:

**`rtp-sn-p 100`**

# rtp-sn-p-override

Allows an override of p in RTP SN calculation. This is disabled by default.

**Product** HSGW

PDSN

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-decomp)#`

**Syntax Description** **`[ default | no ] rtp-sn-p-override`**

**default**

Returns the command to its default value of disabled.

**no**

Disables overriding p in RTP SN calculation.

**Usage Guidelines**

Use this command to allow an override of p in RTP SN calculations.

**Example**

The following command enables the override of p in the RTP SN calculation:

```
rtp-sn-p-override
```

# rtp-time-stride

Sets the time interval used for one TS (RTP Time Stamp) stride. This value is used when timer-based encoding is enabled.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-decomp)#
```

**Syntax Description**

**rtp-time-stride** *time*
**default rtp-time-stride**

**default**

Returns the command to its default value of 20.

***time***

Specifies the time interval to use as an integer from 0 through 999999999.

Default: 20

**Usage Guidelines**

Use this command to set the time interval used for TS STRIDE when timer-based encoding is enabled.

**Example**

The following command sets the time interval to 1000:

```
rtp-time-stride 1000
```

# rtp-ts-stride

Amount by which TS (RTP time stamp) is incremented. This is used for Scaled RTP TS encoding.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-decomp)#`

**Syntax Description**

**rtp-ts-stride** *time*
**default rtp-ts-stride**

**default**

Returns the command to its default value of 160.

***time***

Specifies the time interval to use as an integer from 0 through 999999999.

Default: 160

**Usage Guidelines**

Use this command to set the amount by which TS is incremented.

**Example**

The following command sets the time increment to 1000:

```
rtp-ts-stride 1000
```

# sliding-window-ts

Computes jitter as described in RFC 3095,[4.5.4]

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-decomp)#`

**Syntax Description**

**`sliding-window-ts`** *`size`*
**`default sliding-window-ts`**

**default**

Returns the command to its default value of 4.

***size***

Sets the size of the sliding window. *size* must be an integer from 1 through 1000.

Default: 4

**Usage Guidelines**

Use this command to set the size of the sliding window used to compute jitter for the current RoHC profile.

**Example**

The following command sets the sliding window size to 500:

**`sliding-window-ts 500`**

# total-jitter-ipv4

Specifies the total jitter experienced after the decompression for IPV4.

**Product**

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-decomp)#`

**Syntax Description**

**`total-jitter-ipv4`** *`time`*
**`default total-jitter-ipv4`**

**default**

Returns the command to its default value of 270.

***time***

Specifies the time interval to use (in milliseconds) as an integer value from 0 through 999999999.

Default: 270

**Usage Guidelines** Use this command to set the jitter limit after decompression in ms.

**Example**

The following command sets the jitter after decompression limit to 900 ms:

```
total-jitter-ipv4 900
```

# total-jitter-ipv6

Specifies the total jitter experienced after the decompression for IPV6.

**Product** PDSN

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-decomp)#
```

**Syntax Description**

```
total-jitter-ipv6 time
default total-jitter-ipv6
```

**default**

Returns the command to its default value of 580.

***time***

Specifies the time interval to use (in milliseconds) as an integer from 0 through 999999999.

Default: 580

**Usage Guidelines** Use this command to set the jitter limit after decompression in ms.

**Example**

The following command sets the jitter after decompression limit to 900 ms:

```
total-jitter-ipv6 900
```

# use-clock-option

Controls usage of the RoHC clock option. The clock option informs the compressor of the clock resolution of the decompressor. This allows the compressor to estimate the jitter introduced by the clock of the decompressor when doing timer-based compression of the RTP timestamp.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-decomp)#`

**Syntax Description**

**`[ default | no ] use-clock-option`**

**default**

Returns the command to its default value of enabled.

**no**

Disables use of the RoHC clock option.

**Usage Guidelines**

Use this command to enable and disable the use of the RoHC clock option.

**Example**

The following command enables RoHC clock option usage:

**`use-clock-option`**

The following command disables RoHC clock option usage:

**`no use-clock-option`**

# use-crc-option

Controls usage of the RoHC cyclic redundancy check (CRC) option. The CRC option contains an 8-bit CRC computed over the entire feedback payload, without the packet type and code octet, but including any CID fields,

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-decomp)#`

**Syntax Description**

**`[ default | no ] use-crc-option`**

**default**

Returns the command to its default value of enabled.

**no**

Disables use of the CRC option.

**Usage Guidelines**

Use this command to enable and disable the use of the RoHC CRC option.

**Example**

The following command enables RoHC CRC option usage:

**`use-crc-option`**

The following command disables RoHC CRC option usage:

**`no use-crc-option`**

# use-feedback

Controls use of the feedback channel. A feedback channel sends error recovery requests and (optionally) acknowledgments of significant context updates from the decompressor to the compressor.

**Product**

HSGW

PDSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-decomp)#`

**Syntax Description**

**`[ default | no ] use-feedback`**

**default**

Returns the command to its default value of disabled.

**no**

Disables use of the feedback channel.

**Usage Guidelines** Use this command to enable and disable the use of the RoHC feedback channel.

**Example**

The following command enables RoHC feedback channel usage:

```
use-feedback
```

The following command disables RoHC feedback channel usage:

```
no use-feedback
```

# use-jitter-option

Controls usage of RoHC jitter option. The jitter option allows the decompressor to report the maximum jitter it has observed

**Product** HSGW

PDSN

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-decomp)#
```

**Syntax Description** **`[ default | no ] use-jitter-option`**

**default**

Returns the command to its default value of enabled.

**no**

Disables use of the jitter option.

**Usage Guidelines** Use this command to enable and disable the use of the RoHC jitter option.

**Example**

The following command enables RoHC jitter option usage:

**use-jitter-option**

The following command disables RoHC jitter option usage:

**no use-jitter-option**

# use-reject-option

Controls usage of RoHC reject option. The reject option informs the compressor that the decompressor does not have sufficient resources to handle the flow.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-decomp)#`

**Syntax Description**

**[ default | no ] use-reject-option**

**default**

Returns the command to its default value of disabled.

**no**

Disables use of the reject option.

**Usage Guidelines**

Use this command to enable and disable the use of the RoHC reject option.

**Example**

The following command enables RoHC reject option usage:

**use-reject-option**

The following command disables RoHC reject option usage:

**no use-reject-option**

# use-sn-not-valid-option

Controls usage of the RoHC SN not valid option. The sn-not-valid option indicates that the SN of the feedback is not valid. A compressor must not use the SN of the feedback to find the corresponding sent header when this option is present.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-decomp)#`

**Syntax Description**

**`[ default | no ] use-sn-not-valid-option`**

**default**

Returns the command to its default value of enabled.

**no**

Disables use of the sn-not-valid option.

**Usage Guidelines**

Use this command to enable and disable the use of the RoHC sn not valid option.

**Example**

The following command enables RoHC sn not valid option usage:

**`use-sn-not-valid-option`**

The following command disables RoHC sn not valid option usage:

**`no use-sn-not-valid-option`**

# use-sn-option

Controls usage of RoHC sn option. The sn option provides eight additional bits of SN (Sequence Number, usually the RTP Sequence Number.)

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > RoHC Profile Configuration >

**configure > rohc-profile profile-name** *profile_name* **> decompression-options**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-decomp)#`

## Syntax Description

```
[ default | no ] use-sn-option
```

### default

Returns the command to its default value of enabled.

### no

Disables use of the SN option.

## Usage Guidelines

Use this command to enable and disable the use of the RoHC SN option.

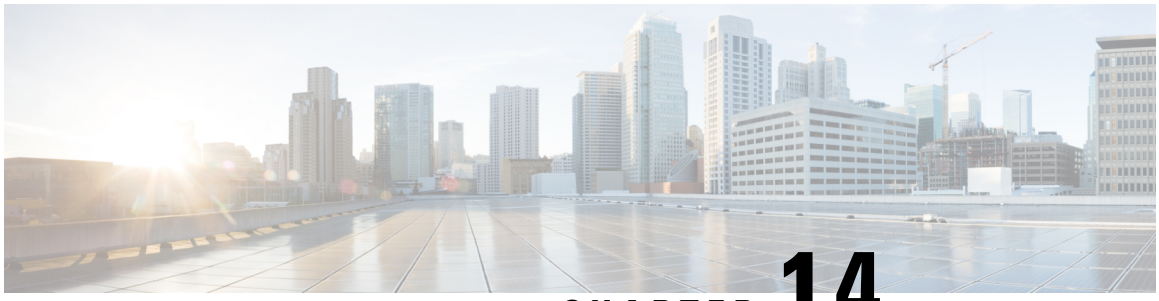
### Example

The following command enables RoHC SN option usage:

```
use-sn-option
```

The following command disables RoHC SN option usage:

```
no use-sn-option
```



CHAPTER 14

# Route-map Configuration Mode Commands

The Route-Map Configuration sub-mode is used for the OSPFv2 and BGP-4 routing protocols. This mode includes commands that configure matching rules and set actions to perform on matched routes.

**Command Modes**

Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure > context** *context_name* **> route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-route-map)#`

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


- do show, on page 126
- end, on page 126
- exit, on page 126
- match as-path, on page 127
- match community, on page 127
- match extcommunity, on page 128
- match interface, on page 129
- match ip address, on page 130
- match ip next-hop, on page 131
- match ipv6 address, on page 131
- match ipv6 next-hop, on page 132
- match metric, on page 133
- match origin, on page 134
- match route-type external, on page 135
- match tag, on page 135
- set as-path, on page 136
- set community, on page 137
- set extcommunity rt, on page 138
- set ip next-hop, on page 139
- set ipv6 next-hop, on page 139
- set local-preference, on page 140

- set metric, on page 141
- set metric-type, on page 142
- set origin, on page 142
- set tag, on page 143
- set weight, on page 144


# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character | is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
end
```

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `exit`

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

# match as-path

Matches an Autonomous System (AS) path access list

**Product** HA

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure > context** *context_name* **> route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-route-map)#`

**Syntax Description** **`[ no ] match as-path`** *`AS_list`*

**no**

Disables matching the specified AS path access list.

***AS_list***

Specifies the name of an AS path access list for matching as an alphanumeric string of 1 through 79 characters.

**Usage Guidelines** This command is used for BGP-4 routing to specify an AS path access list to be matched. Refer to the **ip as-path access-list** command for more information.

**Example**

To match entries in an AS path access list named *ASlist1*, enter the following command;

**`match as-path ASlist1`**

# match community

Configures filtering (permit or deny) via a BGP community-list in a route map.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure** > **context** *context_name* > **route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-route-map)#
```

**Syntax Description**

**[no] match community { named** *named_list* **| standard** *identifier* **}**

**no**

Disables matching the specified community list.

**named *named_list***

Specifies the name of a community list as an alphanumeric string of 1 through 79 characters.

**standard *identifier***

Specifies the name of a community list as an integer from 1 through 99.

**Usage Guidelines**

Configures filtering (permit or deny) via a BGP community-list in a route map.

The community list must have been previously configured via the Context Configuration mode **ip community-list** command.

**Example**

This command matches community-list number 2:

```
match community standard 2
```

# match extcommunity

Configures filtering (permit or deny) via a BGP external community-list in a route map. An external community-list is a Route Target.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure** > **context** *context_name* > **route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-route-map)#
```

**Syntax Description**

**[no] match extcommunity { named** *named_list* **| standard** *identifier* **}**

**no**

Disables matching the specified external community list.

**named *named_list***

Specifies the name of an external community list as an alphanumeric string of 1 through 79 characters.

**standard *identifier***

Specifies the name of an external community list as an integer from 1 through 99.

**Usage Guidelines**

Configures filtering (permit or deny) via a BGP external community-list in a route map. An external community-list is a Route Target.

A BGP extended community defines a route target. MPLS VPNs use a 64-bit Extended Community attribute called a Route Target (RT). An RT enables distribution of reachability information to the correct information table.

The external community list must have been previously configured via the Context Configuration mode **ip extcommunity-list** command.

**Example**

This command matches external community-list number 99:

```
match extcommunity standard 99
```

# match interface

Specifies the next-hop interface name of a route to be matched.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure > context** *context_name* **> route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-route-map)#
```

**Syntax Description**

**[ no ] match interface** *interface_name*

**no**

Disables matching the specified interface name.

***interface_name***

Specifies the name of the virtual interface for matching as an alphanumeric string of 1 through 79 characters.

**Usage Guidelines**

Use this command to specify the next hop interface name for routes to be matched.

### Example

To match routes that have the next hop interface specified as *Interface123*, enter the following command:

```
match interface Interface123
```

# match ip address

Matches IPv4 routes with entries in a route-access-list or prefix-list.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure > context** *context_name* **> route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-route-map)#
```

**Syntax Description**

**[ no ] match ip address { prefix-list | route-access-list }** *list_name*

#### no

Disables matching from the specified prefix list or route access list.

#### prefix-list

Matches any routes with entries in a prefix-list.

#### route-access-list

Matches any routes with entries in a route-access-list.

#### *list_name*

Specifies the name of the IPv4 prefix list or IPv4 route access-list as an alphanumeric string of 1 through 79 characters.

**Usage Guidelines**

Use this command to match routes specified in an IPV4 route-access-list or prefix-list.

### Example

To match routes that are specified in an IPv4 prefix list named *Prefix100*, enter the following command:

```
match ip address prefix-list Prefix100
```

# match ip next-hop

Matches next-hop IPv4 addresses with entries in a speicifed prefix-list or route-access-list.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure > context** *context_name* **> route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-route-map)#`

**Syntax Description**

**`[ no ] match ip next-hop { prefix-list | route-access-list }`** *`list_name`*

**no**

Disables matching from the specified prefix list or route access list.

**prefix-list**

Matches any routes that have a next-hop router IPv4 address that has an entry in the specified prefix list.

**route-access-list**

Matches any routes that have a next-hop router IPv4 address that has an entry in the specified route-access-list.

***list_name***

Specifies the name of the prefix-list or route-access-list as an alphanumeric string of 1 through 79 characters.

**Usage Guidelines**

Use this command to match next-hop IPv4 addresses that have entries in the specified prefix-list or route-access-list.

**Example**

To match next-hop IPv4 addresses with entries in a prefix-list named *Prefix100*, enter the following command:

```
match ip next-hop prefix-list Prefix100
```

# match ipv6 address

Matches IPv6 routes with entries in a specified route-access-list or prefix-list.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure > context** *context_name* **> route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-route-map)#`

**Syntax Description**

**`[ no ] match ipv6 address { prefix-list | route-access-list }`** *`list_name`*

**no**

Disables matching from the specified prefix list or route access list.

**prefix-list**

Matches any routes with entries in a prefix-list.

**route-access-list**

Matches any routes with entries in a route-access-list.

***list_name***

Specifies the name of the IPv6 prefix list or IPv6 route access-list as an alphanumeric string of 1 through 79 characters.

**Usage Guidelines**

Matches IPv6 routes with entries in a specified route-access-list or prefix-list.

**Example**

To match routes that are specified in an IPv6 prefix list named *Prefix600*, enter the following command:

```
match ipv6 address prefix-list Prefix600
```

# match ipv6 next-hop

Matches next-hop IPv6 addresses with entries in specified standard prefix-list or route-access-list.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure > context** *context_name* **> route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-route-map)#`

**Syntax Description** **`[ no ] match ipv6 next-hop { prefix-list | route-access-list }`** *`list_name`*

**no**

Disables matching from the specified prefix list or route access list.

**prefix-list**

Matches any routes that have a next-hop router IPv6 address that has an entry in the specified prefix list.

**route-access-list**

Matches any routes that have a next-hop router IPv6 address that has an entry in the specified route-access-list.

***list_name***

Specifies the name of the prefix-list or route-access-list as an alphanumeric string of 1 through 79 characters.

**Usage Guidelines** Use this command to match next-hop IPv6 addresses that have entries in the specified prefix-list or route-access-list.

**Example**

To match next-hop IPv6 addresses with entries in a prefix-list named *Prefix600*, enter the following command:

```
match ipv6 next-hop prefix-list Prefix600
```

# match metric

Matches routes that have the specified route metric.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure > context** *context_name* **> route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-route-map)#
```

**Syntax Description** **`[ no ] match metric`** *`metric_value`*

**no**

Disables matching of the specified route metric.

***metric_value***

Specifies the route metric to match as an integer from 0 through 4294967295.

**Usage Guidelines** Use this command to match routes that have the specified route metric.

### Example

To match routes with the route metric of 1200, enter the following command:

```
match metric 1200
```

# match origin

Matches the origin code learned from BGP. This command is for route maps that are used with BGP routing only.

**Product** HA

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure > context** *context_name* **> route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-route-map)#
```

**Syntax Description** **[ no ] match origin { egp | igp | incomplete }**

### no

Disables matching of the origin code.

### egp

Matches origins learned via the External Gateway Protocol (EGP)

### igp

Match origins learned via the local Interior Glittery Protocol (IGP)

### incomplete

Match origins with unknown heritage.

**Usage Guidelines** Use this command to match origin codes for BGP routing.

### Example

To match origin codes learned from EGP, enter the following command:

```
match origin egp
```

# match route-type external

Match external Open Shortest Path First (OSPF) routes of the specified type.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure > context** *context_name* **> route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-route-map)#`

**Syntax Description**

**`[ no ] match route-type external { type-1 | type-2 }`**

**no**

Disables matching with external OSPF routes of the specified type.

**type-1**

Only matches type-1 external routes.

**type-2**

Only matches type-2 external routes.

**Usage Guidelines**

Use this command to match external routes of a specific type.

**Example**

The following command matches all external routes that are type-2:

**`match route-type external type-2`**

# match tag

Matches routes with the specified route tag value.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure > context** *context_name* **> route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-route-map)#
```

**Syntax Description**

**[ no ] match tag** *tag_value*

**no**

Disables matching routes with the specified route tag value.

***tag_value***

Specifies the route tag value to match as an integer from 0 through 4294967295.

**Usage Guidelines**

Use this command to match routes that have the specified route tag value.

**Example**

Use the following command match routes that have a route tag value of 1234:

```
match tag 1234
```

# set as-path

Modifies an Autonomous System (AS) path for a route by adding the specified AS numbers to the front of the path.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure > context** *context_name* **> route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-route-map)#
```

**Syntax Description**

**[ no ] set as-path prepend** *asn***+**

**no**

Disables prepending the AS path. Any previously set prepends are removed.

**prepend**

Prepends the AS path.

***asn***

AS number(s) to be prepended to the AS path. You can specify up to 16 different AS numbers to be prepended in the order specified. Each AS number must be separated by a space. *asn* must be an integer from 1 through 65535.

**Usage Guidelines** Use this command to add up to 16 specified AS numbers to the front of the AS path.

### Example

The following command prepends the AS numbers 100, 200, and 1000 to matching AS paths:

```
set as-path prepend 100 200 1000
```

# set community

Sets the BGP community destination for the routes matching the route-map.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure > context** *context_name* **> route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-route-map)#
```

**Syntax Description**

```
set community [additive] { internet | local-AS | no-advertise | no-export
 | none | value AS-community_number AS-community_number AS-community_number+ }
{ internet | local-AS | no-advertise | no-export | none | value
AS-community_number AS-community_number AS-community_number ...  }
{ internet | local-AS | no-advertise | no-export | none | value
AS-community_number AS-community_number AS-community_number ... }
no set community { internet | local-AS | no-advertise | no-export | value
 AS-community_number  }
```

### no

Unsets the specified community destination.

### [additive]

When enabled this option allows multiple BGP destinations and route targets to be included in the same community.

### { internet | local-AS | no-advertise | no-export | value *AS-community_number*

Specifies the destination for the community.

- **internet** – Advertise this route to the internet community, and any router that belongs to it.
- **local-AS** – Use in confederation scenarios to prevent sending packets outside the local autonomous system (AS).
- **no-advertise** – Do not advertise this route to any BGP peer, internal or external.
- **no-export** – Do not advertise to external BGP (eBGP) peers. Keep this route within an AS.
- **none** – No community attribute

- **value** *AS-community_number* – Specifies a community string in AS:NN format, where AS = 2-byte AS-community hexadecimal number and NN = 2-byte hexadecimal number (1 to 11 characters).

You can enter multiple destinations and route targets separated by spaces.

**Usage Guidelines**

Sets the BGP community destinations for the routes matching the route-map.

The community list must have been previously configured via the Context Configuration mode **ip community-list** command.

#### Example

The following command sets the BGP community destination to AS 400:50:

```
set community value 400:50
```

# set extcommunity rt

Sets the BGP external community destination for the routes matching the route-map. The external community is the Route Target (RT).

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure > context** *context_name* **> route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-route-map)#
```

**Syntax Description**

**set extcommunity rt** *rt_number rt_number rt_number*+
**no set extcommunity rt***rt_number* **+**

#### no

Unsets the specified BGP external community (Route Target).

#### *rt_number*

Specifies a Route Target as a string in AS:NN format, where AS = 2-byte AS-community hexadecimal number and NN = 2-byte hexadecimal number (1 to 11 characters). You can enter multiple route targets separated by spaces.

**Usage Guidelines**

Sets the BGP external community destinations (route targets) for the routes matching the route-map.

The external community list must have been previously configured via the Context Configuration mode **ip extcommunity-list** command.

### Example

The following command sets the BGP route target to AS 212:34:

```
set extcommunity rt 212:34
```

# set ip next-hop

Sets the IPv4 address that is applied as the next hop for routes.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure** > **context** *context_name* > **route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-route-map)#
```

**Syntax Description**

**[ no ] set ip next-hop** *ipv4_address*

#### no

Disables the specified next hop IPv4 address.

#### *ipv4_address*

Specifies the IPv4 address of the next hop to which packets are output, entered using IPv4 dotted-decimal notation.

**Usage Guidelines**

Use this command to set the IPv4 address that is used as the next hop for routes.

### Example

To set the next hop for routes to the IPv4 address 209.165.200.234, use the following command:

```
set ip next-hop 209.165.200.234
```

# set ipv6 next-hop

Sets the IPv6 address that is applied as the next hop for routes.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure > context** *context_name* **> route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-route-map)#`

**Syntax Description**

**`[ no ] set ipv6 next-hop`** *`ipv6_address`*

**no**

Disables the specified next hop address.

***ipv6_address***

Specifies the IPv6 address of the next hop to which packets are output, entered using IPv6 colon-separated-hexadecimal notation.

**Usage Guidelines**

Use this command to set the IPv6 address that is used as the next hop for routes.

**Example**

To set the next hop for routes to the IPv6 address 2001:4A2B::1f3F, use the following command:

```
set ipv6 next-hop 2001:4A2B::1f3F
```

# set local-preference

Sets the BGP local preference attribute that is sent by the BGP speaker only to IBGP peers.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure > context** *context_name* **> route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-route-map)#`

**Syntax Description**

**`[ no ] set local-preference`** *`pref_number`*

**no**

Disables the specified local preference.

***pref_number***

Specifies the BGP local preference number as an integer from 1 through 16777214.

**Usage Guidelines**

Sets the BGP local preference attribute that is sent by the BGP speaker only to IBGP peers. This value can be used by peers to determine the exit point of the Autonomous System (AS).

There is no **match** clause corresponding to local preference in the route-map because local-preference is directly used in the route selection algorithm.

### Example

The following command sets the BGP local preference attribute to 33:

```
set local-preference 33
```

# set metric

Sets the route metric for matching routes to a specified value.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure > context** *context_name* **> route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-route-map)#
```

**Syntax Description**

**[ no ] set metric** *metric_value*

### no

Disables the specified metric type.

### *metric_value*

Specifies the metric value that is set for routes as an integer from 1 through 16777214.

**Usage Guidelines**

Use this command to set the route metric for matched routes.

**Note** BGP needs to be restarted to update the configured value.

### Example

To set the route metric to 12345, use the following command:

```
set metric 12345
```

# set metric-type

This command sets the route metric type to either Type-1 or Type-2 in the AS-external-LSA.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure > context** *context_name* **> route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-route-map)#`

**Syntax Description**

**`[ no ] set metric-type { type-1 | type-2 }`**

**type-1**

Sets the route metric to external type-1.

**type-2**

Sets the route metric to external type-2

**Usage Guidelines**

Use this command to set the route metric to either external type-1 or external type-2.

**Example**

To set the route metric to type-1, enter the following command:

**`set metric-type type-1`**

# set origin

Sets the Border Gateway Protocol (BGP) origin code to a specified value. This command is for route maps that are used with BGP routing only.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure > context** *context_name* **> route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-route-map)#`

**Syntax Description**

**`[ no ] set origin { egp | igp | incomplete }`**

**no**

Disables setting the origin code.

**egp**

Sets the origin code to specify that the path is from a remote External Gateway Protocol (EGP) system.

**igp**

Sets the origin code to specify that the path is from a local Interior Gateway Protocol (IGP) system.

**incomplete**

Sets the origin code to specify that the path is from an unknown system.

**Usage Guidelines**

Use this command to set a specified origin code for BGP.

**Example**

To set the origin code to be from an External Gateway Protocol (EGP) system, enter the following command:

```
set origin egp
```

# set tag

Sets the route tag value for matched routes.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure > context** *context_name* **> route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-route-map)#
```

**Syntax Description**

**[ no ] set tag** *tag_value*

**no**

Disables setting the route tag to the specified value.

***tag_value***

Specifies the route tag value as an integer from 0 through 4294967295.

**Usage Guidelines**

Use this command to set the route tag value that is applied to all matched routes.

### Example

To set the route tag value to 12345, enter the following command:

```
set tag 12345
```

# set weight

Sets the weight in the routing table for matching routes to the specified value.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Route-map Configuration

**configure > context** *context_name* **> route-map** *map_name* **{ deny | permit }** *seq_number*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-route-map)#
```

**Syntax Description**

**[ no ] set weight** *value*

**no**

Disables setting the routing weight value.

***value***

Specifies the weight in the routing table as an integer from 1 through 4294967295.

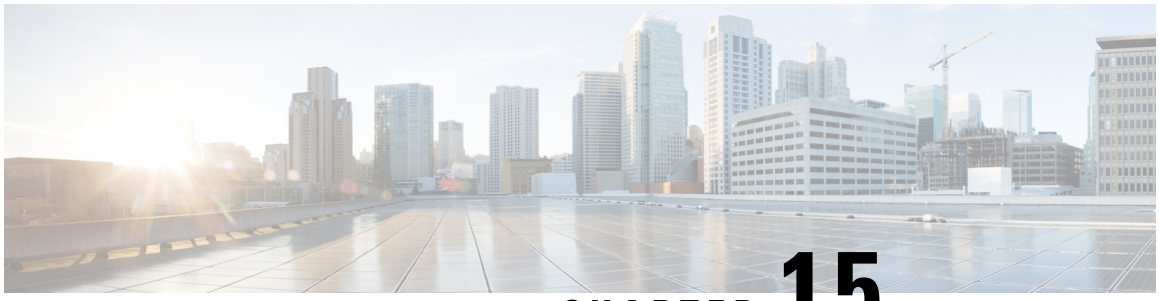
**Usage Guidelines**

Use this command to set the routing table weight on matched routes.

### Example

The following command sets the routing table weight for matched routes to 1000:

```
set weight 1000
```



CHAPTER 15

# RS-232 Port Configuration Mode Commands

The RS-232 Port Configuration Mode is used to manage the RS-232 ports on the SPIO cards.

**Command Modes**

Exec > Global Configuration > RS-232 Port Configuration

**configure > port rs232** *slot_number/port_number*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-port-`*`slot_number/port_number`*`)#`

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


- do show, on page 145
- end, on page 146
- exit, on page 146
- preferred slot, on page 146
- snmp trap link-status, on page 147
- terminal, on page 148


# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
end
```

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
exit
```

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

# preferred slot

Assigns revertive or non-revertive control to port redundancy auto-recovery.

Default: non-revertive operation

**Product** PDSN

FA

HA

GGSN

**Privilege** Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > RS-232 Port Configuration

**configure > port rs232** *slot_number/port_number*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-port-slot_number/port_number)#`

**Syntax Description**

**`[ default | no ] preferred slot`** *`slot_number`*

**default**

Sets the port for non-revertive operation for port redundancy auto-recovery; requiring an administrative user to manually issue a **port switch to** command to return service to the original port.

**no**

Disables revertive, or auto-recovery, operation for selected port.

***slot_number***

Identifies the physical chassis slot where the SPIO card is installed.

**Usage Guidelines**

This command enables or disables revertive port redundancy, wherein after a port failover, when the original port is restored to service (such as link up) the system will return service to that port automatically.

Disabled, which is the default setting, causes non-revertive operation; requiring an administrative user to manually issue a port switch to command to return service to the original port.

This command must be issued on a per port basis, allowing you to configure specific ports to be used on individual line cards or SPIO cards. For example, ports 1 through 4 could be configured as "preferred" on the line card in slot 17, while ports 5 through 8 are "preferred" on the line card in slot 33. In this scenario, both line cards would be in an Active operational state while still providing LC and port redundancy for the other.



**Important** This command is not supported on all platforms.

**Example**

The following command sets the preferred slot to 24:

**`preferred slot 24`**

# snmp trap link-status

Enables or disables the generation of an SNMP trap for link status changes.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > RS-232 Port Configuration

**configure > port rs232** *slot_number/port_number*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-port-slot_number/port_number)#`

**Syntax Description**

**`[ no ] snmp trap link-status`**

**no**

Disables the sending of traps for link status changes.

**Usage Guidelines**

Enable link status change traps when a monitoring facility can use the information or if there are trouble shooting activities are in progress.

**Example**

The following command enables link status change traps:

**`snmp trap link-status`**

# terminal

Configures the console port on the SPIO.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > RS-232 Port Configuration

**configure > port rs232** *slot_number/port_number*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-port-slot_number/port_number)#`

**Syntax Description**

**`terminal { carrierdetect { off | on } | databits { 7 | 8 } | flowcontrol { hardware | none } | parity { even | none | odd } | speed { 115200 | 19200 | 38400 | 57600 | 9600 } | stopbits { 1 | 2 } }`**
**`default terminal { all | databits | flowcontrol | parity | speed | stopbits }`**

**carrierdetect { off | on }**

Specifies whether or not the console port is to use carrier detect when connecting to a terminal.

**databits { 7 | 8 }**

Specifies the number of data bits used to transmit and receive characters. Default: 8

**default terminal all**

Restores all settings to their default values.

**flowcontrol { hardware | none }**

Specifies how the flow of data is controlled between the SPIO and a terminal. Default: none

**parity { even | none | odd }**

Specifies the type of error checking used on the port.

**even**: Enables error checking by setting the parity bit to 1 (if needed) making the number of 1s in the data bits even.

**none**: Disables error checking. This is the default setting.

**odd**: Enables error checking by setting the parity bit to 1 (if needed) making the number of 1s in the data bits odd.

**speed { 115200 | 19200 | 38400 | 57600 | 9600 }**

Specifies the flow of data in bits per second between the console port and terminal. Default: 9600

**stopbits { 1 | 2 }**

Specifies the number of stop bits between each transmitted character. Default: 1

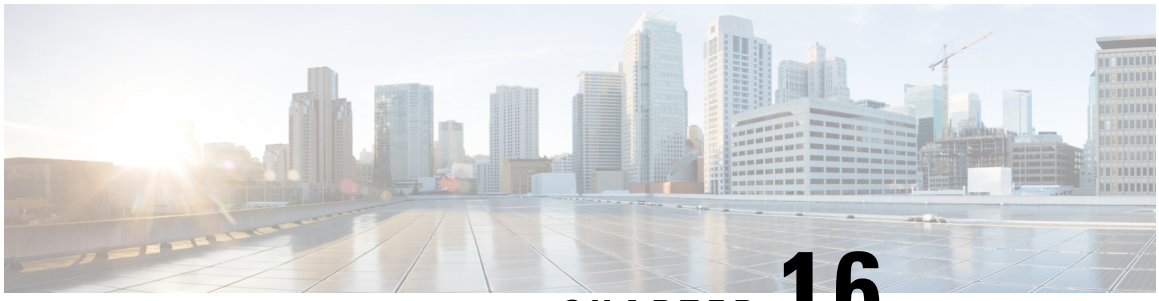
## Usage Guidelines

Sets the SPIO console port parameters for communication with the terminal device.

### Example

The following sequence of commands set the SPIO's console port to operate with specific values. The terminal must support these values.

```
terminal carrierdetect off
terminal databits 7
terminal flowcontrol hardware
terminal parity even
terminal speed 115200
terminal stopbits 1
```



CHAPTER 16

# S102 Pool Area Configuration Mode Commands

**Command Modes**

The commands in this configuration mode manage the configuration of the pool area characteristics.

Exec > Global Configuration > Context Configuration >

**configure > context** *context_name* **> s102-service** *service_name* **pool-area** *pool_area_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-s102-pool-area)#`

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

**Important** The **plmnid** option that is visible in the code is not supported at this time. This option is for future development.


- cell-id, on page 151
- do show, on page 152
- end, on page 153
- exit, on page 153
- hash-value, on page 153
- msc-id, on page 154
- plmnid, on page 155


# cell-id

Configure the sector cell ID to be used to locate the pool-area for the MSC selection process for CDMA2000 message handling in either a CSFB for 1xRTT or SRVCC for 1xRTT scenario.

**Product** MME

**Privilege** Administrator

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

**configure** > **context** *context_name* > **s102-service** *service_name* **pool-area** *pool_area_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-s102-pool-area)#
```

**Syntax Description**

**[ no ] cell-id** *cell-id* **+**

**no**

Erases the specific cell ID information from the S102 pool-area configuration.

***cell-id***

Enter an integer from 1 through 65535 to identify a CDMA2000 sector cell ID that you are assigning to this S102 pool-area configuration.

+ Means you can enter up to 24 cell IDs, separated by a single blank space, in the same command.

**Usage Guidelines**

Configure up to 24 cell IDs per S102 pool-area instance.

**Example**

Use a command similar to the following to define the three cell ID(s) for this S102 pool-area configuration:

```
cell-id 6 8 11 17
```

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`end`**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`exit`**

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

# hash-value

This command configures the hash-value(s) for the S102 pool-area. The hash-value is to be used by the MME for MSC selection for CDMA2000 message handling in either a CSFB for 1xRTT or SRVCC for 1xRTT scenario.



**Important** **Prerequisite:** Each of the MSCs to be included in the pool-area configuration must have been configured and associated with the S102 service before the MSC can be included in the pool-area configuration.

**Product** MME

**Privilege** Administrator

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

**configure > context** *context_name* **> s102-service** *service_name* **pool-area** *pool_area_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-s102-pool-area)#`

**Syntax Description**

**`[ no ] hash-value { hash_value | non-configured-values | range lower_hash_value to higher_hash_value } { msc msc_name }`**

**no**

Erases the configured hash-value information from the S102 pool-area configuration.

***hash_value***

Enter an integer from 0 through 999 to identify a specific MSC.

**non-configured-values msc *msc_name***

Assigns all non-configured hash values to use the named MSC.

*msc_name* Enter a string of 1 to 63 alphanumeric characters to identify one of the MSCs previously configured in the S102 service configuration.

**range *lower_hash_value* to *higher_hash_value* msc *msc_name***

Specifies the range of hash values for an MSC:

- *lower_hash_value* Enter an integer from 0 through 999 to identify the start value for a range of hash. The *lower_hash_value* must be lower than the *end_value*.
- *higher_hash_value* Enter an integer from 0 through 999 to identify the end value for a range of hash. The *higher_hash_value* must be higher than the *start_value*.
- **msc** *msc_name* Enter a string of 1 to 63 alphanumeric characters to identify one of the MSCs previously configured in the S102 service configuration.

**Usage Guidelines**

This command enables the operator to use hash as a filter in the MSC selection process. For more information about MSC selection and how it works, refer to either the *SRVCC for 1xRTT* feature chapter or the *CSFB for 1xRTT* feature chapter in the *MME Administration Guide*.

**Example**

Use a command similar to the following to setup a hash filter for MSC selection for a pool-area definition. The following command configures a hash value range filter of *24 to 43* for the selection of the MSC named *mscHouston* :

```
hash-value range 24 to 43 msc mscHouston
```

# msc-id

Configures the numeric ID for an MSC in the S102 pool-area configuration.



**Important** **Prerequisite:** Each of the MSCs to be included in the pool-area configuration must have been configured and associated with the S102 service before the MSC can be identified in the pool-area configuration.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration >

**configure > context** *context_name* **> s102-service** *service_name* **pool-area** *pool_area_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-s102-pool-area)#
```

**Syntax Description**

**[ no ] msc-id** *msc-id*

**no**

Erases the MSC ID configuration from this S102 pool-area configuration.

***msc-id***

Enter an integer from 1 through 16777215 to identify the unique numeric ID for the MSC.

**Usage Guidelines**

Both the cell ID and the MSC ID must be configured in the S102 pool-area configuration for the MME to have sufficient information to perform MSC selection.

For information about the pool-area, refer to the **pool-area** command in the *S102 Service Configuration Mode Commands* chapter.

For more information about MSC selection and how it works, refer to either the *SRVCC for 1xRTT* feature chapter or the *CSFB for 1xRTT* feature chapter in the *MME Administration Guide*.

**Example**

Identify the unique numeric ID, such as *2555*, for the MSC that has been configured for the S102 pool-area:

```
msc-id 2555
```

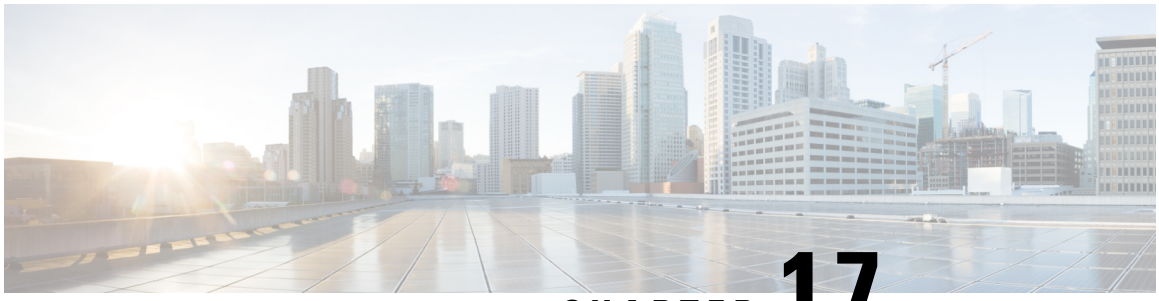
# plmnid

**Product**

MME

**Important**

The **plmnid** option that is visible in the code is not supported at this time. This option is for future development.



CHAPTER 17

# S102 Service Configuration Mode Commands

The S102 Service configuration mode is used to create and manage the configuration instance for the S102 Service which controls the S102 interface. This service works in conjunction with the MME Service.

**Command Modes**

Exec > Global Configuration > Context Configuration > S102 Service

**configure > context** *context_name* **> s102-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-s102-service)#
```

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

**Important** The **default** command prefix is visible in the S102 Service configuration mode. However, it is not supported at this time and has been included for the purpose of future development.


- 1xrtt, on page 157
- bind, on page 158
- do show, on page 159
- end, on page 160
- exit, on page 160
- ip, on page 160
- msc, on page 161
- non-pool-area, on page 162
- pool-area, on page 163


# 1xrtt

Identifies the type of CDMA2000 single-carrier radio transmission technology (1xRTT) functionality, CSFB or SRVCC, to be enabled for this S102 service.

**Product**

MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S102 Service

**configure > context** *context_name* **> s102-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-s102-service)#`

**Syntax Description**

**`[ no ] 1xrtt { csfb | srvcc }`**

**no**

Removes the 1xRTT identification from the S102 service/interface configuration.

**csfb**

Enables CSFB for 1xRTT for the S102 service/interface.

**srvcc**

Enables SRVCC for 1xRTT for the S102 service/interface.

**Usage Guidelines**

This command determines the type of signaling and functionality to be supported on the S102 interface, either circuit-switched fallback (CSFB) or single radio voice call continuity (SRVCC). The S102 interface provides the tunnel for the MME to pass CDMA2000 messages to/from the 1xCS IWS (interworking solution function)/MSC (mobile switching center).

For details of usage and configuration, refer to either the *CSFB for 1xRTT* feature chapter or the *SRVCC for 1xRTT* feature chapter in the *MME Administration Guide*.

**Example**

Use the following command to configure the S102 interface to support CSFB for 1xRTT:

**`1xrtt csfb`**

Use the following command to remove an S102 interface configuration for SRVCC for 1xRTT:

**`no 1xrtt srvcc`**

# bind

Bind and unbind a logical IP address and port to the S102 interface.

**Product**

MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S102 Service

**configure > context** *context_name* **> s102-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-s102-service)#
```

**Syntax Description**

**`[ no ] bind ipv4-address`** *`ipv4_address`* **`[ port`** *`port_number`* **`]`**

**no**

Removes the logical interface IPv4 address binding (unbinds) from the S102 service/interface.

**ipv4-address *ipv4_address***

Specifies the source IPv4 address of the S102 interface in IPv4 dotted-decimal notation.

**port *port_number***

Including this keyword is optional. If included, it configures the numeric identification of the port to be bound to the S102 interface.

*port_number* Enter an integer from 1 through 65535.

**Usage Guidelines**

Bind the S102 service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an S102 interface that provides the session connectivity for the MME to pass CDMA2000 messages to/from the 1xCS IWS (interworking solution function)/MSC (mobile switching center).

**Caution** This is a critical configuration. Any change to this configuration will cause the S102 service to restart. Removing or disabling this configuration will stop the S102 service.

**Example**

The following command binds the logical IP interface with the IPv4 address of 209.165.200.246 to the S102 service.

```
bind ipv4-address 209.165.200.246
```

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# ip

This command configures the IP parameters on the S102 interface.

**Product** MME

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > S102 Service

**configure > context** *context_name* **> s102-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-s102-service)#
```

**Syntax Description**

**`[ no ] ip qos-dscp`** *`dscp_value`*

**no**

Removes IP parameter configuration from the S102 service/interface.

**qos-dscp *dscp_value***

The **qos-dscp** keyword designates the Quality of Service - Differentiated Services Code Point value to the packet leaving through the S102 interface.

*dscp_value* is a value assigned to the packet for DSCP marking. The value can be a pre-defined DSCP value or an arbitrary value ranging from 0x01 to 0x3F.

**Usage Guidelines**

S102 interface allows Differentiated Services Code Point (DSCP) marking functionality. DSCP marking helps in packet traffic management. DSCP marking can be performed only on IPv4 packets leaving the S102 interface.

Either the pre-defined DSCP values can be used for marking, or any arbitrary value ranging from 0x01 to 0x3F can be assigned. The default DSCP value is 0x00 or be (Best Effort). The default DSCP value is automatically set when the configuration is disabled.

**Example**

The following command shows the IP configuration for DSCP marking on the S102 service.

```
ip qos-dscp ef
```

# msc

Command creates a configuration instance for a single mobile switching center (1x RTT MSC) in the S102 service configuration. The MSCs are used by the SRVCC and CSFB functions when the MME handles CDMA2000 messages from/to UEs.

**Product**

MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S102 Service

**configure > context** *context_name* **> s102-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-s102-service)#
```

**Syntax Description**

**`[ no ] msc`** *`msc_name`*

**no**

Erases the MSC configuration from the S102 service configuration.

***msc_name***

Identifies a specific MSC. The name must be a string of 1 through 63 alphanumeric characters. We recommend that each defined MSC name be unique on the system.

**Usage Guidelines**

This command creates an instance of an MSC configuration for the S102 service configuration and it provides access to the S102 MSC configuration mode commands to configure parameters related to the MSC.

The MSC(s) configured with this command can be identified in the **pool-area** and **non-pool-area** configurations to setup MSC selection. For more details about MSC selection, refer to the *SRVCC for 1xRTT* or *CSFB for 1xRTT* feature chapters in the *MME Administration Guide*.

It is possible to associate up to 10 MSCs with the S102 interface/service configuration. Repeat the **msc**, **ipv4-address**, and **exit** commands sequence as often as needed to identify all MSCs.

**Example**

Use a command similar to the following one to assign a unique name to identify an MSC in the S102 service configuration:

```
msc msc1
```

# non-pool-area

This command configures a non-pool-area instance to be used by the MME for MSC selection for CDMA2000 message handling in either a CSFB for 1xRTT or SRVCC for 1xRTT scenario.

**Important** **Prerequisite:** Each of the MSCs to be included in the non-pool-area configuration must have been configured and associated with the S102 service before the MSC can be identified in the non-pool-area configuration.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S102 Service

**configure > context** *context_name* **> s102-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-s102-service)#
```

**Syntax Description**

**Important** The **plmn** option that is visible in the code is not supported at this time and so it is not included in the following syntax description. This option is included in the code for future development.

```
non-pool-area non_pool_area_name msc msc_name msc-id msc_id cell-id cell_id +
no non-pool-area non_pool_area_name cell-id cell_id +
```

**no**

Erases the configured non-pool-area information.

***non_pool_area_name***

Enter a string of 1 to 63 alphanumeric characters to uniquely identify this non-pool-area configuration to be used for MSC selection.

**msc *msc_name***

Identify a 1x RTT mobile switching center (MSC) that is associated with the S102 service/interface configuration.

*msc_name* Enter a string of 1 to 63 alphanumeric characters to identify one of the MSCs previously configured in the S102 service configuration.

**msc-id *msc_id***

*msc_id*Enter an integer from 1 through 16777215 to identify the unique numeric ID for the MSC.

**cell-id *cell_id* +**

*cell_id*Enter an integer from 1 through 65535 to identify a CDMA2000 sector cell ID that you are assigning to this non-pool area configuration.

**+** Indicates that more than one cell ID can be included in the command. Enter up to 24 cell IDs, separated by a single blank space, in the same command.

**Usage Guidelines**

Up to 10 MSC pool or non-pool areas can be configured per S102 service in support of MSC selection for the MME handling either SRVCC or CSFB 1xRTT CDMA2000 messages from a UE. Both the MSC-Id and the Cell-Id are used to locate the pool or non-pool area for the MSC selection process.

For information about the pool-area, refer to the **pool-area** command sheet also in the S102 Service configuration mode.

For more information about MSC selection and how it works, refer to either the *SRVCC for 1xRTT* feature chapter or the *CSFB for 1xRTT* feature chapter in the *MME Administration Guide*.

**Example**

Use a command similar to the following to setup a non-pool-area definition. The following command configures a non-pool-area named *npoolLondon1* and includes an MSC named *mscLondon* that has a numeric ID of *2443* and includes cells *5, 6, 7, and 22*:

```
non-pool-area npoolLondon1 msc mscLondon msc-id 2443 cell-id 5 6 7 22
```

# pool-area

This command creates a pool-area instance to be used by the MME for MSC selection for CDMA2000 message handling in either a CSFB for 1xRTT or SRVCC for 1xRTT scenario.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S102 Service

**configure > context** *context_name* **> s102-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-s102-service)#
```

**Syntax Description**

**[ no ] pool-area** *pool_area_name*

**no**

Erases the pool-area instance from the S102 service configuration.

***pool_area_name***

Enter a string of 1 to 63 alphanumeric characters to uniquely identify this pool-area configuration to be used for MSC selection.

**Usage Guidelines**

Up to 10 MSC pool and/or non-pool areas can be configured per S102 service in support of MSC selection for the MME handling either SRVCC or CSFB 1xRTT CDMA2000 messages from a UE. Both the MSC-Id and the Cell-Id are used to locate the pool or non-pool area for the MSC selection process.

Issuing this command also takes the MME into the S102 Pool Area configuration mode for the commands to configure the pool-area characteristics: Cell ID, hash-value, and MSC ID. Refer to the *S102 Pool Area Configuration Mode Commands* in this document.

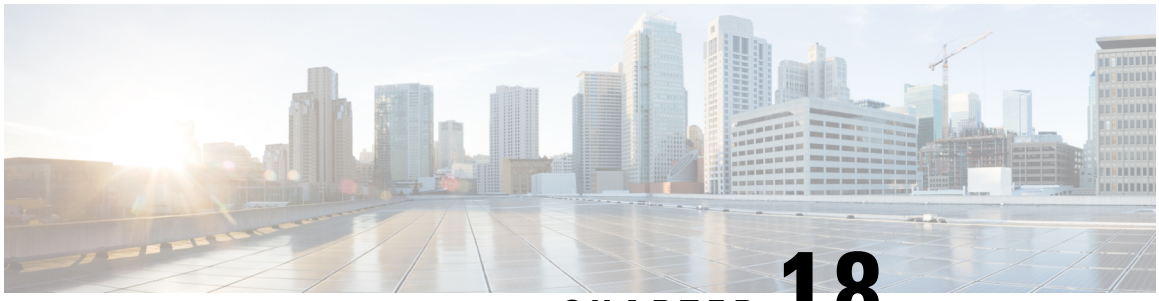
For information about the non-pool-area, refer to the **non-pool-area** command section also in the *S102 Service Configuration Mode Commands* chapter.

For more information about MSC selection and how it works, refer to either the *SRVCC for 1xRTT* feature chapter or the *CSFB for 1xRTT* feature chapter in the *MME Administration Guide*.

### Example

The following command creates the S102 pool-area instance named *s102pool-1*:

```
pool-area s102pool-1
```



CHAPTER 18

# S102 MSC Configuration Mode Commands

The commands of the S102 MSC configuration mode define the characteristics of the CDMA2000 1xRTT mobile switching center (MSC) associated with the S102 interface.

**Command Modes**

Exec > Global Configuration > Context Configuration > S102 Service Configuration > S102 MSC Configuration

**configure > context** *context_name* **> s102-service** *service_name* **msc** *msc_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-s102-msc)#
```

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


- do show, on page 165
- end, on page 166
- exit, on page 166
- ipv4-address, on page 166


# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# ipv4-address

Adds the IPv4 address of the interface associated with the MSC, and optionally the port ID, to the S102 service configuration.

**Product** MME

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > S102 Service Configuration > S102 MSC Configuration

**configure > context** *context_name* **> s102-service** *service_name* **msc** *msc_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-s102-msc)#
```

## Syntax Description

**[ no ] ipv4-address** *ipv4_address* **port** *port_number*

### no

Erases the specific IPv4 address configuration for the MSC from the S102 service configuration.

### *ipv4_address*

Identifies IPv4 address of the interface to the MSC. The value for the IPv4 address must be entered in standard IPv4 dotted-decimal notation.

### port *port_number*

If this keyword option is included with the command, it configures an identifying port number for the MSC. The port number must be an integer from 1 through 65535.

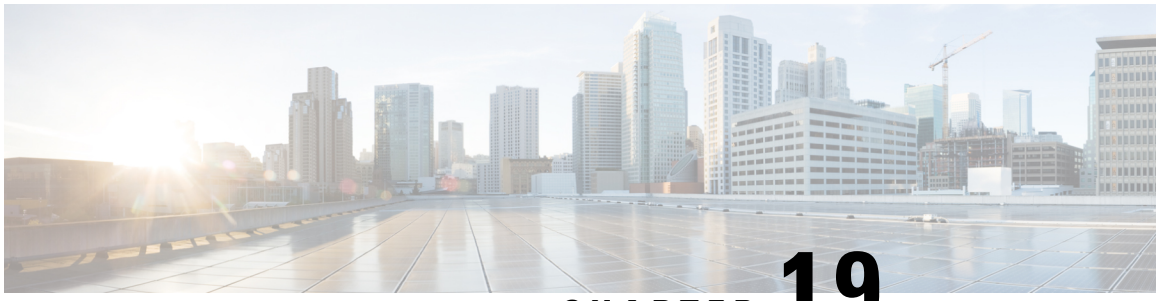
## Usage Guidelines

It is possible to associate up to 10 IWS/MSCs with the S102 interface/service configuration. Repeat the **msc**, **ipv4-address**, and **exit** commands sequence as often as needed to identify all MSCs.

### Example

Use a command similar to the following to define the target IPv4 address and port number for the MSC's interface:

```
msc 111.111.111.1 port 4334
```



CHAPTER 19

# S1AP Cause Code Configuration Mode Commands

The cause code group object allows an operator to group together a set of cause codes. This group can then be used as a named object in other commands.

**Command Modes**

Exec > Global Configuration > LTE Policy Configuration > S1AP Cause Code Configuration

**configure > lte-policy > cause-code-group** *group_name*

Entering the above command sequence results in the following prompt:

```
[local]  host_name (s1ap-cause-code)
```

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


- class, on page 169
- do show, on page 170
- end, on page 171
- exit, on page 171


# class

Configures a set of cause codes within a cause code group.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > LTE Policy Configuration > S1AP Cause Code Configuration

**configure > lte-policy > cause-code-group** *group_name*

Entering the above command sequence results in the following prompt:

```
[local]  host_name (s1ap-cause-code)
```

**Syntax Description**

**[no] class { miscellaneous | nas | protocol | radio | transport } cause** *cause_no*

**no**

Removes the specified cause code class.

**miscellaneous**

Specifies the class of miscellaneous cause codes.

**nas**

Specifies the class of NAS cause codes.

**protocol**

Specifies the class of protocol cause codes.

**radio**

Specifies the class of radio cause codes.

**transport**

Specifies the class of transport cause codes.

**cause *cause_no***

Specifies the cause codes to add to this class. Cause codes must be defined one at a time.

*cause_no* is a numeric cause code value, as defined in 3GPP TS 36.413.

**Usage Guidelines**

Use this command to configure the specific cause codes within this S1AP Cause Code Group.

A maximum of 16 cause codes can be added to a cause-code-group entry.

Refer to the **policy service-request** command and **policy tau** command in the MME Service Configuration Commands Chapter to configure the behavior of the MME when the intial context setup fails during a service request procedure or while processing a TAU request.

The specific action taken by the MME can be mapped to the cause codes defined in this command.

**Example**

The following commands add causes **failure-in-radio-interface-procedure** and **interaction-with-other-procedure** to the cause code group.

```
class radio cause 26
class radio cause 29
```

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege** Security Administrator, Administrator

**Syntax Description** `do show`

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `end`

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

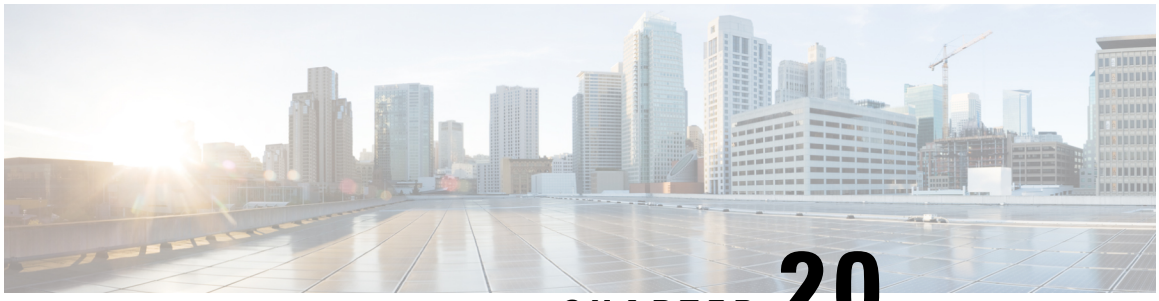
**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `exit`

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

exit



CHAPTER 20

# S1-U Relay Configuration Mode Commands

**Important** In Release 20, 21.0 and 21.1, HeNBGW is not supported. Commands in this configuration mode must not be used in these releases. For more information, contact your Cisco account representative.

The S1-U Relay configuration option enables the S1-U Relay service functionality to the HeNB-GW Access Service. . In this mode user can configure associations to the Access and Network GTP-U services for S1-U Relay

**Command Modes** Exec > Global Configuration > Context Configuration > HeNB-GW Access Service Configuration > S1-U Relay Configuration

**configure > context** *context_name* **> henbgw-access-service** *access_svc_name* **> s1u-relay**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(s1u-relay)#
```

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


- associate, on page 173
- do show, on page 174
- end, on page 175
- exit, on page 175
- ip, on page 175


# associate

Associates previously configured Access GTP-U service as well as the Network GTP-U service to this HeNB-GW Access Service for S1-U relay service functionality. The Access and Network GTP-U services must be configured in the Context Configuration mode before using this configuration.

**Product** HeNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HeNB-GW Access Service Configuration > S1-U Relay Configuration

**configure > context** *context_name* **> henbgw-access-service** *access_svc_name* **> s1u-relay**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(s1u-relay)#
```

**Syntax Description**

**associate { access-gtpu-service** *access_gtpu_svc* **| network-gtpu-service** *network_gtpu_svc* **} [ context** *ctxt_name* **]**
**no associate { access-gtpu-service | network-gtpu-service }**

**no**

Removes the associated Access or Network GTP-U service from this HeNB-GW Access service configuration.

***access_gtpu_svc***

Identifies the name of the pre-configured Access GTP-U service in Context Configuration Mode to associate with this HeNB-GW Access Service for S1-U relay.

*acess_gtpu_svc* is an alphanumeric string of 1 through 63 characters.

***network_gtpu_svc***

Identifies the name of the pre-configured Network GTP-U service to associate with this HeNB-GW Access Service for S1-U relay.

*network_gtpu_svc* is an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to bind/associate a pre-configured Access or Network GTP-U service to this HeNB-GW Access service. When S1-U Relay is enabled, the association to ingress and egress GTP-U services is considered as critical configuration for the HeNB-GW Access service. When S1-U relay is enabled, both access and network gtpu services needs to be in STARTED state for the HENBGW access service to be started.

**Example**

Following command associates a Network GTP-U service named *net_gtpu* in egress context with a specific HeNB-GW Access service:

**associate network-gtpu-service net_gtpu context egress**

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description** `do show`

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `end`

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `exit`

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

# ip

Configures the Internet protocol (IP) parameters including downlink and uplink of data for specified HENBGW ACCESS service.

**Product** HeNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HeNB-GW Access Service Configuration > S1-U Relay Configuration

**configure > context** *context_name* **> henbgw-access-service** *access_svc_name* **> s1u-relay**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(s1u-relay)#
```

**Syntax Description**

**Release 19.2 and later:**

**ip { downlink | uplink } qci-dscp-mapping-table** *table_name*

**Release 18 and earlier:**

**ip { downlink | uplink } qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef }**



**Important** The **qos-dscp** keyword is deprecated from 19.2 and later releases.

**no ip { downlink | uplink } qci-dscp-mapping-table**

**no**

Removes the IP parameters for downlink/uplink data from this HeNB-GW Access service configuration.

Removes the QCI-DSCP mapping table for downlink/uplink data from this HeNB-GW Access service configuration.

**downlink**

Direction (towards henb) in which DSCP marking shall be done.

**uplink**

Direction (towards sgw) in which DSCP marking shall be done.

**qci-dscp-mapping-table *table_name***

QCI-DSCP mapping table to refer for this HENBGW ACCESS service.

*table_name* is the table name , which is a string of size 1 to 63.

**qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef }**

Default: **af11**

Specifies the DSCP for the specified QoS traffic pattern. **qos-dscp** can be configured to any one of the following:

**af11**: Assured Forwarding 11 per-hop-behavior (PHB)

**af12**: Assured Forwarding 12 PHB

**af13**: Assured Forwarding 13 PHB

**af21**: Assured Forwarding 21 PHB

**af22**: Assured Forwarding 22 PHB

**af23**: Assured Forwarding 23 PHB

**af31**: Assured Forwarding 31 PHB

**af32**: Assured Forwarding 32 PHB

**af33**: Assured Forwarding 33 PHB

**af41**: Assured Forwarding 41 PHB

**af42**: Assured Forwarding 42 PHB

**af43**: Assured Forwarding 43 PHB

**be**: Best effort forwarding PHB

**ef**: Expedited forwarding PHB

## Usage Guidelines

Use this command to configure the Internet protocol (IP) parameters including downlink and uplink of data for specified HENBGW ACCESS service.

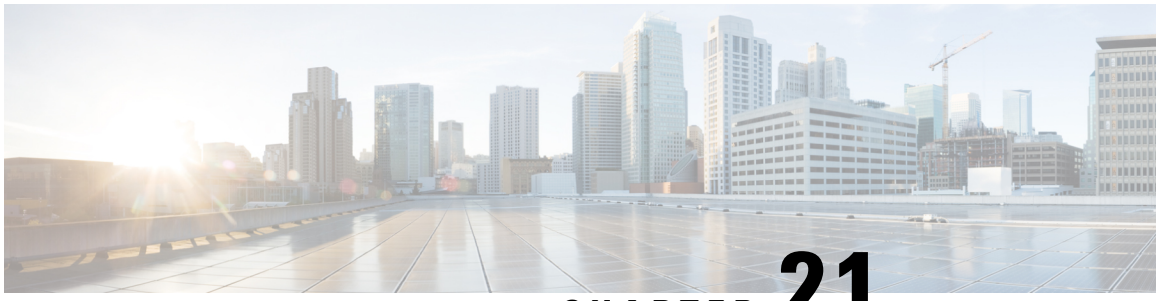
### Example

Following command configures the DSCP-level for uplink data traffic through a specific HeNB-GW Access service to **af31**:

```
ip uplink qos-dscp af31
```

Following command configures the QCI-DSCP mapping table table1.

```
ip uplink qci-dscp-mapping-table table1
```



CHAPTER 21

# SAEGW Service Configuration Mode Commands

**Command Modes**

The System Architecture Evolution Gateway (SAEGW) Service Configuration Mode is used to create and manage the relationship between specified services used for S-GW and P-GW network traffic.

Exec > Global Configuration > Context Configuration > SAEGW Service Configuration

**configure > context** *context_name* **> saegw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-saegw-service)#
```

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


- associate, on page 179
- do show, on page 181
- gtpc handle-collision upc nrupc, on page 181
- end, on page 182
- exit, on page 182
- sxa-tunnel-del-at-dsr-on-sgw-change, on page 182


# associate

Associates the SAEGW service with specific pre-configured services configured in the same context.

**Product**

SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SAEGW Service Configuration

**configure > context** *context_name* **> saegw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-saegw-service)#
```

## Syntax Description

**[ no ] associate { pgw-service** *name* **| gtpu-service** *service_name* **up-tunnel | sgw-service** *name* **sx-service** *name* **}**

### no

Removes the selected association from this service.

### pgw-service *name*

Specifies that the SAEGW service is to be associated with an existing P-GW service within this context.

*name* must be an alphanumeric string of 1 through 63 characters and be an existing P-GW service.

### sgw-service *name*

Specifies that the SAEGW service is to be associated with an existing S-GW service within this context.

*name* must be an alphanumeric string of 1 through 63 characters and be an existing S-GW service.

**Important** S-GW egress eGTP service must be in the same context as this SAEGW service. In addition, PMIP is not supported for the S-GW service egress.

### sx-service *name*

Specifies that the SAEGW service is to be associated with an existing Sx service within this context.

*name* must be an alphanumeric string of 1 through 63 characters and be an existing Sx service.

### up-tunnel

Configures the interface type as up-tunnel (tunnel towards User Plane function).

## Usage Guidelines

Use this command to associate the SAEGW service with other pre-configured services configured in the same context.

**Important** Each P-GW or S-GW service may only be associated with one SAEGW service; however, there may be multiple SAEGW services configured on a system in separate contexts.

### Example

The following commands associate this SAEGW service with a P-GW service called *pgw1* and a S-GW service called *sgw2*:

```
associate pgw-service pgw1
associate sgw-service sgw2
```

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution**

There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# gtpc handle-collision upc nrupc

This command helps in enabling or disabling collision handling between SGSN initiated UPC and NRUPC request.

**Product**

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SAEGW Service Configuration

**configure > context** *context_name* **>saegw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-saegw-service)#
```

**Syntax Description**

```
[ no | default ] gtpc handle-collision upc nrupc
```

**no**

Disables collision handling between SGSN initiated UPC and NRUPC request.

**default**

Sets default collision handling behavior between SGSN initiated UPC and NRUPC request. By default, collision handling is enabled.

### handle-collision upc nrupc

Enables/Disables collision handling between SGSN initiated UPC and network requested UPC. By default, collision handling is enabled.

**Usage Guidelines** This command is used to enable or disable collision handling between SGSN initiated UPC and NRUPC request.

### Example

The following example disables collision handling between SGSN initiated UPC and NRUPC request.

```
no gtpc handle-collision upc nrupc
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
end
```

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
exit
```

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

# sxa-tunnel-del-at-dsr-on-sgw-change

This command enables or disables the Sxa tunnel deletion at DSR during X2 based and S1 based handover with SGW relocation.

**Product** SAEGW

**Privilege** Security Administrator, Administrator

## Command Modes

Exec > Global Configuration > Context Configuration > SAEGW Service Configuration

**configure > context** *context_name* **> saegw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-saegw-service)#
```

## Syntax Description

**[ no ] sxa-tunnel-del-at-dsr-on-sgw-change**

**no**

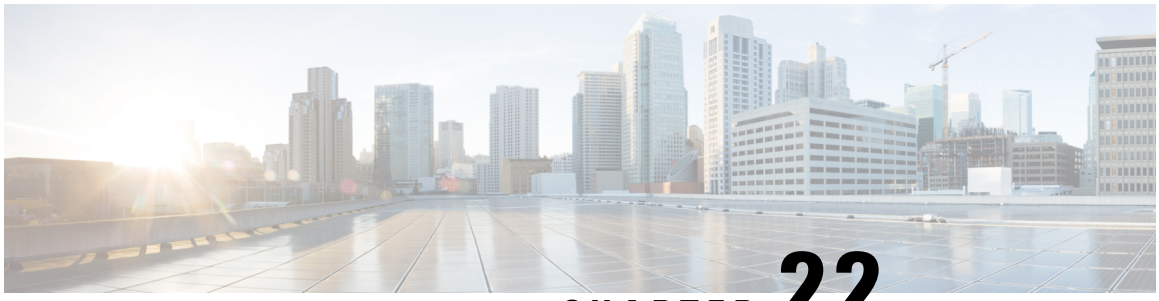
Disable the Sxa tunnel deletion at DSR during X2/S1 based handover.

**sxa-tunnel-del-at-dsr-on-sgw-change**

Enable the Sxa tunnel deletion at DSR during X2/S1 based handover with SGW relocation.

## Usage Guidelines

This command is used to enable or disable the Sxa tunnel deletion at DSR during X2/S1 based handover with SGW relocation.



CHAPTER 22

# SaMOG Service Configuration Mode Commands

**Command Modes**

Creates SaMOG service and enters SaMOG service configuration mode.

Exec > Global Configuration > Context Configuration > SAMOG Service Configuration

**configure > context** *context_name* **> samog-service** *samog_service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-samog-service)#`

**Important** Available commands or keywords/variables vary based on platform type, product version, and installed license(s).


- associate, on page 185
- do show, on page 187
- end, on page 188
- exit, on page 188
- max-sessions, on page 188
- reporting-action, on page 189
- timeout, on page 190


# associate

SaMOG associates another service to this SAMOG service.

**Product**

SaMOG

**Command Modes**

Exec > Global Configuration > Context Configuration > SAMOG Service Configuration

**configure > context** *context_name* **> samog-service** *samog_service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-samog-service)#`

**Syntax Description**

**associate { apgroupname-list** *aplistname1* reject-call **cgw-service** *cgw_service_name* **| dhcp-service** *dhcp_service_name* **[ level { system | user } ] | dhcpv6-service** *dhcpv6_service_name* **| mrme-service** *mrme_service_name* **| subscriber-map**

*subscriber_map_name* **}**
**no associate {** apgroupname-list reject-call **cgw-service | dhcp-service | dhcpv6-service | mrme-service | subscriber-map }**

**no**

Disables the association of the service with the SaMOG service.

The **no associate dhcp-service** command does not disassociate existing sessions, and only new sessions will not be established. Existing sessions continue to use the DHCPv4 service to which it was bound during session establishment.

The **no associate dhcpv6-service** command stops the SaMOG service from processing DHCPv6 packets.

**cgw-service *cgw_service_name***

The CGW service should be configured before associating the same with SaMOG service.

*cgw_service_name* must be an alphanumeric string between 1 and 63 characters.

**dhcp-service *dhcp_service_name* [ level { system | user } ]**

Specifies the DHCPv4 service to associate with the SaMOG service. DHCPv4 is optional while starting an SaMOG service.

*dhcp_service_name* must be an alphanumeric string from 1 through 63.

While the association of the DHCPv4 service with the SaMOG service is optional, DHCPv4 service must be associated with the SaMOG service for the SaMOG Ethernet over GRE (EoGRE) feature to function. If no DHCPv4 service is configured and associated, and at least one EoGRE access type Radius client exist, the output of the **show configuration errors** command will display a warning under the **SaMOG service system errors** section.



**Important** The associated DHCPv4 service must not be used for any service other than SaMOG, as packets are always forwarded over the EoGRE tunnel only.

**level { system | user }**: Specifies the processing level of the DHCP server messages. **system** will enable DHCP server messages to be processed at the system and user-level. **user** will enable DHCP server messages to be processed at the user-level only. The default value for processing DHCP messages is user level.

**dhcpv6-service *dhcpv6_service_name***

Specifies the DHCPv6 service to associate with the SaMOG service, to process DHCPv6 packets. Configure the DHCPv6 server using the **bind address** command in the DHCPv6 Service Configuration Mode.

*dhcpv6_service_name* must be an alphanumeric string from 1 through 63 characters.

**mrme-service *mrme_service_name***

The MRME service should be configured before associating the same with SaMOG service.

*mrme_service_name* must be an alphanumeric string from 1 through 63 characters.

**subscriber-map *subscriber_map_name***

The subscriber map service should be configured before associating the same with SaMOG service.

*subscriber_map_name* must be an alphanumeric string from 1 through 63 characters.

**associate apgroupname-list**

Associates the configured apgroupname-list with samog-service.

**no associate apgroupname-list reject-call**

Dis-associates APGROUPNAME list from the SaMOG and all the AP group names present in the list are allowed to establish session.

**Usage Guidelines**

Use this command to associate the SaMOG service to CGW service, DHCPv4 service, MRME service, or Subscriber Mapping.

**Example**

The following command associates subscriber-map *smap* with SaMOG Service.

```
associate subscriber-map smap
```

The following command associates cgw-service *cgw* with SaMOG Service.

```
associate cgw-service cgw
```

The following command associates mrme-service *mrme* with SaMOG Service.

```
associate mrme-service mrme
```

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# max-sessions

Configures maximum number of subscribers SAMOG service can support, ranging from 0 to 4000000.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > SAMOG Service Configuration

**configure > context** *context_name* **> samog-service** *samog_service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-samog-service)#
```

**Syntax Description**

**max-sessions** *max_sessions*
**default max-sessions**

**max-sessions *max_sessions***

Configures maximum number of subscribers SAMOG service can support.

*max_sessions* is an integer value between *0* and *4000000*.

**default**

Sets the default value, 4000000 for Max Sessions.

**Usage Guidelines**

Use this command to configure the maximum number of subscribers SAMOG service can support.

**Example**

Use the following command to configure the maximum number of subscribers SAMOG service can support:

**max-sessions** *500*

# reporting-action

Configures reporting of events.

**Product**

SaMOG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SAMOG Service Configuration

**configure > context** *context_name* **> samog-service** *samog_service_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-samog-service)#`

**Syntax Description**

**[ no ] reporting-action event-record**

**no**

Disables RTT record generation for this SaMOG service.

**event-record**

Configures event records.

**Syntax Description**

Use this command to configure the reporting of events for the SaMOG service.

### Example

The following command configures the reporting of event records:

**reporting-action event-record**

# timeout

Configures the session's time-to-live (TTL) settings under SAMOG service.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SAMOG Service Configuration

**configure** > **context** *context_name* > **samog-service** *samog_service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-samog-service)#`

**Syntax Description**

**timeout { absolute** *absolute_value* **| idle** *idle_value* **| setup-timeout** *setup_timeout_value* **}**
**default timeout [ absolute | idle | setup-timeout ]**
**no timeout [ absolute | idle ]**

#### default

Sets/restores the default value assigned for timeout.

The default value of absolute and idle timeout is *0*, which indicates the function is disabled.

The default value of setup-timeout is *60*.

#### no

Enables / Disables the timeout option.

#### absolute *absolute_value*

Specifies the maximum duration of the session, in seconds, before the system automatically terminates the session.

*absolute_value* must be an integer between *0* and *2147483647*.

#### idle *idle_value*

Specifies the maximum duration a session can remain idle, in seconds, before the system automatically terminates the session. Zero indicates that the timeout function is disabled. Default is *0*.

*idle_value* must be an integer between *0* and *2147483647*.

**setup-timeout *setup_timeout_value***

Specifies the maximum time allowed for session setup in seconds. Default is *60* seconds.

*setup_timeout_value*must be an integer between *0* and *1000000*.

## Usage Guidelines

Use this command to configure the session's time-to-live (TTL) settings under SAMOG service.

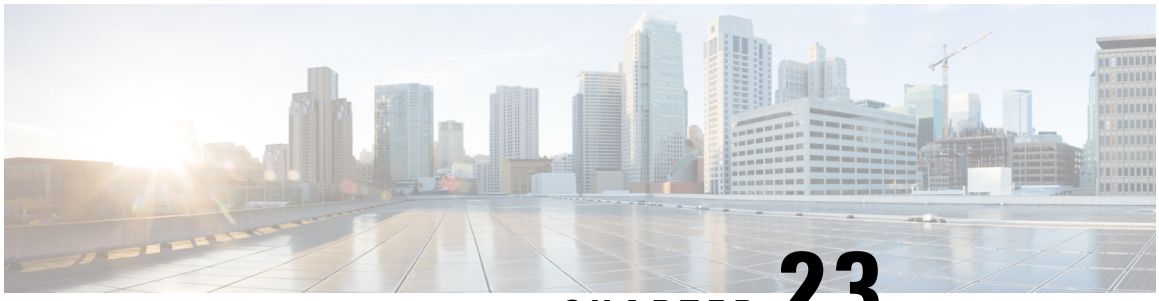
### Example

Use the following command to configure the setup-timeout to 500 seconds:

```
timeout setup-timeout 500
```

Use the following command to configure the absolute timeout to 120 seconds:

```
timeout absolute 120
```



CHAPTER 23

# SBc Service Configuration Mode Commands

The SBc (SBc-AP) interface is used by the MME to communicate with Cell Broadcast Centers (CBC) and deliver Public Warning Messages to eNodeBs. The SBc Service provides support on the MME for the Commercial Mobile Alert System (CMAS).

**Command Modes**

Exec > Global Configuration > Context Configuration > SBc Service Configuration

**configure > context** *context_name* **> sbc-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sbc-service)#
```

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

**Important** Beginning with Release 18.4, a valid license key is required to access the commands in this configuration mode. For information about obtraining such a license, contact your Cisco Representative.


- associate, on page 193
- bind, on page 194
- cbc-associations, on page 195
- do show, on page 196
- end, on page 196
- exit, on page 197
- ip, on page 197
- sbc-mme, on page 198
- send, on page 199


# associate

This new command specifies the SCTP parameter template to employ for this SBc-AP interface.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SBc Service Configuration

**configure > context** *context_name* **> sbc-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sbc-service)#
```

**Syntax Description**

**associate sctp-param-template** *sctp_param_template_name*
**no associate sctp-param-template**

**no**

Disassociates the specified SCTP Parameter Template from this SBc service.

**sctp-param-template *sctp_param_template_name***

Associates the previously created SCTP Parameter Template with this SBc service.

*sctp_param_template_name* must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Associates a previously created SCTP Parameter Template with this SBc service.

Configuration of the SCTP Parameter template is a pre-requisite for this command.

Changes to the configuration will restart the SBc service.

Associating the SBc service to the SCTP parameter template is not required for the SBc service to be operational.

Refer to the **sctp-param-template** command in the *Global Configuration Mode Commands (L-S) chapter* for more information about configuring a SCTP Parameter Template.

# bind

Binds the SBc service to a local SCTP IP address. This interface is used by the SBc service to communicate with the Cell Broadcast Center (CBC).

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SBc Service Configuration

**configure > context** *context_name* **> sbc-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sbc-service)#
```

**Syntax Description**

**bind { ipv4-address** *ipv4_address_value1* **[ ipv4-address** *ipv4_address_value2* **] | ipv6-address** *ipv6_address_value1* **[ ipv6-address** *ipv6_address_value2* **]**
**no bind**

**no**

Removes the interface binding from this SBc service.

**ipv4-address *ipv4_address_value1* [ ipv4-address *ipv4_address_value2* ]**

Specifies the IPv4 address of an interface in the current context through which communication with the CBC occurs.

A second IPv4 address can be specified for multi-homing purposes with the optional **ipv4-address** keyword.

**ipv6-address *ipv6_address_value1* [ ipv6-address *ipv6_address_value2* ]**

Specifies the IPv6 address of an interface in the current context through which communication with the CBC occurs.

A second IPv6 address can be specified for multi-homing purposes with the optional **ipv6-address** keyword.

**Usage Guidelines**

Use this command to bind the SBc service to an IP address.

The command is service critical; removing the configuration will stop the SBc service.

Up to two IPv4 or two IPv6 addresses can be specified for multi-homing purposes.

Refer to the **sbc-mme** command in this chapter to specify the SCTP port number to be used.

**Example**

The following command configures 2 IPv4 addresses for the SCTP connection (for multi homing):

```
bind ipv4-address 209.165.200.234 ipv4-address 209.165.200.244
```

# cbc-associations

Configures the maximum number of Cell Broadcast Center (CBC) connections allowed for this SBc service.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SBc Service Configuration

**configure > context** *context_name* **> sbc-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sbc-service)#
```

**Syntax Description**

**{ default | no } cbc-associations maximum** *number*

**default**

Returns the maximum number of CBC associations allowed to the default of 1.

**no**

Removes the configured maximum number of CBC associations allowed, and returns the setting to the default value of 1.

**maximum *number***

Configures the maximum number of CBC associations allowed for this SBc service.

*number* must be an integer from 1 to 2.

Default: 1.

**Usage Guidelines** Use this command to configure the maximum number of CBC associations allowed for this SBc service.



**Caution** Changes to this configuration will restart the SBc service.

# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`end`**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`exit`**

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

# ip

This command configures the IP parameters on the SGs interface.

**Product** MME

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > MME SGs Service Configuration

**configure > context** *context_name* **> sgs-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-sgs-service)#`

**Syntax Description** **`[ no ] ip qos-dscp`** *`dscp_value`*

**no**

Removes IP parameter configuration from the SGs service/interface.

**qos-dscp *dscp_value***

The **qos-dscp** keyword designates the Quality of Service - Differentiated Services Code Point value to the packet leaving through the SGs interface.

*dscp_value* is a value assigned to the packet for DSCP marking. The value can be a pre-defined DSCP value or an arbitrary value ranging from 0x01 to 0x3F.

**Usage Guidelines** SGs interface allows Differentiated Services Code Point (DSCP) marking functionality. DSCP marking helps in packet traffic management. DSCP marking can be performed on both IPv4 and IPv6 packets leaving the SGs interface.

Either the pre-defined DSCP values can be used for marking, or any arbitrary value ranging from 0x01 to 0x3F can be assigned. The default DSCP value is 0x00 or be (Best Effort). The default DSCP value is automatically set when the configuration is disabled.

### Example

The following command shows the IP configuration for DSCP marking on the SGs service.

```
ip qos-dscp ef
```

# sbc-mme

Configures the SCTP port to be used for the SBc interface.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SBc Service Configuration

**configure** > **context** *context_name* > **sbc-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sbc-service)#
```

**Syntax Description**

**sbc-mme sctp port** *port_num*
**[ default | no ] sbc-mme sctp port**

#### default

Returns the command to the default SCTP port of 29168.

#### no

Removes the configured SCTP port value, and returns the command to the default SCTP port of 29168.

#### sctp port *port_num*

Configures the SCTP port to be used for the SBc interface.

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

Default: 29168.

**Usage Guidelines**

Use this command to configure the SCTP port number for this SBc service.

### Example

The following command configures this SBc service to use SCTP port number 21112:

```
mme-sbc sctp-port 21112
```

# send

This command enables or disables the warning indication messages towards CBC from MME.

.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SBc Service Configuration

**configure > context** *context_name* **> sbc-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-sbc-service)#`

**Syntax Description**

**`[ no | default ]  send { stop-warning-ind | write-replace-warning-ind }`**

**no**

Removes the configuration of sending the warning indication [ stop warning / write replace warning ] messages towards CBC from MME.

**default**

Sets the default configuration of sending the warning indication [ stop warning / write replace warning ] messages towards CBC from MME. By default sending of warning indication messages are disabled.

**send stop-warning-ind**

Enables the stop warning indication messages towards CBC from MME.

**send write-replace-warning-ind**

Enables the write-replace-warning indication messages towards CBC from MME.

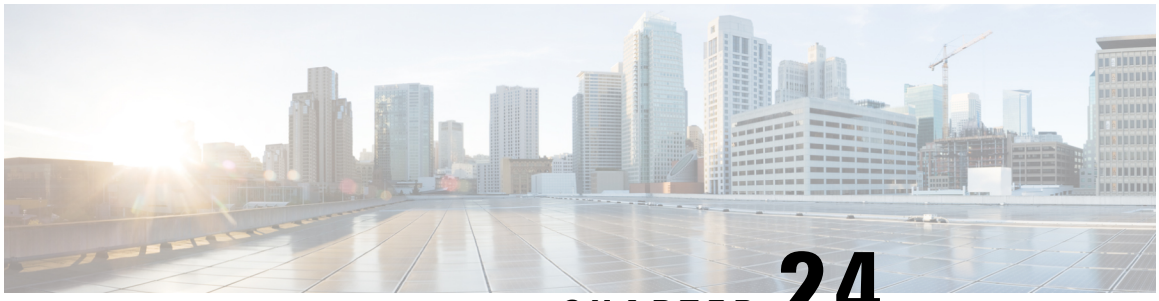
**Usage Guidelines**

Use this command to enables or disables the warning indication messages towards CBC from MME.

**Example**

The following command to stop warning indication message towards CBC from MME:

**`send stop-warning-ind`**



CHAPTER 24

# SCCP Network Configuration Mode Commands

Signaling Connection Control Part (SCCP) is a routing protocol in the SS7 protocol suite in layer 4, which provides end-to-end routing for TCAP messages to their proper database.

**Command Modes**

The SCCP Network Configuration Mode is used to configure properties for Signaling Connection Control Part (SCCP) services for SS7.

Exec > Global Configuration > SCCP Network Configuration

**configure > sccp-network** *id_number*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-sccp-network-sccp_id)#`

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


- associate, on page 201
- description, on page 202
- destination, on page 203
- do show, on page 205
- end, on page 205
- exit, on page 206
- global-title-translation, on page 206
- hop-count, on page 207
- self-point-code, on page 208
- timeout, on page 209


# associate

Associates an SS7 routing domain with the SCCP network.

**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

**Product**

SGSN

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SCCP Network Configuration

**configure > sccp-network** *id_number*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sccp-network-sccp_id)#
```

**Syntax Description**

**associate ss7-routing-domain** *rd_id*
no associate

**no**

Removes the association with the SS7 routing domain from the system configuration.

***rd_id***

This number identifies an already defined SS7 routing domain.

*rd_id:* enter an integer from 1 through 12.

**Usage Guidelines**

Use this command to associate SS7 routing domain configurations with SCCP network configurations.

**Example**

The following command associates the SCCP network with SS7 routing domain 2:

**associate ss7-routing-domain** *2*

# description

This command defines a string that describes the SCCP network. The description is used for operator reference.



**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

**Product**

SGSN

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SCCP Network Configuration

**configure > sccp-network** *id_number*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sccp-network-sccp_id)#
```

**Syntax Description**

**description** *string*
**no description**

***string***

This is a string to describe the SCCP network.

*string* must be an alphanumeric string from 1 through 127 characters in length. If there are spaces in the string the string must be enclosed in double-quotes. For example; "This is a Description".

**no**

Removes the description from the system configuration.

**Usage Guidelines**

Use this command to configure a description of this SCCP service for operator reference.

**Example**

The following command sets the description to "This is the SCCP Service Number 1":

```
description "This is the SCCP Service Number 1."
```

# destination

This command configures the SCCP network destination information. Use this command multiple times to set all of the destination information required.



**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

**Product**

SGSN

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SCCP Network Configuration

**configure > sccp-network** *id_number*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sccp-network-sccp_id)#
```

**Syntax Description**

**destination dpc** *pt_code* **{ name** *route_name* **| next-hop** *pt_code* **[ priority** *priority* **] | ssn** *subsys_num* **| version** *sccp_ver* **}**

**no destination dpc** *p_code* **[ name** *route_name* **| ssn** *ssn_num* **| version** *sccp_ver* **]**

**no**

Deletes the specified destination information from the SCCP network configuration.

**dpc *pt_code***

Specifies the SCCP destination point code.

*pt_code:* Must be in SS7 point code dotted-decimal ###.###.### format or decimal ######## format.

**name *route_name***

The name of the SCCP destination route.

*route_name:* enter an alphanumeric string from 1 through 64 characters in length.

**next-hop *pt_code* [ priority *priority***

Associates the next destination defined in the SS7 routing domain and assigns the next-hop a priority for use.

*pt_code:* Must be in SS7 point code dotted-decimal ###.###.### format or decimal ######## format.

*priority:* Must be an integer from 0 to 15, with 0 setting the highest priority.

**ssn *subsys_num***

The destination subsystem number.

*subsys_num:* enter an integer from 1 through 255.

**version *sccp_ver***

*sccp_ver:* enter one of the following to select the SCCP variant:

- ANSI88
- ANSI92
- ANSI96
- BELL05
- CHINA
- GSM0806
- ITU88
- ITU92
- ITU96

## Usage Guidelines

Use this command to configure the destination information for the SCCP network.

### Example

The following commands set the name of the destination route to default_route, the subsystem number to 1, and the variant version to ITU96, all with a destination point code of 1:

```
destination dpc 1 name default_route
destination dpc 1 ssn 1
destination dpc version ITU96
```

# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** SGSN

HNB-GW

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
end
```

**Usage Guidelines** Return to the Exec mode.

# exit

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

**Product**

SGSN

HNB-GW

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**exit**

**Usage Guidelines**

Return to the global configuration mode.

# global-title-translation

This command associates a GTT address-map with this SCCP network.



**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

**Product**

SGSN

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SCCP Network Configuration

**configure > sccp-network** *id_number*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-sccp-network-`*`sccp_id`*`)#`

**Syntax Description**

**global-title-translation address-map instance** *instance*
**no global-title-translation address-map instance** *instance*

**no**

Deletes the GTT address-map instance associated with this SCCP network.

***instance***

This value uniquely identifies a specific previously defined instance of a GTT address-map.

*instance:* enter an integer from 1 to 4096.

**Usage Guidelines**

Use this command to link a GTT address-map, configured with the GTT Address Map configuration mode, to a specific SCCP network configuration.

### Example

**global-title-translation address-map instance** *gtt-map1*

# hop-count

This command specifies the hop count for this SCCP network.



**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

## Product

SGSN

HNB-GW

## Privilege

Security Administrator, Administrator

## Command Modes

Exec > Global Configuration > SCCP Network Configuration

**configure > sccp-network** *id_number*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-sccp-network-sccp_id)#`

## Syntax Description

**hop-count** *hop_cnt*
**default hop-count**

### default

Resets the hop-count value to the system default of 5.

### *hop_cnt*

The hop count to assign to this SCCP network.

*hop_cnt:* enter an integer from 1 to 15.

## Usage Guidelines

Use this command to define the hop count for this SCCP network.

### Example

The following command sets the hop count to 3:

**hop-count** *3*

# self-point-code

This command specifies the SS7 point code for this SCCP service.

**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

**Product**

SGSN

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SCCP Network Configuration

**configure > sccp-network** *id_number*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-sccp-network-sccp_id)#`

**Syntax Description**

**self-point-code** *point_code*
**no self-point-code**

**no**

Deletes the configured self point code.

***point_code***

Defines the point code to assign to this SCCP network service.

*point_code:* value entered must adhere to the point code variant selected when the SCCP network instance was defined:

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

**Usage Guidelines**

Use this command to assign the self point code to use for this SCCP service.

**Example**

The following command sets an ITU-based point code for this SCCP service:

**self-pointcode** *4.121.5*

The following command removes the configured self-point code:

```
no self-pointcode
```

# timeout

This command configures the timeout parameters for this SCCP network.

**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

**Product**

SGSN

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SCCP Network Configuration

**configure > sccp-network** *id_number*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-sccp-network-`*`sccp_id`*`)#`

**Syntax Description**

```
timeout { attack-timer | congestion-timer | conn-est-timer | crd-timer |
 decay-timer | iar-timer | ias-timer | interval-timer | reassembly-timer
 | release-timer | repeat-release-timer | reset-timer | sst-timer } +
default timeout
no timeout timer
```

**attack-timer *time***

Defines the time before the attack timer expires.

*time:* enter an integer between 1 and 10.

**congestion-timer *time***

Defines the time before the congestion timer expires.

*time:* enter an integer between 1 and 10.

**conn-est-timer *time***

Defines the time before the connection timer expires.

*time:* enter an integer between 6 and 12.

**crd-timer *time***

Defines the time before the coordinated-state-change timer expires.

*time:* enter an integer between 60 and 120.

**decay-timer *time***

Defines the time before the decay timer expires.

*time:* enter an integer between 1 and 10.

**iar-timer *time***

Defines the time before the inactivity-receive timer expires.

*time:* enter an integer between 60 and 120.

**ias-timer *time***

Defines the time before the inactivity-send timer expires.

*time:* enter an integer between 30 and 60.

**interval-timer *time***

Defines the time before the interval timer expires.

*time:* enter an integer between 6 and 12

**reassembly-timer *time***

Defines the time before the reassembly-timer expires.

*time:* enter an integer between 10 and 20.

**release-timer *time***

Defines the time before the release-assembly timer expires.

*time:* enter an integer between 1 and 2.

**repeat-release-timer *time***

Defines the time before repeat-release timer expires.

*time:* enter an integer between 1 and 2

**reset-timer *time***

Defines the amount of time before the reset timer expires.

*time:* enter an integer between 1 and 2

**sst-timer *time***

Defines the amount of time before the subsystem status test timer expires.

*time:* enter an integer between 5 and 1200.

**default**

Resets the timeout parameter to the system default.

**no**

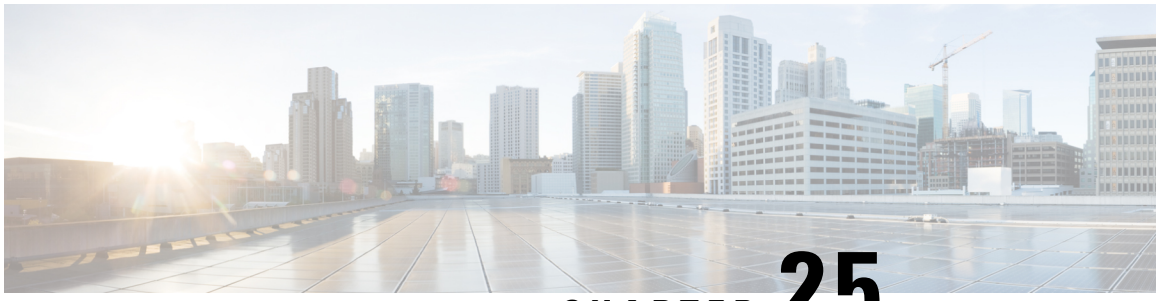
Deletes the specified timer configuration.

## Usage Guidelines

Use this command to assign timeout timers and timeout values for this SCCP service.

### Example

```
timeout reset-timer 75
```



CHAPTER 25

# SCTP Parameter Template Configuration Mode Commands

This chapter provides information about commands used to configure parameters for Stream Control Transmission Protocol (SCTP) associations. The commands become part of a template that can be associated with services running on the system.

**Command Modes**

Exec > Global Configuration > SCTP Parameter Template Configuration

**configure > sctp-param-template** *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

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


- do show, on page 214
- end, on page 214
- exit, on page 214
- sctp-alpha, on page 215
- sctp-alt-accept-flag, on page 215
- sctp-beta, on page 216
- sctp-checksum-type, on page 217
- sctp-cookie-life, on page 218
- sctp-max-assoc-retx, on page 218
- sctp-max-in-strms, on page 219
- sctp-max-init-retx, on page 220
- sctp-max-mtu-size, on page 220
- sctp-max-out-strms, on page 221
- sctp-max-path-retx, on page 222
- sctp-min-mtu-size, on page 223
- sctp-rto-initial, on page 224
- sctp-rto-max, on page 224
- sctp-rto-min, on page 225

- sctp-sack-frequency, on page 226
- sctp-sack-period, on page 226
- sctp-start-mtu-size, on page 227
- timeout, on page 228


# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character | is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
end
```

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# sctp-alpha

Configures the SCTP retransmission timeout (RTO) alpha value.

**Product** MME

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > SCTP Parameter Template Configuration

**configure > sctp-param-template** *template_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(sctp-param-template)#`

**Syntax Description**

**sctp-alpha** *value*
**default sctp-alpha**

**default**

Returns the command to its default setting of 5.

***value***

Default: 5

Specifies the SCTP retransmission timeout alpha value. *value* must be an integer from 0 through 65535.

**Usage Guidelines** Use this command to configure the SCTP RTO alpha value. The RTO alpha value is used in calculating the smoothed round-trip time (SRTT) and the round-trip time variation (RTTVAR) for new round trip time (RTT) measurements.

**Example**

The following command sets the SCTP RTO alpha value to *10*:

**sctp-alpha 10**

# sctp-alt-accept-flag

Configures the SCTP alternate accept flag for additional life time for the association.

**Product** MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > SCTP Parameter Template Configuration

**configure > sctp-param-template** *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax Description**

**sctp-alt-accept-flag { disable | enable }**
**default sctp-alt-accept-flag**

**default**

Returns the command to its default setting of enable.

**disable | enable**

Specifies if the alternate accept flag is enabled or disabled.

**Usage Guidelines**

Use this command to configure the SCTP alternate accept flag for additional life time for the association.

**Example**

The following command disables the alternate accept flag for the SCTP association:

**sctp-alt-accept-flag disable**

# sctp-beta

Configures the SCTP retransmission timeout (RTO) beta value.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > SCTP Parameter Template Configuration

**configure > sctp-param-template** *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax Description**

**sctp-beta** *value*
**default sctp-beta**

**default**

Returns the command to its default setting of 10.

***value***

Specifies the SCTP retransmission timeout beta value as an integer from 0 through 65535. Default: 10

**Usage Guidelines**

Use this command to configure the SCTP RTO beta value. The RTO beta value is used in calculating the smoothed round-trip time (SRTT) and the round-trip time variation (RTTVAR) for new round trip time (RTT) measurements.

**Example**

The following command sets the SCTP RTO beta value to *20*:

```
sctp-beta 20
```

# sctp-checksum-type

Configures the checksum type used to increase the integrity of the SCTP packets during transmission.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > SCTP Parameter Template Configuration

**configure > sctp-param-template** *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax Description**

```
sctp-checksum-type { adler32 | crc32 }
default sctp-checksum-type
```

**default**

Returns the command to its default setting of CRC32.

**adler32 | crc32**

Specifies the type of checksum used to increase data integrity of SCTP packets.

**adler32**: Specifies that the Adler-32 checksum algorithm is used to increase data integrity for SCTP packets.

**crc32**: Specifies that a 32-bit cyclic redundancy check is used to increase data integrity of SCTP packets.

**Usage Guidelines**

Use this command to select the checksum for data integrity of SCTP packets.

**Example**

The following command enables the Adler-32 checksum algorithm used to increase data integrity of SCTP packets:

```
sctp-checksum-type adler32
```

# sctp-cookie-life

Configures the lifetime of the SCTP cookie.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > SCTP Parameter Template Configuration

**configure > sctp-param-template** *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax Description**

**sctp-cookie-life** *value*
**default sctp-cookie-life**

**default**

Returns the command to its default setting of 600 (60000 milliseconds).

***value***

Default: 600 (60000 milliseconds)

Specifies the lifetime of the SCTP cookie. *value* is an integer from 50 through 1200. The range translates to 5000 milliseconds to 120000 milliseconds, as the granularity is in 100-millisecond increments.

**Usage Guidelines**

Use this command to configure the lifetime of the SCTP cookie.

**Example**

The following command configures the lifetime of the SCTP cookie to 80000 milliseconds:

```
sctp-cookie-life 800
```

# sctp-max-assoc-retx

Configures the maximum number of retransmissions for SCTP associations.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > SCTP Parameter Template Configuration

**configure > sctp-param-template** *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax Description**

**sctp-max-assoc-retx** *value*
**default sctp-max-assoc-retx**

**default**

Returns the command to its default setting of 10.

***value***

Specifies the maximum number of retransmissions allowed by this template for SCTP associations as an integer from 0 through 255. Default: 10

**Usage Guidelines**

Use this command to configure the maximum number of retransmissions allowed.

**Example**

The following command configures the maximum number of retransmissions to *7*:

**sctp-max-assoc-retx 7**

# sctp-max-in-strms

Configures the maximum number of incoming SCTP streams.

**Product**

MME

SGSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > SCTP Parameter Template Configuration

**configure > sctp-param-template** *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax Description**

**sctp-max-in-strms** *value*
**default sctp-max-in-strms**

**default**

Returns the command to its default setting of 16.

***value***

Specifies the maximum number of incoming SCTP streams as an integer from 1 through 16. Default: 16.

The MME restricts the allowable range as 2-16. If a value of 1 is entered, value 2 will be applied for any MME service associated with this SCTP parameter template.

**Usage Guidelines** Use this command to configure the maximum number of incoming SCTP streams.

#### Example

The following command configures the maximum number of incoming SCTP streams to *5*:

```
sctp-max-in-strms 5
```

# sctp-max-init-retx

Configures the maximum number of retransmissions for SCTP initiations.

**Product** MME

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > SCTP Parameter Template Configuration

**configure > sctp-param-template** *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax Description**

```
sctp-max-init-retx value
default sctp-max-init-retx
```

#### default

Returns the command to its default setting of 5.

#### *value*

Specifies the maximum number of retransmissions for SCTP initiations as an integer from 0 through 255. Default: 5

**Usage Guidelines** Use this command to configure the maximum number of retransmissions for SCTP initiations.

#### Example

The following command configures the maximum number of retransmissions for SCTP initiations to *10*:

```
sctp-max-init-retx 10
```

# sctp-max-mtu-size

Configures the maximum transmission unit (MTU) size (in bytes) for SCTP streams.

**Product** MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > SCTP Parameter Template Configuration

**configure > sctp-param-template** *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax Description**

**sctp-max-mtu-size** *bytes*
**default sctp-max-mtu-size**

**default**

Returns the command to its default setting of 1500 bytes.

***bytes***

Specifies the maximum MTU size (in bytes) for SCTP streams as an integer from 508 through 65535. Default: 1500.

In the StarOS 21.17.17 release, the maximum MTU size (in bytes) for SCTP streams as an integer is from 512 through 65535. Default: 1500.

**Usage Guidelines**

Use this command to configure the maximum MTU size, in bytes, for SCTP streams.

**Note** To modify the **sctp-max-mtu-size** value, follow the steps in the maintenance mode:

1. Un configure and configure back the SCTP association from Diameter endpoint.
2. Reset the Diameter peer with the CLI **diameter reset connection endpoint***endpoint name*.

**Example**

The following command configures the maximum MTU size for SCTP streams to *3000*:

```
sctp-max-mtu-size 3000
```

# sctp-max-out-strms

Configures the maximum number of outgoing SCTP streams.

**Product**

MME

SGSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > SCTP Parameter Template Configuration

**configure > sctp-param-template** *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax Description**

**sctp-max-out-strms** *value*
**default sctp-max-out-strms**

**default**

Returns the command to its default setting of 2.

***value***

Specifies the maximum number of outgoing SCTP streams as an integer from 1 through 16.

MME Default 16.

SGSN Default: 2.

**Usage Guidelines**

Use this command to configure the maximum number of outgoing SCTP streams.

The MME restricts the allowable range as 2-16. If a value of 1 is entered, value 2 will be applied for any MME service associated with this SCTP parameter template.

For the SGSN, if the user tries to configure the value of **sctpmax-out-strms** less than "2", a message is displayed and the default value is set.

**Example**

The following command configures the maximum number of outgoing SCTP streams to *5*:

**sctp-max-out-strms 5**

# sctp-max-path-retx

Configures the maximum number of retransmissions of SCTP paths.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > SCTP Parameter Template Configuration

**configure > sctp-param-template** *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax Description**

**sctp-max-path-retx** *value*
**default sctp-max-path-retx**

**default**

Returns the command to its default setting of 5.

***value***

Specifies the maximum number of retransmissions of SCTP paths as an integer from 0 through 255. Default: 5

**Usage Guidelines**

Use this command to configure the maximum number of retransmissions of SCTP paths. An SCTP path is a connection between an endpoint address and a peer endpoint address.

**Example**

The following command configures the maximum number of retransmissions of SCTP paths to *10*:

```
sctp-max-path-retx 10
```

# sctp-min-mtu-size

Configures the minimum maximum transmission unit (MTU) size (in bytes) for SCTP streams.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > SCTP Parameter Template Configuration

**configure > sctp-param-template** *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax Description**

**sctp-min-mtu-size** *bytes*
**default sctp-min-mtu-size**

**default**

Returns the command to its default setting of 508 bytes.

***bytes***

Specifies the minimum MTU size (in bytes) for SCTP streams as an integer from 508 through 65535. Default: 508

**Usage Guidelines**

Use this command to configure the minimum MTU size, in bytes, for SCTP streams.

**Example**

The following command configures the minimum MTU size for SCTP streams to *1000*:

```
sctp-min-mtu-size 1000
```

# sctp-rto-initial

Configures the initial time for SCTP retransmission timeouts (RTOs).

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > SCTP Parameter Template Configuration

**configure > sctp-param-template** *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax Description**

**sctp-rto-initial** *value*
**default sctp-rto-initial**

**default**

Returns the command to its default setting of 30 (3000 milliseconds).

***value***

Specifies the initial time for SCTP RTO as an integer from 1 through 1200. The granularity is in 100ms increments (20 = 2000ms). Default: 30 (3000 milliseconds)

**Usage Guidelines**

Use this command to configure the initial time for SCTP RTOs.

**Example**

The following command configures the initial SCTP RTO to 6000ms:

```
sctp-rto-initial 60
```

# sctp-rto-max

Configures the maximum time for SCTP retransmission timeouts (RTOs).

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > SCTP Parameter Template Configuration

**configure > sctp-param-template** *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax Description**

**sctp-rto-max** *value*
**default sctp-rto-max**

**default**

Returns the command to its default setting of 600 (60000 milliseconds).

***value***

Specifies the maximum time for SCTP RTOs as an integer from 5 through 1200. The granularity is in 100ms increments (120 = 12000ms). Default: 600 (60000 milliseconds)

**Usage Guidelines**

Use this command to configure the maximum time for SCTP RTOs.

**Example**

The following command configures the maximum time for SCTP RTOs to 120000ms:

**sctp-rto-max 120**

# sctp-rto-min

Configures the minimum SCTP retransmission timeout (RTO).

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > SCTP Parameter Template Configuration

**configure > sctp-param-template** *template_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(sctp-param-template)#`

**Syntax Description**

**sctp-rto-min [ units-10ms ]** *value*
**default sctp-rto-min**

**default**

Returns the command to its default setting of 10 (1000 milliseconds).

**units-10ms**

Including this keyword specifies that the integer *value* is to be calculated using 10ms increments (instead of 100ms increments) to allow for finer granularity. *value* is an integer from 0 through 500.

***value***

Specifies the minimum time for SCTP RTOs as an integer from 1 through 50. The granularity is in 100ms increments (20 = 2000ms). Default: 10 (1000 milliseconds)

**Usage Guidelines** Use this command to configure the minimum time for SCTP RTOs.

**Example**

The following command configures the minimum time for SCTP RTOs to 2000ms:

```
sctp-rto-min 20
```

# sctp-sack-frequency

Configures the frequency of transmission of SCTP selective acknowledgements (SACK).

**Product** MME

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > SCTP Parameter Template Configuration

**configure > sctp-param-template** *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax Description**

```
sctp-sack-frequency value
default sctp-sack-frequency
```

**default**

Returns the command to its default setting of 2.

***value***

Specifies the frequency of SCTP selective acknowledgements as an integer from 1 through 20. Default: 2

**Usage Guidelines** Use this command to configure the frequency of SCTP selective acknowledgements.

**Example**

The following command configures the frequency of SCTP selective acknowledgements to 10:

```
sctp-sack-frequency 10
```

# sctp-sack-period

Configures the delay before sending an SCTP selective acknowledgement (SACK).

**Product** MME

**Privilege** Administrator

**Command Modes**

Exec > Global Configuration > SCTP Parameter Template Configuration

**configure > sctp-param-template** *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax Description**

**sctp-sack-period [ units-10ms ]** *value*
**default sctp-sack-period**

**default**

Returns the command to its default setting of 2 (200 milliseconds).

**units-10ms**

Including this keyword specifies that the integer *value* is to be calculated using 10ms increments (instead of 100ms increments) to allow for finer granularity. *value* is an integer from 0 through 50.

***value***

Specifies the period for SCTP selective acknowledgements as an integer from 0 through 5. The granularity is in 100ms increments (3 = 300ms). Default: 2 (200 milliseconds).



**Important** If this value is set to 0, the MME service will automatically configure a 10 ms sack period in order to allow proper initialization of the CCPU SCTP stack.

**Usage Guidelines**

Use this command to configure the period for SCTP selective acknowledgements.

**Example**

The following command configures the period for SCTP selective acknowledgements to 400ms (using the 10ms granularity):

```
sctp-sack-period units-10ms 40
```

# sctp-start-mtu-size

Configures the start maximum transmission unit (MTU) size (in bytes) for SCTP streams.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > SCTP Parameter Template Configuration

**configure > sctp-param-template** *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax Description**

**sctp-start-mtu-size** *bytes*
**default sctp-start-mtu-size**

**default**

Returns the command to its default setting of 1500 bytes.

***bytes***

Specifies the start MTU size (in bytes) for SCTP streams as an integer from 508 through 65535. Default: 1500

**Usage Guidelines**

Use this command to configure the start MTU size, in bytes, for SCTP streams.

**Example**

The following command configures the start MTU size for SCTP streams to *3000*:

**sctp-start-mtu-size 3000**

# timeout

Configures timeouts for SCTP data chunk bundle transmissions and/or SCTP heartbeat request responses.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > SCTP Parameter Template Configuration

**configure > sctp-param-template** *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax Description**

**timeout { sctp-bundle [ units-10ms ]** *timer* **| sctp-heart-beat** *value* **}**
**[ default | no ] timeout { sctp-bundle | sctp-heart-beat }**

**default**

Returns the command to its default setting of disabled for **sctp-bundle** and 30 seconds for **sctp-heart-beat**.

**no**

Removes the selected configuration.

**sctp-bundle [ units-10ms ]** ***timer***

Specifies that SCTP data chunks are to be queued until this timer expires at which time the data chunks are bundled and committed for transmission.

*timer* is an integer from 1 through 65535, in 100ms increments (10 = 1000ms or 1 second).

**[ units-10ms ]**: Including this optional keyword specifies that the integer *timer* is to be calculated using 10ms increments (instead of 100ms increments) to allow for finer granularity.

Default: Disabled.

**sctp-heart-beat *value***

Default: 30 seconds

Specifies the SCTP heartbeat timeout (in seconds) as an integer from 1 through 300. An SCTP heartbeat is sent to a peer to determine reachability. If an acknowledgement is not received before this timer runs out, heartbeat requests are no longer sent and the peer is considered unreachable.

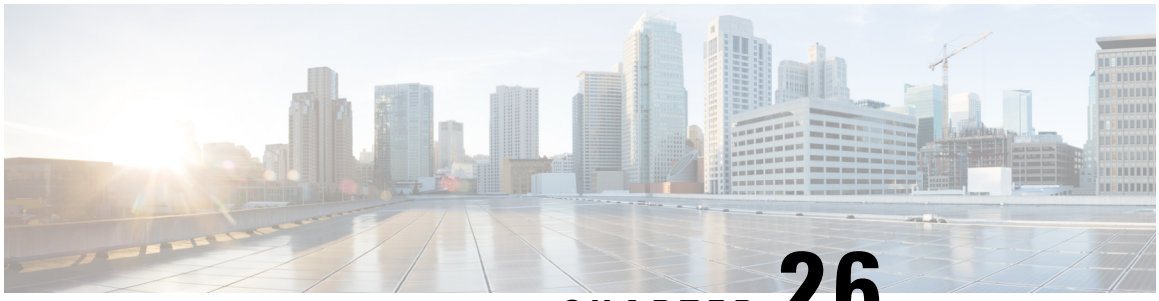
## Usage Guidelines

Use this command to configure timeouts for SCTP data chunk bundle transmissions and/or SCTP heartbeat request responses.

### Example

The following command enables the SCTP data chunk bundle timeout value and configures it to 2 seconds:

```
timeout sctp-bundle 20
```



CHAPTER 26

# Security Configuration Mode Commands

The Security configuration mode is a sub-mode of the Global Configuration mode. This sub-mode enables you to define or modify the connection with the Talos Intelligence content-filtering server and configure URL categorization parameters.

**Command Modes**

Exec > Global Configuration > Security Configuration

**configure > security**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-security)#
```

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


- category, on page 231
- end, on page 232
- exit, on page 232
- server, on page 232


# category

Adds or removes a URL categorization server.

**Important** This is a license-controlled feature. For more information, contact your Cisco account or support representative.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Security Configuration

**configure > security**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-security)#
```

**Syntax Description** **`[ no ] category server`** *server_name*

**no**

Removes the specified URL categorization server.

***server_name***

Specifies the name of the URL categorization server. *server_name* must be an alpha and/or numberic string from 1 through 31 characters that is case sensitive.

**Usage Guidelines** Use this command to create or remove a URL categorization server from the Security configuration mode.

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`end`**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`exit`**

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

# server

This command creates or specifies a Talos Security Intelligence (TSI) server entry and enters the TSI Server Configuration mode.



**Important** This is a license-controlled feature. For more information, contact your Cisco account or support representative.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Security Configuration

**configure > security**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-security)#
```

**Syntax Description**

**`[ no ] server talos-intelligence`** *`server_name`*

**no**

Removes the specified Talos Security Intelligence server.

***server_name***

Specifies the name of the Talos Security Intelligence server to create, configure, or remove. *server_name* must be an alpha and/or numeric string from 1 through 31 characters that is case sensitive.

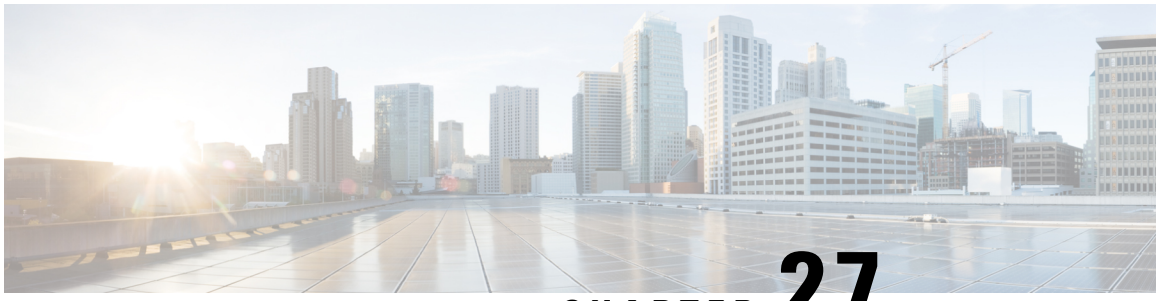
**Usage Guidelines**

Use this command to create, configure, or remove a Talos Security Intelligence server from the Security configuration mode.

Entering this command results in the following prompt:

```
[local]host_name(config-server-tsi)#
```

The various parameters available for configuration of a TSI server entry are defined in the *TSI Server Configuration Mode Commands* chapter.



CHAPTER 27

# Service Chain Configuration Mode Commands

The Service Chain configuration mode is a sub-mode of the Global Configuration mode. This sub-mode associates nsh-format to service-chain.

**Command Modes**

Exec > Global Configuration > Service Chain Configuration

**configure > service-chain**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-service-chain)#
```

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


- end, on page 235
- exit, on page 235
- nsh-format, on page 236


# end

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**end**

**Usage Guidelines**

Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# nsh-format

This command associates nsh format with service-chain.

**Product** P-GW

SAEGW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Service Chain Configuration

**configure > service-chain**

Entering the above command sequence results in the following prompt:

`[local]host_name(config-service-chain)#`

**Syntax Description** **[ no ] nsh-format** *<nsh_format_name>*

**no**

Disassociates nsh format with the service-chain configuration.

**nsh-format**

Associates nsh format with service chain.

***nsh_format_name***

Specifies the name of nsh-format. This is entered as an alphanumeric string of 1 through 63 characters.

**Usage Guidelines** Use this command to associate nsh-format with service-chain.

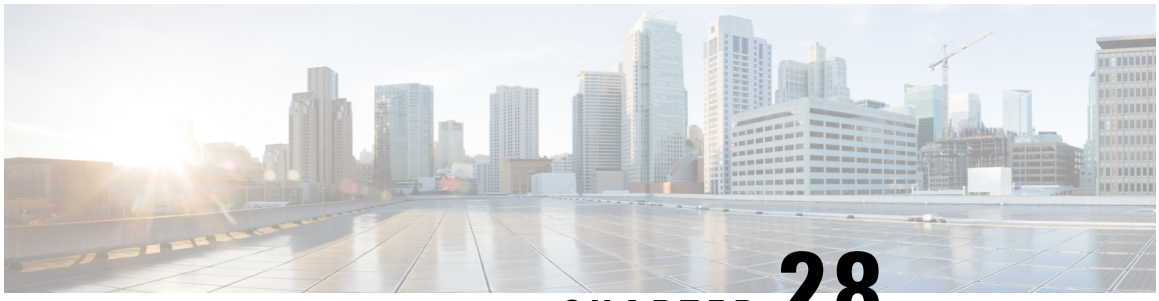
**Example**

The following commands associates a nsh-format to service-chain:

**nsh-format ns1**

The following commands disassociates the nsh-format with service-chain:

**no nsh-format**



CHAPTER 28

# Service Redundancy Protocol Configuration Mode Commands

The Service Redundancy Protocol Mode is used to configure properties for Interchassis Session Recovery (ICSR) services.

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

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

**Important** SRP commands must be identically configured on both the active and standby ICSR chassis.


- advertise-routes-in-standby-state, on page 238
- audit, on page 239
- bfd-mon-ignore-dead-interval, on page 241
- bind, on page 241
- chassis-mode, on page 242
- checkpoint session, on page 243
- configuration-interval, on page 245
- dead-interval, on page 245
- delay-interval, on page 246
- delta-route-modifier, on page 247
- do show, on page 248
- dscp-marking, on page 248
- end, on page 249
- exit, on page 250
- guard-timer, on page 250

- handle-interim-resource-msg, on page 251
- hello-interval, on page 252
- internal-switchover-retry-interval, on page 253
- monitor authentication-probe, on page 254
- monitor bfd , on page 255
- monitor bgp, on page 256
- monitor diameter, on page 257
- monitor hsrp, on page 259
- monitor sx , on page 260
- monitor system, on page 261
- num-internal-switchover-retry, on page 262
- peer-ip-address, on page 263
- priority, on page 264
- retain-complete-sess-info, on page 265
- route-modifier, on page 265
- standby database-recovery, on page 266
- switchover allow-all-data-traffic, on page 267
- switchover allow-early-active-transition, on page 268
- switchover allow-volte-data-traffic, on page 269
- switchover control-outage-optimization, on page 269


# advertise-routes-in-standby-state

Enables advertising BGP routes from an ICSR chassis in standby state.

**Product**

All products that support ICSR

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
advertise-routes-in-standby-state [ hold-off-time hold-off-time ] [
reset-bfd-nbrs bfd-down-time ]
default advertise-routes-in-standby-state [ hold-off-time] [reset-bfd-nbrs]
no advertise-routes-in-standby-state [ hold-off-time] [reset-bfd-nbrs]
```

**default**

Sets the specified route advertisement option to its default value–:

- **hold-off-time** – 30 seconds
- **reset-bfd-nbrs** – ??? milliseconds

**no**

Disables the specified type of route advertisement.

**[ hold-off-time *hold-off-time* ]**

This option delays advertising the BGP routes until the timer expires. Specify *hold-off-time* in seconds as an integer from 1 to 300.

**[ reset-bfd-nbrs *bfd-down-time* ]**

After resetting BFD, this option keeps the BFD sessions down for the configured number of milliseconds to improve network convergence. Specify *bfd-down-time* as an integer from 50 to 120000.

**Usage Guidelines**

Use this command and its keywords to take advantage of faster network convergence accrued from deploying BGP Prefix Independent Convergence (PIC) in the Optical Transport Network Generation Next (OTNGN).

BGP PIC is intended to improve network convergence which will safely allow for setting aggressive ICSR failure detection timers.

**Example**

The following command enables route advertisement from a standby ICSR chassis after a 40-second delay and will suppress BFD sessions for 50 milliseconds following a BFD reset.

```
advertise-routes-in-standby-state hold-off-time 40 reset-bfd-nbrs 50
```

# audit

Sets the start time and periodicity for ICSR Service Redundancy Protocol (SRP) audits. This command can also be used to enter a schedule for running the audit.

**Product**

All products supporting ICSR

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[no] audit cron [ daily hour hour_number minute minute_number ] [ day-of-month
 day_number ] [ month month_number ] [ week-of-day day_name ]
[no] audit daily-start-time hour minute
[no] audit periodicity minutes
default audit periodicity
```

**default**

Resets the specified parameter to its default setting of 60.

**no**

Disables the specified function.

**audit cron [ daily hour *hour_number* minute *minute_number* ] [ day-of-month *day_number* ] [ month *month_number* ] [ week-of-day *day_name* ]**

Configures a cron job (time-based job scheduler) for running the audit. Supported scheduling variables include:

- **daily hour** *hour_number* **minute** *minute_number* – configures the hour and minute of the day when the job will run. Specify *hour_number* as an integer from 0 to 23 and *minute_number* as an integer from 0 to 59.
- **day-of-month** *day_number* – configures the day of the month when the job will run. Specify *day_number* as an integer from 1 to 31.
- **month** *month_number* – configures the month of the year when the job will run. Specify month_number as an integer from 1 to 12.
- **week-of-day** *day_name* – configures the week day on which the job will run. Specify *day_name* as one of the following names: friday, monday, saturday, sunday, thursday, tuesday, or wednesday.

**daily-start-time *hour minute***

Specifies the daily start time. *hour* is a two-digit integer from 00 through 23. *minute* is a two-digit interval from 00 through 59. For example, a start time of 06 00 indicates that the audit will begin at 6:00 AM.

**periodicity *minutes***

Specifies the interval in minutes for generating SRP audit statistics as an integer from 60 through 43200. For example, a periodicity of 90 indicates that SRP audit statistics will be generated every 90 minutes beginning at the specified start time. Default = 60.

## Usage Guidelines

Use this command and its keywords to specify the start time and periodicity for generating ICSR SRP audit statistics.

You can also schedule audits to be run based on time-of-day, day-of-week, day-of-month and month-of-year.

This audit ensures that two ICSR peers are in synch and identifies any discrepancies prior to scheduled or unscheduled switchover events.

### Example

The following command sequence specifies a start time of midnight and a periodicity of every two hours for generating SRP statistics:

```
audit daily-start-time 06 00
audit periodicity 90
```

The following command schedules the audit to run at midnight every Sunday.

```
cron daily hour 0 minute 0 week-of-day sunday
```

# bfd-mon-ignore-dead-interval

Causes the standby ICSR chassis to ignore the dead interval and remain in the standby state until all the BFD chassis-to-chassis monitors fail.

**Product**

All products that support ICSR.

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**bfd-mon-ignore-dead-interval**
**default bfd-mon-ignore-dead-interval**

**default**

Disables this feature.

**Usage Guidelines**

Enable this feature in association with BFD chassis-to-chassis monitoring to support more aggressive ICSR failure detection times.

For additional information, see the descriptions of the **dead-interval** and **monitor bfd** commands.

**Example**

The following command enables this feature:

**bfd-mon-ignore-dead-interval**

# bind

Binds the service to the IP address of the local chassis.

**Product**

All products supporting ICSR

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
bind address { ipv4 _address | ipv6_address }
no bind address
```

**no**

Removes the IP bind address.

***ipv4 _address | ipv6_address***

Specifies the system IP address using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Important** Both peers must be using the same address family (IPv4 or IPv6) or the Service Redundancy Protocol (SRP) connection will not be established.

**Usage Guidelines** Defines the IP address of the local chassis defined as part of the ICSR configuration.

**Example**

The following example binds the service to the IP address *10.1.1.1*:

```
bind address 10.1.1.1
```

# chassis-mode

Defines the chassis's operational mode - primary or backup - for ICSR.

**Product** All products supporting ICSR

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
chassis-mode { backup | primary }
default chassis-mode
```

**default**

Resets the chassis mode to the default setting of backup.

**backup**

(Default) Configures the system as the backup chassis operating in standby state.

#### primary

Configures the system as the primary chassis operating in active state.

**Usage Guidelines** Sets the chassis mode (primary or backup) for the system within the framework of ICSR.

#### Example

The following example configures the system as the primary chassis operating in active state

```
chassis-mode primary
```

# checkpoint session

Configures checkpointing parameters between ICSR active and standby chassis.

**Product** All products supporting ICSR

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
checkpoint session compression { lz4 | zlib }
checkpoint session duration { ims-session | non-ims-session } seconds
checkpoint session nack { macro | micro } [ max-response number ]
checkpoint session periodic-interval minutes
default checkpoint session { compression | duration { ims-session |
non-ims-session } | periodic-interval }
no checkpoint session { compression | duration { ims-session |
non-ims-session } | nack { macro | micro } | periodic-interval }
```

#### default

Resets the following checkpoint session parameters to their default values:

- compression = zlib
- duration = 60 seconds
- periodic-interval = 48 minutes

#### no

Disables **compression, duration, nack,** and **periodic-interval** features.

#### compression { lz4 | zlib }

Specifies whether the LZ4 or zlib compression algorithm will be used to compress SRP payload messages.

LZ4 compression is effective only if both chassis are configured with LZ4. If any one chassis has zlib (default) configured, the compression algorithm reverts to zlib. The algorithm is negotiated only during initial socket establishment. Once agreed no more negotiation takes place until the TCP socket connection is reset.

**Important** A change in the configured compression algorithm resets the TCP Link.

**duration { ims-session | non-ims-session } *seconds***

Specifies whether the checkpoint duration is being set for IMS (IP Multimedia Subsystem) or non-IMS sessions. The duration is the amount of time that a call must be active before it is check pointed. and is expressed as an integer from 0 through 65535 (Default = 60).

**nack { macro | micro } [ max-response *number* ]**

Enables a NACK feature for checkpoints. When this feature is enabled, the standby chassis sends a NACK in response to the receipt of a micro-checkpoint (MC) that fails to be successfully applied. The standby chassis will send more NACKs (configurable, default = 3) within a 10-minute window if an FC is not received. NACKs will continue to be sent within the 10-minute reset window until an FC is received and applied, or the configured number of maximum-responses is reached.

**max-response** is the total number NACKs that can be sent within the 10-minute window in response to a failed MC or FC expressed as an integer from 1 through 65535 (Default = 3).

**Note** The time interval window of 10 minutes is not configurable.

**periodic-interval *minutes***

Configures the minimum periodic checkpoint duration in multiples of 12 minutes for sending macro-checkpoints (FCs) from the Active to the Standby chassis. The interval is specified as an integer divisible by 12 in the range from 24 through 1440 (Default = 48 minutes). The interval range for sending full checkpoints is 24 minutes to 24 hours (1140 minutes).

## Usage Guidelines

Sets the type of compression algorithm to be used for SRP payload messages.

Sets the amount of time the chassis waits before check pointing an existing call session. Checkpoints can be separately set for IMS and/or non-IMS sessions.

Enable the NACK feature for handling checkpointing messaging on the Standby chassis.

Configures the interval between the sending of macro-checkpoints (full checkpoints) between the active and standby chassis.

**Important** The **compression**, **nack** and **periodic-interval** keywords will only appear if a special ICSR optimization feature license has been purchased and installed. Contact your Cisco account representative for assistance.

For additional information on ICSR checkpointing, see the *System Administration Guide*.

### Example

The following example configures sets the checkpoint session duration for an IMS session to 6500 seconds:

```
checkpoint session duration ims-session 6500
```

The following command resets the periodic interval for sending full checkpoints to 36 minutes:

```
checkpoint session periodic-interval 36
```

# configuration-interval

Defines the configuration validation interval.

**Product**

All products supporting ICSR

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**configuration-interval** *interval*
**default configuration-interval**

#### default

Resets the configuration interval to the default setting of 3600 seconds.

#### *interval*

Specifies the amount of time (number of seconds) between one configuration validation and the next configuration validation. *interval* must be an integer from 1 through 65535. Default = 3600.

**Usage Guidelines**

This configures the interval between configuration validations of the primary and backup chassis.

### Example

The following example sets the configuration interval to 34 seconds:

```
configuration-interval 34
```

# dead-interval

Defines the timeout interval before a peer is determined to be down.

**Product** All products supporting ICSR

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**dead-interval** *interval*
**default dead-interval**

**default**

Resets the dead interval to the default setting of 30 seconds.

***interval***

Specifies the amount of time (in seconds) for the dead interval. *interval* must be an integer from 1 through 65535. Default = 30.

**Usage Guidelines** This command specifies the amount of time that one chassis waits to receive a communication from a peer before the listening chassis determines that the peer chassis is down.

**Example**

The following example sets the dead interval to 65 seconds:

**dead-interval 65**

# delay-interval

Configures the delay time for starting the dead timer after configuration files are loaded.

**Product** All products supporting ICSR

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**delay-interval** *interval*
**default delay-interval**

**default**

Sets or restores the default value assigned for the specified parameter.

***interval***

Specifies the amount of time (in seconds) for the delay interval. *interval* must be an integer from 1 through 65535.

**Usage Guidelines**

This configures interval for starting the dead timer after configuration files are loaded.

**Example**

The following example sets the delay interval to 65 seconds after the configuration files are loaded:

```
delay interval 65
```

# delta-route-modifier

Specifies the delta used to compute the route modifier difference between the active and standby chassis. This delta is applied only in the standby state. *For Release 15.0 or higher,* it is used in both states.

**Product**

All products supporting ICSR

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**delta-route-modifier** *value*
**default delta-route-modifier**

**default**

Sets or restores the default value assigned for the specified parameter. Default = 1.

***value***

Specifies the value to be used when computing the route-modifier. *value* must be an integer from 1 through 15 (for 21.7 and later releases), or 1 through 7 (for releases prior to 21.7). Default: 1.

**Usage Guidelines**

The delta-route-modifier is used to compute the route modifier difference between active and standby chassis.

**Example**

The following example sets the delta for the route modifier to 2:

```
delta-route-modifier 2
```

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# dscp-marking

Sets DSCP marking values for SRP control and checkpoint (session maintenance) messages.

**Product**

All products supporting ICSR

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**dscp-marking { control | session }** *dscp_value*
**default dscp-marking { control | session }**

**default**

Sets the DSCP value to its default: **be** (Best Effort Per-Hop-Behaviour).

**{ control | session }**

Specifies the SRP message type for which a DSCP value is being set.

- **control** – SRP control messages [originate from vpnmgr]
- **session** – checkpoint messages (session maintenance) [originate from sessmgr]

***dscp_value***

Specifies the DSCP value to be used:

- **af11** – Assured Forwarding Class 1 low drop PHB (Per Hop Behavior)
- **af12** – Assured Forwarding Class 1 medium drop PHB
- **af13** – Assured Forwarding Class 1 high drop PHB
- **af21** – Assured Forwarding Class 2 low drop PHB
- **af22** – Assured Forwarding Class 2 medium drop PHB
- **af23** – Assured Forwarding Class 2 high drop PHB
- **af31** – Assured Forwarding Class 3 low drop PHB
- **af32** – Assured Forwarding Class 3 medium drop PHB
- **af33** – Assured Forwarding Class 3 high drop PHB
- **af41** – Assured Forwarding Class 4 low drop PHB
- **af42** – Assured Forwarding Class 4 medium drop PHB
- **af43** – Assured Forwarding Class 4 high drop PHB
- **be** – Best effort Per-Hop-Behaviour (default)
- **cs1** – Class selector 1 PHB
- **cs2** – Class selector 2 PHB
- **cs3** – Class selector 3 PHB
- **cs4** – Class selector 4 PHB
- **cs5** – Class selector 5 PHB
- **cs6** – Class selector 6 PHB
- **cs7** – Class selector 7 PHB
- **ef** – Expedited Forwarding PHB, for low latency traffic



**Important** If *dscp_value* is set incorrectly, packet drops may occur in intermediate devices.

**Usage Guidelines** Use this command to enable DSCP marking of SRP and checkpoint messages in ICSR environments.

**Example**

The following command sequence sets DSCP marking of control messages to Expedited Forwarding:

```
dcsp-marking control ef
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# guard-timer

Configures the redundancy-guard-period and monitor-damping-period for SRP service monitoring.

**Product** All products supporting ICSR

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
guard-timer { aaa-switchover-timers { damping-period seconds | guard-period
 seconds } | diameter-switchover-timers { damping-period seconds | guard-period
 seconds } | srp-redundancy-timers { aaa  { damping-period seconds |
guard-period seconds } | bgp { damping-period seconds | guard-period seconds }
 | diam  { damping-period seconds | guard-period seconds } }
default guard-timer aaa-switchover-timers { damping-period | guard-period
 }
default guard-timer diameter-switchover-timers { damping-period |
guard-period }
default guard-timer srp-redundancy-timers { aaa { damping-period |
guard-period } | bgp { damping-period | guard-period } | diam  {
damping-period | guard-period } }
```

**default**

Sets the specified guard timer to its default value:

- **damping-period** = 60 seconds
- **guard-period** = 60 seconds

#### aaa-switchover-timers

Sets timers that prevent back-to-back ICSR switchovers due to an AAA failure (post ICSR switchover) while the network is still converging.

#### diameter-switchover-timers

Sets timers that prevent a back-to-back ICSR switchover due to a Diameter failure (post ICSR switchover) while the network is still converging.

#### srp-redundancy-timers

Sets timers that prevent an ICSR switchover while the system is recovering from a local card-reboot/critical-task-restart failure.

#### damping-period *seconds*

Configures a delay time to trigger an ICSR switchover due to a monitoring failure within the guard-period. Specify *seconds* as an integer from 0 to 300.

#### guard-period *seconds*

Configures the local-failure-recovery network-convergence timer. Specify *seconds* as an integer from 0 to 300.

#### { aaa | bgp | diam }

Specifies the type of SRP redundancy timer:

- **aaa** – local failure followed by AAA monitoring failure
- **bgp** – local failure followed by BGP monitoring failure
- **diam** – local failure followed by Diameter monitoring failure

### Usage Guidelines

Use these guard timers to ensure that local failures, such as card reboots and task restarts, do not result in ICSR events which can be disruptive.

#### Example

The following command sets an SRP redundancy AAA guard period of 45 seconds:

```
guard-timer srp-redundancy-timers aaa guard-period 45
```

# handle-interim-resource-msg

Enables the proper handling of version 16.1 SRP Interim Resource messages during an ICSR upgrade from prior releases.

### Product

All products supporting ICSR

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**handle-interim-resource-msg version-16.1**
**no handle-interim-resource-msg version-16.1**

**no**

Disables this feature after it has been enabled. By default this feature is disabled to preserve compatibility with release versions prior to 16.1.

**Usage Guidelines**

Use this feature to properly handle Interim Resource messages when upgrading to StarOS 16.1. If you do not enable this feature, an ICSR configuration may experience PCRF binding problems (5002 error code message) when performing an ICSR upgrade from previous StarOS versions.

**Example**

The following command enables this feature:

**handle-interim-resource-msg version-16.1**

# hello-interval

Defines the lapse time between sending the hello message.

**Product**

All products supporting ICSR

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**hello-interval** *interval*
**default hello-interval**

**default**

Resets the hello interval to the default setting of 10 seconds.

***interval***

Specifies the lapse time (in seconds) between sending the hello message. *interval* must be an integer from 1 through 65535. Default = 10.

**Usage Guidelines**

This command configures the hello interval - the amount of time that lapses between the sending of each hello message. Each chassis sends the other chassis a hello message at the expiration of every hello interval.

**Example**

The following example sets the hello interval to 35 seconds:

```
hello-interval 35
```

# internal-switchover-retry-interval

Defines the interval between internal switchover retries.

**Product**

All products supporting ICSR

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
internal-switchover-retry-interval interval
default internal-switchover-retry-interval
```

**default**

Resets the internal switchover retry interval to the default setting of 60 seconds.

***interval***

Specifies the amount of time (in seconds) between internal switchover retries. *interval* must be an integer from 10 through 120. Default = 60.

**Usage Guidelines**

This configures the interval between internal switchover retries. The system only initiates internal switchovers if Service Redundancy Protocol (SRP) monitoring is configured.



**Important** See the **monitor authentication-probe**, **monitor bgp**, or **monitor diameter** commands for more information on associated SRP monitoring.

### Example

The following example sets the internal switchover retry interval to 34 seconds:

```
internal-switchover-retry-interval 34
```

# monitor authentication-probe

Enables SRP monitoring of the connection between the specified AAA server and the primary chassis.

**Product**

All products supporting ICSR

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**`[ no ] monitor authentication-probe context`** *`context_name`* **`{`** *`ipv4_address`* **`|`** *`ipv6_address`* **`} [ group`** *`group_id`* **`] [ port`** *`port_number`* **`]`**

#### no

Turns off the monitoring.

#### context *context_name*

Identifies the context being used.

*context_name* must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

#### *ipv4 _address* | *ipv6_address*

Defines the IP address of the AAA server to be monitored in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

#### group *group_id*

Defines a Service Redundancy Protocol (SRP) peer group as an integer from 0 through 9. Default = 0.

In an Interchassis Session Recovery (ICSR) configuration, failover would occur if all peers within a group fail.

#### port *port_number*

Identifies a specific AAA server port for the authentication probe. *port_number* must be an integer from 1 through 65535.

**Usage Guidelines**

This command initiates monitoring of the connection between the primary chassis and the specified AAA server through the use of authentication probe packets. If the connection drops, the standby chassis becomes active.

### Example

The following example initiates the connection monitoring between the primary chassis and AAA server *10.2.3.4* at port *1025*:

```
monitor authentication-probe context test1 10.2.3.4 port 1025
```

# monitor bfd

Enables SRP monitoring of the connection between the specified Bidirectional Forwarding Detection (BFD) neighbor and the primary chassis.

**Product**

All products supporting ICSR

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**`[ no ] monitor bfd context`** *`context_name`* **`{`** *`ipv4_address`* **`|`** *`ipv6_address`* **`} { chassis-to-chassis | chassis-to-router }`**

#### no

Disables monitoring.

#### context *context_name*

Identifies the context being used. *context_name* must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

The context refers to where the BFD peer is configured (SRP context).

#### *ipv4 _address* | *ipv6_address*

Defines the IP address of the BFD neighbor to be monitored, entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

It refers to the IP address of the configured BFD (ICSR) peer.

#### chassis-to-chassis | chassis-to-router

**chassis-to-chassis**: BFD runs between primary and backup chassis on non-SRP links.

**chassis-to-router**: BFD runs between chassis and router.

**Usage Guidelines** This command initiates monitoring of the connection between the primary chassis and the specified BFD neighbor in the specified context. If the connection drops, the standby chassis becomes active.



**Important** BFD monitoring must run between chassis-to-chassis or chassis-to-router.

For additional information, see the description of the **bfd-mon-ignore-dead-interval** command.

### Example

The following example initiates the chassis-to-chassis connection monitoring between the primary chassis and BFD neighbor *12.2.1.54*:

```
monitor bfd context test 12.2.1.54 chassis-to-chassis
```

# monitor bgp

Enables SRP monitoring of the connection between the specified Border Gateway Protocol (BGP) peer and the primary chassis.

**Product** All products supporting ICSR

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description** **[ no ] monitor bgp [ context** *context_name* **{** *ipv4_address* **|** *ipv6_address* **} [ group** *group_id* **[ vrf** *vrf_name* **] ] ] [ exclusive-failover ] | [ vrf-srp-validate ]**

#### no

Disables monitoring.

#### context *context_name*

Identifies the context being used. *context_name* must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

#### *ipv4_address* | *ipv6_address*

Specifies the IP address of the BGP peer to be monitored in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**group *group_id***

Defines a Service Redundancy Protocol (SRP) peer group as an integer from 0 through 9. Default = 0.

In an Interchassis Session Recovery (ICSR) configuration, failover would occur if all peers within a group fail (instead of all BGP peers in a context). This option is useful in deployments in which a combination of IPv4 and IPv6 peers are spread across multiple paired VLANs and IPv4 or IPv6 connectivity is lost by all members of a peer group.

**vrf *vrf_name***

Defines the VPN Routing/Forwarding instance as an alphanumeric string of 1 through 63 characters.

**exclusive-failover**

Flags BGP monitor failure on a single BGP peer failure.

On implementing this keyword, the behavior is as follows:

- BGP peer group is Up if any BGP peer in that group is Up.
- Including a BGP peer in group 0 is same as making it non-group (omitting group).
- BGP monitor is down if any BGP peer group or any non-group BGP peer is down.

**vrf-srp-validate**

Enables SRP validation for BGP VRF configuration.

**Usage Guidelines**

This command initiates monitoring of the connection between the primary chassis and the specified BGP peer in the specified context. If the connection drops, the standby chassis becomes active.

**Example**

The following example initiates the connection monitoring between the primary chassis and BGP peer *125.2.1.56*:

```
monitor bgp context test 125.2.1.56
```

# monitor diameter

Enables SRP monitoring of the connection between the specified Diameter server and the primary chassis.

**Product**

All products supporting ICSR

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

## Syntax Description

**[ no ] monitor diameter context** *context_name* **endpoint** *endpoint_name* **[ fqdn** *fqdn* **| group** *group_id* **| peer {** *ipv4_address* **|** *ipv6_address* **} ] [ port** *port_number* **]**

### no

Turns off the monitoring.

### context *context_name*

Identifies the context being used. *context_name* must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

### endpoint *endpoint_name*

Identifies the endpoint being used. *endpoint_name* must be for the Diameter server expressed as an alphanumeric string of 1 through 63 characters.

### fqdn *fqdn*

Identifies a Fully Qualified Domain Name (FQDN). *fqdn* must be for the Diameter server expressed an alphanumeric string of 1 through 127 characters.

### group *group_id*

Defines a Service Redundancy Protocol (SRP) peer group as an integer from 0 through 9. Default = 0.

In an Interchassis Session Recovery (ICSR) configuration, failover would occur if all peers within the specified group fail.

### peer { *ipv4_address* | *ipv6_address* }

Defines the IP address of the Diameter server to be monitored, entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

### port *port_number*

Identifies a specific port to monitor. *port_number* must be the port for the Diameter server and an integer from 1 through 65535.

## Usage Guidelines

This command initiates monitoring of the connection between the primary chassis and the specified Diameter server in the specified context. If the connection drops, the standby chassis becomes active.



**Important** Endpoint name, FQDN, IP address, and port must all match the Diameter protocol configured values for the peer state to be updated.

### Example

The following example initiates the connection monitoring between the primary chassis and the Diameter server on context *test1* and endpoint *end2*:

```
monitor diameter context test1 10.6.7.8 endpoint end2
```

# monitor hsrp

Enables monitoring of the Hot Standby Router Protocol (HSRP) connection between the ASR 9000 Route Switch Processor (RSP) and the StarOS Security Gateway (SecGW) running in a virtual machine on the Virtualized Services Module. HSRP is employed in high availability (HA) SecGW configurations. (ASR 9000 VSM only)

**Product**

SecGW

**Privilege**

System Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**monitor hsrp interface** *if_name* **afi-type** *type* **hsrp-group** *hsrp_group*
**no monitor hsrp**

**no**

Turns off the monitoring.

**interface *if_name***

Specifies the name of an existing RSP interface as an alphanumeric string of 1 through 63 characters.

**afi-type *type***

Specifies the RSP name of an existing Address Family Type (IPv4 or IPv6) as an alphanumeric string of 4 through 15 characters.

**hsrp-group *hsrp_group***

Specifies the RSP name of an existing HSRP Group ID as an integer from 0 through 4095.

**Usage Guidelines**

Use this command to enable monitoring of the HSRP connection between the ASR 9000 RSP and the SecGW running in a virtual machine on the VSM.

This command must be associated with the Service Redundancy Protocol (SRP) context.

A maximum of one HSRP monitor is supported per VPC-VSM instance.



**Important** The above parameters must match those of the HSRP configuration in the ASR 9000 RSP.

### Example

The following command enables monitoring of Cisco HSRP on an ASR 9000 VSM running SecGW in a virtual machine:

```
monitor hsrp interface GigabitEthernet0/1/0/3 afi-type ipv4 hsrp-group 2
```

# monitor sx

Enables or disables Sx monitoring on the Active UP and Standby UP.

**Product**

All products supporting ICSR

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**`[ no ] monitor sx [ { context`** *`context_name`* **`| bind-address {`***`ipv4_address`* **`|`***`ipv6_address`* **`} | { peer-address {`***`ipv4_address`* **`|`** *`ipv6_address`* **`} } ] | [ disallow-switchover-on-peer-monitor-fail [ timeout`** *`seconds`***`] ]`**

#### no

Disables monitoring.

#### context *context_name*

Specifies the context of the Sx service. *context_name* must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

#### bind-address {*ipv4 _address* | *ipv6_address*}

Defines the service IP address of the Sx service entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

#### peer-address {*ipv4 _address* | *ipv6_address*}

Defines the service IP address of the Sx service entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

#### disallow-switchover-on-peer-monitor-fail [ timeout *seconds* ]

Prevents the switchback of the UP to Active state when the working status of the UP to CP link is unknown.

**timeout** *seconds*: Timeout after which the switchback is allowed even if the Sx failure status is not reset in the Standby peer. The valid values range from 0 to 2073600 (24 days).

**Note** Assigning 0 seconds as the the timeout allows unplanned switchover.

If **timeout** keyword is not specified, the Active chassis waits indefinitely for the Sx failure status to be reset in the Standby peer.

The default configuration is to allow unplanned switchover due to Sx monitor failure in all conditions.

**Usage Guidelines** This command enables or disables Sx monitoring on the Active UP and Standby UP.

# monitor system

Enables or disables failure monitoring on the VPC-DI system.

**Product** All products supporting ICSR

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] monitor system card-fail**

**monitor system vpp delay-period** *0-300 seconds*

**no monitor system vpp**

**no**

Disables card fault monitoring.

**card-fail**

Enables card failure monitoring on the VPC-DI system. When configured, the VPN monitor checks the card failure status to assess if it is feasible to trigger an ICSR switchover.

The following scenarios trigger an ICSR switchover on the VPC-DI platform:

- When any Active SF card fails without Standy card.
- During a planned SF card migration failure without a standby card available.

**vpp delay-period { *0-300 seconds*}**

Specifies the delay period in seconds for a switchover, after a VPP failure.

If the delay period is a value greater than zero, then the switchover is initiated after the specified delay period when VPP fails. The last VPP status notification within the delay period is the final trigger for switchover

action. The default value is 0 seconds. When the value is 0, there is an immediate switchover when VPP goes down.

The need for delay is to address the scenario wherein the VPP is temporarily down and the revival is in process. This implies that a switchover may not be necessary.

**Usage Guidelines**

Use this command to enable or disable failure monitoring on the VPC-DI system.

This command is disabled by default.



**Note** This CLI command is *not* supported on the ASR 5500 or VPC-SI platforms. It is supported only on the VPC-DI platform.

### Example

The following command enables card failure monitoring.

```
monitor system card-fail
```

# num-internal-switchover-retry

Defines the number of times an internal switchover would be retried.

**Product**

All products supporting ICSR

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**num-internal-switchover-retry** *retries*
**default num-internal-switchover-retry**

### default

Resets the configuration interval to the default setting of 3 retries.

### *retries*

The number of times an internal switchover would be retried in case of standby chassis. *retries* must be an integer from 1 through 10.

Default: 3

**Usage Guidelines**

This configures the number of times an internal switchover would be retried in case of standby chassis failure to respond or become active.

### Example

The following example sets the retry number to *5*:

```
num-internal-switchover-retry 5
```

# peer-ip-address

Specifies the IP address for the peer chassis.

**Product**

All products supporting ICSR

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
peer-ip-address { ipv4_address | ipv6_address }
no peer-ip-address
```

#### no

Removes the peer IP address of the backup chassis.

#### *ipv4_address* | *ipv6_address*

Specifies the IP address of the backup chassis, entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Important** Both peers must be using the same address family (IPv4 or IPv6) or the Service Redundancy Protocol (SRP) connection will not be established.

**Usage Guidelines**

This command is used to identify the peer chassis in the ICSR configuration. From the primary's perspective, the peer is the backup and from the backup's perspective, the peer is the primary.

### Example

The following example specifies *10.2.3.4* as a backup peer system to the primary system:

```
peer-ip-address 10.2.3.4
```

# priority

Sets the initial ICSR priority of each peer chassis.

**Important** **priority** takes affect only during simultaneous initializing of all chassis in an ICSR configuration, and only if a misconfiguration has both chassis in the same mode (both Primary or both Backup).

**Product**

All products supporting ICSR

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**priority** *priority_value*
**default priority**

**default**

Resets the priority to the default setting of 125.

***priority_value***

Specifies the priority for the chassis. *priority_value* must be an integer from 1 through 255, where 1 is the highest priority. Default = 125.

**Usage Guidelines**

This command determines which chassis transitions to the Active state when all chassis have the same mode configuration. **priority** acts as a tie breaker for the state determination only when all chassis initialize simultaneously. The chassis with the higher priority (lower number) becomes Active, while the chassis with the lower priority (higher number) becomes Standby.

Once chassis become operational (after initialization), if there is an event requiring a chassis change of state, then each chassis returns to its previous state (Active or Standby) after both chassis recover.

**Example**

The following example sets the priority value to 5:

```
priority 5
```

# retain-complete-sess-info

The new CLI command is added to retain complete session information locally when transitioning to the Standby state during a switchover.

**Product**

P-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**retain-complete-sess-info**
**[no] retain-complete-sess-info**

**no**

Disables the command.

**Usage Guidelines**

The new CLI command is added to retain complete session information locally when transitioning to the Standby state during a switchover.

**Example**

The following command retains complete session information when transitioning from Active to Standby state during a switchover:

**retain-complete-sess-info**

# route-modifier

Sets the route modifier for the peer chassis.

**Product**

All products supporting ICSR

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**route-modifier threshold** *threshold_value*
**default route-modifier**

**default**

Resets the route modifier to the default setting of 16.

***threshold_value***

Specifies the value that causes the route-modifier counter to be reset to the initial value. *threshold_value* must be an integer from 2 through 32. Default = 16.

**Usage Guidelines**

This command is used to determine when the route modifier should be reset to its initial value to avoid rollover.

**Example**

The following example sets the route modifier threshold to *10*:

```
route-modifier threshold 10
```

# standby database-recovery

Configures the preferred method of SRP database synchronization on the Standby ICSR chassis.

**Product**

All products supporting ICSR

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
standby database-recovery { aggressive | normal }
default standby database-recovery
```

**default**

Restore SRP database recovery method to normal

**{ aggressive | normal }**

The **normal** (default) method for synchronizing the SRP database requires tens of seconds of delay whenever the TCP connection between the Active and Standby session managers is established. Once the TCP connection is established, heart beat messages are exchanged between both ICSR chassis every 3 seconds. The standby chassis waits for 7 heart beat messages from the active chassis before it is ready to accept data. This causes the significant delay in session manager database synchronization on the standby chassis.

The **aggressive** method for synchronizing the session manager database reduces recovery time in the following scenarios:

- Standby Session Manager crash
- Packet processing card crash on Standby chassis

- Standby chassis crash/reboot
- Temporary loss and recovery of SRP connection

The **aggressive** method reduces the number of heartbeat messages and amount of housekeeping information exchanged between ICSR chassis.

**Usage Guidelines** Use this command to enable a more aggressive method for synchronizing the session manager database on a Standby ICSR chassis.

### Example

The following command enables the aggressive method of session manager database recovery on a standby ICSR chassis:

```
standby database-recovery aggressive
```

# switchover allow-all-data-traffic

Allows all data traffic (VoLTE and non-VoLTE) during switchover transition. This command overwrites the **switchover allow-volte-data-traffic** command if enabled on a P-GW.



**Important** A special ICSR license is required to run this command. Contact your Cisco account representative for additional information.

**Product** P-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
switchover allow-all-data-traffic
no switchover allow-all-data-traffic
```

### no

Disables this feature. The default behavior is to not allow data traffic during switchover.

**Usage Guidelines** Use this command to allow all data traffic (VoLTE and non-VoLTE) during an ICSR switchover. This feature reduces data traffic outage during the switchover.



**Important** This CLI command must be run on both the active and standby chassis to enable this feature.

All data traffic is allowed on the active chassis during flushing and internal auditing. The billing information is reconciled in the background once the flush is complete.

### Example

The following command enables this feature:

```
switchover allow-all-data-traffic
```

# switchover allow-early-active-transition

Enables or disables early transition to active state during an ICSR switchover. By default this feature is disabled.



**Important** A special ICSR license is required to run this command. Contact your Cisco account representative for additional information.



**Important** You must enable the **switchover allow-all-data-traffic** or **allow-volte-data-traffic** (without **maintain accounting**) command on both chassis prior to enabling this command.

**Product**

All products supporting ICSR

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
switchover allow-early-active-transition
no switchover allow-early-active-transition
```

**no**

Disables early transition following an ICSR switchover.

**Usage Guidelines**

Use this command in conjunction with the **switchover allow-all-data-traffic** or **allow-volte-data-traffic** (without **maintain accounting**) command to further reduce data outage during a planned switchover. The outage window is the amount time between initiating an ICSR switchover and when the newly active chassis starts processing data.

### Example

The following command enables this feature:

```
switchover allow-early-active-transition
```

# switchover allow-volte-data-traffic

Allows VoLTE data traffic during ICSR switchover transition.

**Important** A special ICSR license is required to run this command. Contact your Cisco account representative for additional information.

**Product**

P-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
switchover allow-volte-data-traffic [ maintain-accounting ]
```

**[ maintain-accounting ]**

When enabled this option maintains accounting accuracy for VoLTE calls.VoLTE data is allowed on the active chassis after VoLTE accounting statistics are flushed.

**Usage Guidelines**

Use this command to allow VoLTE data traffic during ICSR switchover transition. VoLTE data traffic is allowed on the active chassis during flushing and internal auditing. There may be some billing inaccuracy. Non-VoLTE data traffic is allowed after flushing and the internal audit are completed.

This feature is superseded when the **switchover allow-all-data- traffic** command is enabled.

**Example**

The following command enables this feature:

```
switchover allow-volte-data-traffic maintain-accounting
```

# switchover control-outage-optimization

Optimizes restoration of control traffic (call-setup, modification, deletion) following an ICSR switchover.

**Important** A special ICSR license is required to run this command. Contact your Cisco account representative for additional information.

**Product**

All products supporting ICSR

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

**configure > context** *context_name* **> service-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
switchover control-outage-optimization
no switchover control-outage-optimization
```

**no**

Disables optimization for restoring control traffic following an ICSR switchover.

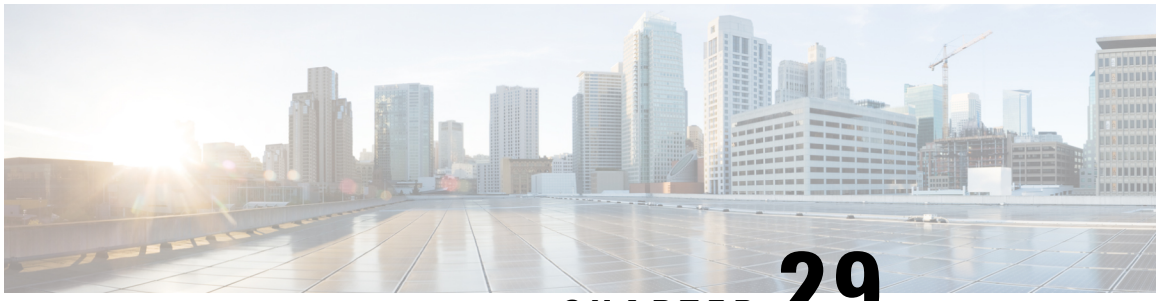
**Usage Guidelines**

Use this command to optimize restoration of control traffic following an ICSR switchover.

### Example

The following command enables this feature:

```
switchover control-outage-optimization
```



CHAPTER 29

# Session Event Module Configuration Mode Commands

**Command Modes**

The Session Event Module Configuration Mode is used to configure how subscriber-specific event data is handled on the S-GW. As users attach, detach, and move through the network, they trigger signaling events that need to be recorded. To provide a per-subscriber level of reporting, the S-GW sends a stream of user event data to an event reporting server over SFTP.

Exec > Global Configuration > Context Configuration > Session Event Module Configuration

**configure > context** *context_name* **> session-event-module**

Entering the above command sequence results in the following prompt:

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

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


- do show, on page 271
- end, on page 272
- event, on page 272
- exit, on page 275
- file, on page 276


# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character | is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# event

Sets the method and destination for transferring event files.

**Product** P-GW

SAEGW

S-GW

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Session Event Module Configuration

**configure > context** *context_name* **> session-event-module**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
event { purge { storage-limit bytes | time-limit seconds } | push-interval
value | push-trigger space-usage-percent trigger_percentage |
remove-file-after-transfer | transfer-mode { pull [ module-only ] | push
 primary { encrypted-url encrypted_url | url url } [ max-files files ] [
module-only ] [ secondary { encrypted-secondary-url url | secondary-url
url } ] [ via local-context ] } | use-harddisk }
default event [ purge | push-interval | push-trigger space-usage-percent
 | remove-file-after-transfer | transfer-mode | file name | rotation
```

```
volume | rotation time | compression | extension  | use-harddisk ]
no event [ purge | remove-file-after-transfer | use-harddisk ]
```

**default**

Configures the default setting for the specified keyword(s):

- **purge**: Not enabled.
- **push-interval**: 300 seconds
- **push-trigger**: 80 percent
- **remove-file-after-transfer**: Disabled
- **transfer mode**: Pull
- **file name**: Specifies the RTT file name where the records are stored.
- **rotation volume**: The volume based on which the RTT file is generated.
- **rotation time**: The time based on which the RTT file is generated.

**Note** The RTT files are pushed to the external server based on the rotation volume or rotation time, whichever occurs first.

- **compression**: Specifies the file compression type. If enabled, the RTT file is generated as a Gzip file, else it is generated as a normal file.
- **extension**: Specifies the RTT file extension (.csv).
- **use-harddisk**: Disabled

**no**

Disables the configured event file storage and processing in this mode:

- **purge**: Disables the deleting of record files on the hard disk based on a storage limit or a time limit.
- **remove-file-after-transfer**: Retains a copy of the file even after it has been pushed or pulled to another server.
- **use-harddisk**: Disables data storage on the system's hard disk.

**purge { storage-limit *bytes* | time-limit *seconds* }**

Configures parameters for deleting event records from the hard drive. This command is not enabled by default.

**storage-limit** *bytes*: Specifies that event records are to be deleted from the hard drive upon reaching a storage limit defined in bytes.

*bytes* must be an integer value from 10485760 to 146800640.

**time-limit** *seconds*: Specifies that event records are to be deleted from the hard drive upon reaching a time limit defined in seconds.

*seconds* must be an integer value from 600 to 2592000.

**push-interval *value***

Default: 300

Specifies the transfer interval (in seconds) when event files will be pushed to an external file server.

*value* must be an integer from 30 through 3600.

**push-trigger space-usage-percent *trigger_percentage***

Default: 80

Specifies the disk space utilization percentage threshold at which an automatic push is triggered and files are transferred to the external server.

*trigger_percentage* must be an integer from 10 through 80.

**remove-file-after-transfer**

Default: Disabled

Specifies that the system must delete event files after they have been transferred to the external file server.

**transfer-mode { pull [ module-only ] | push primary { encrypted-url *encrypted_url* | url *url* } [ max-files *files* ] [ module-only ] [ secondary { encrypted-secondary-url *url* | secondary-url *url* } ] [ via local-context ] }**

Specifies the transfer mode to be used when transferring event files to an external file server.

- **pull**: Specifies that the destination server will pull the event files. This is the default mode.
- **push**: Specifies that the system will push event files to the destination server.
- **primary encrypted-url** *encrypted_url*: Specifies the primary URL location to which the system pushes the files in encrypted format.

  *encrypted_url* must be an alphanumeric string of 1 through 8192 characters.
- **primary url** *url*: Specifies the primary URL location to which the system pushes the event files. *url* must be an alphanumeric string of 1 through 1024 characters in the format: *//user:password@host:[port]/direct*.
- **max-files** *number*: Specifies the maximum number of files that can be transferred per push.

  *number* must be an integer from 4 to 4000.
- **module-only**: Specifies that the transfer of event records is to be applied only to the module type for which the configuration was originally created. If this option is not enabled, the transfer will occur for all record types.
- **secondary encrypted-secondary-url** *url*: Specifies the secondary URL location to which the system pushes the files in encrypted format.

  *url* must be an alphanumeric string of 1 through 8192 characters.
- **secondary-url** *url*: Specifies the secondary URL location to which the system pushes the event files.

  *url* must be an alphanumeric string of 1 through 1024 characters in the format: *//user:password@host:[port]/direct*

- **via local-context**: Specifies that the local context, and, subsequently, the SPIO management ports, will be used to pull or push event files from/to the event server.

### use-harddisk

Default: Disabled

Specifies that the hard disk drive on the SMC is to be used to store P-GW or S-GW event records.

**Usage Guidelines**

Use this command to configure how the P-GW or S-GW event records are moved and stored. By default, records are stored in the PSC RAM where the CDRMOD instance is running.

The **event use-harddisk** command can be run only in a context where CDRMOD is running. Configuring in any other context will result in failure with the message "Failure: Please Check if CDRMOD is running in this context or not."

If push transfer mode is configured, the server URL to which the event files will be transferred must be specified.

When changing the transfer-mode from pull to push, disable the pull setting before changing the transfer mode to push. The push to server URL must be accessible from the local context. Also, make sure that its base directory contains an **event** subdirectory.

After changing the transfer mode from push to pull, enable pull on the destination server. Any ongoing push activity will continue until all the file transfers are completed. If there is no ongoing push activity at the time of this configuration change, the push-related configuration is nullified immediately.

### Example

The following command sets the space usage trigger for pushing files to the event server to 60%:

```
event push-trigger space-usage-percent 60
```

The following command specifies that the event files are to be transferred to a server with the URL of user:password@event-server.com:

```
event transfer-mode pull primary url //user:password@event-server.com
```

# exit

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**exit**

**Usage Guidelines**

Use this command to return to the parent configuration mode.

# file

Sets the format and handling characteristics of event files.

**Product**

P-GW

SAEGW

S-GW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Session Event Module Configuration

**configure > context** *context_name* **> session-event-module**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**file [ compression { gzip | none } ] [ current-prefix** *string* **] [ delete-timeout** *seconds* **] [ directory** *directory_name* **] [ exclude-checksum-record ] [ field-separator { hyphen | omit | underscore } ] [ file-sequence-number rulebase-seq-num ] [ headers ] [ name** *file_name* **] [ reset-indicator ] [ rotation [ num-records** *number* **| time** *seconds* **| volume** *bytes* **] ] [ sequence-number { length** *length* **| omit | padded | padded-six-length | unpadded } ] [ storage-limit** *limit* **] [ time-stamp { expanded-format | rotated-format | unix-format } ] [ trailing-text** *string* **] [ trap-on-file-delete ] [ xor-final-record ] +**
**default file [ compression ] [ current-prefix ] [ delete-timeout ] [ directory ] [ field-separator ] [ file-sequence-number ] [ headers ] [ name ] [ reset-indicator ] [ rotation { num-records | time | volume } ] [ sequence-number ] [ storage-limit ] [ time-stamp ] [ trailing-text ] +**

**default**

Configures the default setting for the specified keyword(s).

**compression { gzip | none }**

Specifies compression of P-GW or S-GW event files.

- **gzip**: Enables GNU zip compression of the event file at approximately 10:1 ratio.
- **none**: Disables Gzip compression.

**current-prefix *string***

Specifies a string to add to the beginning of the event file that is currently being used to store records.

*string* must be an alphanumeric string of 1 through 31 characters. Default: **curr**

**delete-timeout *seconds***

Specifies a time period, in seconds, after which event files are deleted. By default, files are never deleted.

*seconds* must be an integer from 3600 through 31536000. Default: Disabled

**directory *directory_name***

Specifies a subdirectory in the default directory in which to store event files.

*directory_name* must be an alphanumeric string of 1 through 191 characters. Default: **/records/event**

**exclude-checksum-record**

Excludes the final record containing #CHECKSUM followed by the 32-bit Cyclic Redundancy Check (CRC) of all preceding records from the event file.

Default: Disabled, a checksum record is included in the event file header.

**field-separator [ hyphen | omit | underscore ]**

Specifies the type of separators between two fields of an event file name:

- **hyphen**: Specifies the field separator as a "-" (hyphen) symbol between two fields.
- **omit**: Removes or omits the field separator between two fields.
- **underscore**: Specifies the field separator as an "_" (underscore) symbol between two fields.

**file-sequence-number rulebase-seq-num**

Specifies that the file name sequence numbers be unique per rulebase and event format name combination.

**headers**

Includes a file header summarizing the record layout.



**Important** This keyword is not supported for S-GW event reporting.

**name *file_name***

Specifies a string to be used as the base file name for event files.

*file_name* must be an alphanumeric string of 1 through 31 characters. The file name format is as follows:

*base_sequencenum_timestamp* Default: **event**

- *base*: Specifies type of record in file or contains the operator-specified string. Default: **event**
- *sequencenum*: This is a 5-digit sequence number to detect the missing file sequence. It is unique among all event files on the system.
- *timestamp*: Adds a file creation timestamp (UTC time) in MMDDYYYYHHMMSS format.

**reset-indicator**

Specifies the inclusion of the reset indicator counter (value from 0 through 255) in the event file name. The counter is incremented whenever any of the following conditions occur:

- A peer chassis has taken over in compliance with Interchassis Session Recovery (ICSR).
- The sequence number (see **sequence-number** keyword) has rolled over to zero.

**rotation { num-records *number* | time *seconds* | volume *bytes* }**

Specifies when to close an event file and create a new one.

- **num-records** *number*: Specifies the maximum number of records that should be added to an event file. When the number of records in the file reaches this value, the file is complete.

  *number* must be an integer 100 through 10240. Default: 1024

- **time** *seconds*: Specifies the period of time to wait (in seconds) before closing the current event file and creating a new one.

  *seconds* must be an integer from 30 through 86400. Default: 3600

- **volume** *bytes*: Specifies the maximum size of the event file (in bytes) before closing it and creating a new one.

  *bytes* must be an integer from 51200 through 62914560. Note that a higher setting may improve the compression ratio when the compression keyword is set to gzip. Default: 102400

**sequence-number { length *length* | omit | padded | padded-six-length | unpadded }**

Includes with a specified format or excludes the sequence number in the file name.

- **length** *length*: Includes the sequence number with the specified length.

  *length* must be the file sequence number length with preceding zeroes in the file name, and must be an integer from 1 through 9.

- **omit**: Excludes the sequence number from the file name.
- **padded**: Includes the padded sequence number with preceding zeros in the file name. This is the default setting.
- **padded-six-length**: Includes the padded sequence number with six preceding zeros in the file name.
- **unpadded**: Includes the unpadded sequence number in the file name.

Default: **padded**

**storage-limit *limit***

Files will be deleted when the specified amount of space (in bytes) is reached.

*limit* must be an integer from 10485760 through 536870912. Default: 33554432

**time-stamp { expanded-format | rotated-format | unix-format }**

Specifies the format of the file creation timestamp to be included in the file name.

- **expanded-format**: Specifies the UTC (Universal Time Coordinated) MMDDYYYYHHMMSS format.
- **rotated-format**: Specifies the time stamp format to YYYYMMDDHHMMSS format.
- **unix-format**: Specifies the UNIX format of *x.y*, where *x* is the number of seconds since 1/1/1970 and *y* is the fractional portion of the current second that has elapsed.

**trailing-text *string***

Specifies the inclusion of an arbitrary text string in the file name as an alphanumeric string of 1 through 30 characters.

**trap-on-file-delete**

Instructs the system to send an SNMP notification (trap) when an event file is deleted due to lack of space.

Default: Disabled

**xor-final-record**

Specifies inserting an exclusive OR (XOR) checksum (instead of a CRC checksum) into the event file header if the **exclude-checksum-record** is left at its default setting. Default: Disabled

**+**

More than one of the previous keywords can be entered within a single command.

## Usage Guidelines

Use this command to configure event file characteristics.

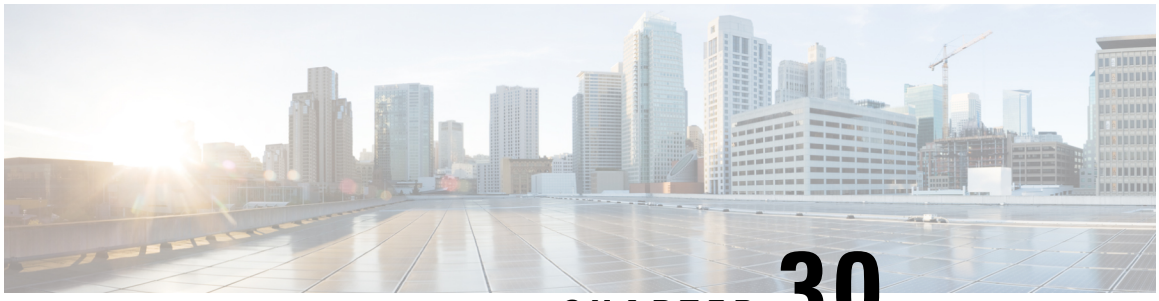
### Example

The following command sets the prefix of the current active event file to *Current*:

```
file current-prefix Current
```

The following command sets the base file name to *Eventfile*:

```
file name Eventfile
```



CHAPTER 30

# Session Priority Profile Configuration Mode Commands

The Session Priority Profile Configuration Mode Commands are used to configure the priority-related parameters for a high-priority session on UPF. These sessions can be a WPS, emergency, or IMS. Based on the configured parameters for a session, the messages are processed or throttled in case of an overload scenario.

**Command Modes**

Exec > Global Configuration > Session Priority Profile Configuration

**configure > session-priority-profile** *spp_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-session-priority)#`


- priority, on page 281


# priority

Configures the priority for a session.

**Product**

UPF

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Session Priority Profile Configuration

**configure > session-priority-profile** *spp_name*

**Syntax Description**

**`priority`** *`priority_value`* **`type { wps | emergency | ims } [ throttle | precedence`** *`precedence_value`* **`]`**

**priority *priority_value***

Specify the priority value of a session.

Must be an integer 0-15.

**type**

Specify the session type.

Must be one of the following:

- wps
- emergency
- ims

**throttle**

Defines the behavior for flows of priority sessions during overload/self-protection state to be throttled.

If **throttle** keyword is configured for a priority, UPF throttles the new flows for this priority session in overload or self-protection state. Therefore, the packets get dropped.

If **throttle** is not mentioned, UPF does not drop any packet for this session.

The default value is "Enabled" in Session-Priority-Profile, if the priority is not configured.

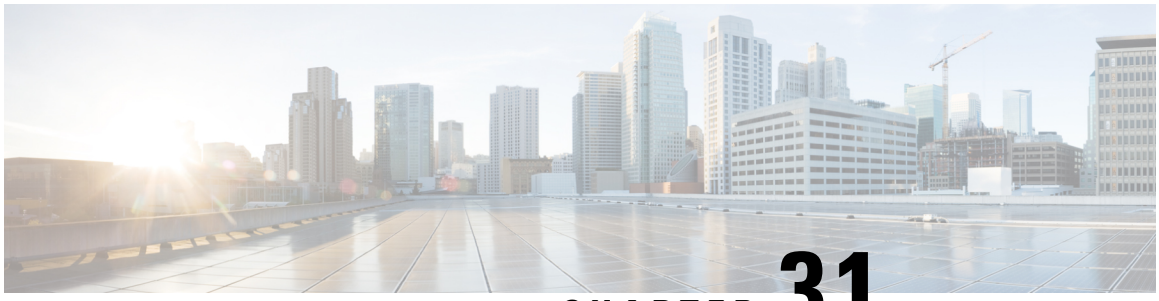
**precedence *precedence_value***

Specify the precedence value.

Must be an integer in the range of 1-4.

## Usage Guidelines

Use this command to configure the priority of a message for a WPS, emergency, or IMS session.



CHAPTER 31

# Session Trace Template Configuration Mode Commands

The commands of the Session Trace Template configuration mode define the various template parameters needed to manage the trace functionality of the Session Trace and Cell Traffic Trace features. These functions are described in your product Administration Guide.

**Command Modes**

Exec > Global Configuration > Session Trace Template Configuration

**configure > template-session-trace network-element { { enb template-name cell-trace } | { { ggsn | hnbgw | mme | pgw | saegw | sgw } template-name** *template_name* **} }**

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-sesstrc-template)#`

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


- archive, on page 283
- disk-limit, on page 284
- do show, on page 285
- end, on page 286
- exit, on page 286
- interface, on page 286
- target-interface, on page 289
- target-ne, on page 291
- trace-extension, on page 293


# archive

This command defines the archive directory capacity and other related parameters.

**Product** MME

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Session Trace Template Configuration

**configure > template-session-trace network-element { { enb template-name cell-trace } | { { ggsn | hnbgw | mme | pgw | saegw | sgw } template-name** *template_name* **} }**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sesstrc-template)#
```

**Syntax Description** **[ no ] archive files** *number_of_files* **size** *size***timer***timer_value*

**files *number_of_files***

Specifies the number of files that go into a directory before it is closed for archiving. The range is an integer from 1 to 10000.

**size**

Specifies the total file size in Megabytes (MB) an Archive Directory can hold. The range is an integer from 1 to 10.

**timer *timer_value***

Specifies the timer expiry limit for files to be collected in the directory after which the pending directories are archived. The timer value is specified in seconds.

**Usage Guidelines** The **archive** command is specific to the Cell Traffic Trace. This command is available under the **cell-trace** template under the eNodeB network element.

The **archive** command is used to archive file directories in a cell traffic tracing procedure. The file directories archived are displayed using a C Type file format. The C Type file includes trace information, which are available in the following fields: IMEI, IMSI, eNodeB identity, UE S1 AP identity and the MME UE S1 AP identity.

**Example**

The following configuration archives 100 files that can be stroed in a diectory of size 2 MB with timer limit of 200 seconds:

```
archive files 100 size 2 timer 200
```

# disk-limit

This command defines the total space reserved for files in the hard-disk.

**Product** MME

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Session Trace Template Configuration

**configure > template-session-trace network-element { { enb template-name cell-trace } | { { ggsn | hnbgw | mme | pgw | saegw | sgw } template-name** *template_name* **} }**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sesstrc-template)#
```

**Syntax Description**

**[ no ] disk-limit** *disk_size*

**no**

Disables its following configured options.

***disk_size***

Specifies the disk reservation size in megabytes (MB). The disk-limit size ranges from 1 MB to 20480 MB. If disk-limit is not configured, a default size of 200 MB is allocated in the hard disk.

**Usage Guidelines**

The **disk-limit** command is specific to Cell Traffic Trace. This command is available under the **cell-trace** template under the eNodeB network element.

The **disk-limit** command defines the total space to be reserved on the hard disk. If disk-limit alone is configured then compression is not considered. However, a default size of 200 MB is allocated in the hard disk for storing Cell Traffic Trace files.

**Example**

The following configuration reserves 100 MB of space in the hard-disk for storing Cell Traffic Trace files:

```
disk-limit 100
```

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**do show**

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`end`**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`exit`**

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

# interface

This command specifies the name of the interface applicable for a specific Network Element (NE) on which subscriber session traces have to be collected.

**Product** GGSN

MME

P-GW

SAEGW

S-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Session Trace Template Configuration

**configure > template-session-trace network-element { { enb template-name cell-trace } | { { ggsn | hnbgw | mme | pgw | saegw | sgw } template-name** *template_name* **} }**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sesstrc-template)#
```

## Syntax Description

**[ no ] interface** *interface_name*

**no**

Disables its following configured options.

***interface_name***

Specifies the interface name for tracing. The available interfaces depend on the **network-element** selected.

**GGSN**. The available **ggsn** interfaces are:

- **all**: Specifies that all interfaces are to be traced.
- **gi**: Specifies that the interface where the trace will be performed is the Gi interface between the GGSN and RADIUS server.
- **gmb**: Specifies that the interface where the trace will be performed is the Gmb interface between the GGSN and BM-SC.
- **gn**: Specifies that the interface where the trace will be performed is the Gn interface between the GGSN and the SGSN.
- **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the GGSN and PCRF.
- **gy**: Specifies that the interface where the trace will be performed is the Gy interface between the GGSN and OCS.

**HNBGW**. The available interfaces for **hnbgw** are as follows:

- **all**: Specifies that all **hnbgw** interfaces are to be traced.
- **iucs**: Specifies that the interface where the trace will be performed is the **iucs** interface between the HNB-GW and the Mobile Switching Centre (3G MSC) in a 3G UMTS Femtocell Access Network.
- **iups**: Specifies that the interface where the trace will be performed is the **iups** interface between the HNB-GW and the SGSN.

**MME**. The available interfaces for **mme** are as follows:

- **all**
- **s10:** Specifies that the interface where the trace will be performed is the S10 interface between the MME and another MME.
- **s11:** Specifies that the interface where the trace will be performed is the S11 interface between the MME and the S-GW.
- **s13:** Specifies that the interface where the trace will be performed is the S13 interface between the MME and the EIR.
- **s1mme:** Specifies that the interface where the trace will be performed is the S1-MME interface between the MME and the eNodeB.
- **s3:** Specifies that the interface where the trace will be performed is the S3 interface between the MME and an SGSN.
- **s6a:** Specifies that the interface where the trace will be performed is the S6a interface between the MME and the HSS.

**PGW**. The available interfaces for **pgw** are as follows:

- **all**: Specifies that all interfaces are to be traced.
- **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.

- **gy**: Specifies that the interface where the trace will be performed is the Gy interface between the P-GW and OCS.
- **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the P-GW and the HSGW.
- **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the P-GW and an ePDG.
- **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the P-GW and a trusted, non-3GPP access device.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between an S-GW and P-GW located within the same administrative domain (non-roaming).
- **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the P-GW and the 3GPP AAA server.
- **s8**: Specifies that the interface where the trace will be performed is the S8 interface -- an inter-PLMN reference point between the S-GW and the P-GW used during roaming scenarios.
- **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the P-GW and the PDN.

**SAEGW**: The available interfaces for the SAEGW are as follows:

- **func-pgw interface**: The following interfaces are available for a configured P-GW under an SAEGW service:
  - **all**: Specifies that all interfaces are to be traced.
  - **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
  - **gy**: Specifies that the interface where the trace will be performed is the Gy interface between the P-GW and OCS.
  - **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the P-GW and the HSGW.
  - **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the P-GW and an ePDG.
  - **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the P-GW and a trusted, non-3GPP access device.
  - **s5**: Specifies that the interface where the trace will be performed is the S5 interface between an S-GW and P-GW located within the same administrative domain (non-roaming).
  - **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the P-GW and the 3GPP AAA server.
  - **s8**: Specifies that the interface where the trace will be performed is the S8 interface -- an inter-PLMN reference point between the S-GW and the P-GW used during roaming scenarios..
  - **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the P-GW and the PDN.
- **func-sgw interface**: The following interfaces are available for a configured S-GW under an SAEGW service:
  - **all**: Specifies that all interfaces are to be traced.
  - **gxc**: Specifies that the interface where the trace will be performed is the Gxc interface between the S-GW and the PCRF.
  - **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the S-GW and the MME.

- **s4**: Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and an SGSN.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the S-GW and the P-GW.
- **s8**: Specifies that the interface where the trace will be performed is the S8 interface between the S-GW and the P-GW.

**SGW**. The available interfaces for the S-GW are as follows:

- **all**: Specifies that all interfaces are to be traced.
- **gxc**: Specifies that the interface where the trace will be performed is the Gxc interface between the S-GW and the PCRF.
- **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the S-GW and the MME.
- **s4**: Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and an SGSN.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the S-GW and the P-GW.
- **s8**: Specifies that the interface where the trace will be performed is the S8 interface between the S-GW and the P-GW.

**Usage Guidelines**

The **interface** command is specific to Session Tracing. This command is available in the template for the MME NE. This command specifies the interfaces for Session Tracing from the MME.

### Example

The following command selects S1-MME as the interface for session tracing:

```
interface s1mme
```

# target-interface

This command specifies the interface for the selected Network Element for session tracing.

**Product**

GGSN

HNBGW

MME

P-GW

SAEGW

S-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Session Trace Template Configuration

**configure > template-session-trace network-element { { enb template-name cell-trace } | { { ggsn | hnbgw | mme | pgw | saegw | sgw } template-name** *template_name* **} }**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sesstrc-template)#
```

## Syntax Description

**target-interface** *interface_name*

***interface_name***

Specifies the interface for the selected Network Element for tracing.

- Available **target-interface** options for **enb** are as follows:
  - **all**
  - **s1mme:** Specifies that the interface where the trace will be performed is the S1-MME interface between the MME and the eNodeB.
  - **uu:** Specifies that the interface where the trace will be performed is the UU interface between the MME and the eNodeB.
  - **x2:** Specifies that the interface where the trace will be performed is the X2 interface between the MME and the eNodeB.
- Available **target-interface** options for **pgw** are as follows:
  - **all**
  - **gx:** Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
  - **s2a:** Specifies that the interface where the trace will be performed is the S2a interface between the PGW and the HSGW.
  - **s2b:** Specifies that the interface where the trace will be performed is the S2b interface between the PGW and an ePDG.
  - **s2c:** Specifies that the interface where the trace will be performed is the S2c interface between the PGW and a trusted, non-3GPP access device.
  - **s5:** Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.
  - **s6b:** Specifies that the interface where the trace will be performed is the S6b interface between the PGW and the 3GPP AAA server.
  - **s8:** Specifies that the interface where the trace will be performed is the S8b interface between the PGW and the S-GW.
  - **sgi:** Specifies that the interface where the trace will be performed is the SGi interface between the PGW and the PDN.
- Available **target-interface** options for **sgw** are as follows:
  - **all**
  - **gxc:** Specifies that the interface where the trace will be performed is the Gx interface between the PGW and the PCRF.
  - **s11:** Specifies that the interface where the trace will be performed is the S11 interface between the MME and the S-GW.
  - **s4:** Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and the SGSN.
  - **s5:** Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.
  - **s8:** Specifies that the interface where the trace will be performed is the S8b interface between the PGW and the S-GW.

**Usage Guidelines**

The **target-interface** specifies the interface for tracing for a specified NE. This keyword is prompted only when a specific Network Element is selected using the **target-ne** command.

**Example**

The following configures session tracing for the network element **pgw** and its S8 interface:

```
target-ne pgw target-interface s8
```

# target-ne

This command initiates tracing towards other network elements.

**Product**

GGSN

HNBGW

MME

P-GW

SAEGW

S-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Session Trace Template Configuration

**configure > template-session-trace network-element { { enb template-name cell-trace } | { { ggsn | hnbgw | mme | pgw | saegw | sgw } template-name** *template_name* **} }**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sesstrc-template)#
```

**Syntax Description**

**[ no ] target-ne { all | { enb | pgw | sgw } [ target-interface** *interface_name* **] }**

**no**

Disables its following configured options.

**all**

Selects all interfaces supported under MME for session trace.

**target-interface *interface_name***

Specifies the interface for the selected Network Element for tracing.

- Available **target-interface** options for **enb** are as follows:
  - **all**

- **s1mme:** Specifies that the interface where the trace will be performed is the S1-MME interface between the MME and the eNodeB.
- **uu:** Specifies that the interface where the trace will be performed is the UU interface between the MME and the eNodeB.
- **x2:** Specifies that the interface where the trace will be performed is the X2 interface between the MME and the eNodeB.

- Available **target-interface** options for **pgw** are as follows:
  - **all**
  - **gx:** Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
  - **s2a:** Specifies that the interface where the trace will be performed is the S2a interface between the PGW and the HSGW.
  - **s2b:** Specifies that the interface where the trace will be performed is the S2b interface between the PGW and an ePDG.
  - **s2c:** Specifies that the interface where the trace will be performed is the S2c interface between the PGW and a trusted, non-3GPP access device.
  - **s5:** Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.
  - **s6b:** Specifies that the interface where the trace will be performed is the S6b interface between the PGW and the 3GPP AAA server.
  - **s8:** Specifies that the interface where the trace will be performed is the S8b interface between the PGW and the S-GW.
  - **sgi:** Specifies that the interface where the trace will be performed is the SGi interface between the PGW and the PDN.

- Available **target-interface** options for **sgw** are as follows:
  - **all**
  - **gxc:** Specifies that the interface where the trace will be performed is the Gx interface between the PGW and the PCRF.
  - **s11:** Specifies that the interface where the trace will be performed is the S11 interface between the MME and the S-GW.
  - **s4:** Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and the SGSN.
  - **s5:** Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.
  - **s8:** Specifies that the interface where the trace will be performed is the S8b interface between the PGW and the S-GW.

## Usage Guidelines

The **target-ne** command is specific to Session Tracing. This command is available in the template for the MME NE. This command initiates tracing towards other network elements. The **target-interface** specifies the interface for tracing for a specified NE.

### Example

The following configures session tracing for the network element **pgw** and its S8 interface:

```
target-ne pgw target-interface s8
```

# trace-extension

This command defines the UE or ENodeB identity extension parameters for C Type file.

**Product**

MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Session Trace Template Configuration

**configure > template-session-trace network-element { { enb template-name cell-trace } | { { ggsn | hnbgw | mme | pgw | saegw | sgw } template-name** *template_name* **} }**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sesstrc-template)#
```

**Syntax Description**

**[ no ] trace-extension enb-id ue-s1ap-id**

**enb-id**

Specifies the Global EnodeB identity.

**ue-s1ap-id**

Specifies the eNodeB UE S1AP Identity and MME UE S1AP Identity

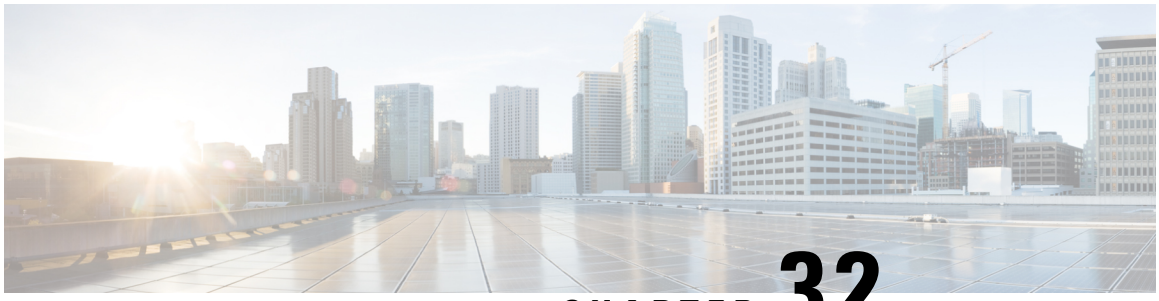
**Usage Guidelines**

The **trace-extension** keyword is used to provide additional cell trace information from the global UE identity, eNodeB UE identity and the MME UE identity fields in the C Type files.

**Example**

The following configuration enables trace extension:

```
trace-extension  enb-id ue-s1ap-id
```



CHAPTER 32

# SGSN ASP Configuration Mode Commands

**Command Modes**

The ASP (application server process) configuration mode defines the M3UA end-point parameters for a specific SS7 routing domain instance. The ASP instance is generated and accessed via the SS7 routing domain configuration mode commands.

Exec > Global Configuration > SS7 Routing Domain Configuration > ASP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> asp instance** *asp_number*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-ss7-rd-`*`ss7rd_id`*`-asp-inst-instance)#`

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


- do show, on page 295
- end, on page 296
- end-point, on page 296
- exit, on page 298


# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**`do show`**

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

Exits the current mode and returns to the Exec Mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Change the mode back to the Exec Mode.

# end-point

This command defines or deletes the IP address and/or port number to be associated with the local SCTP end-point for this ASP. At least one address needs to be configured before the end-point can be activated.

**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

When using the **bind** keyword, this command also activates the end-point once the address has been defined. Once bound, it cannot be reconfigured until it is unbound with the **no end-point bind** command.

**Product** SGSN

HNB-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > SS7 Routing Domain Configuration > ASP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> asp instance** *asp_number*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-asp-inst-instance)#
```

## Syntax Description

```
end-point { address ip_address context context_id | bind | port port_number
 }
no end-point { address ip_address context context_id | bind }
```

**address ip_address context context_id:**

Specifies the IP address and the context associated with the address for this end-point.

ip_address**:** must be defined using the standard IPv4 dotted decimal notation or the colon notation of IPv6.

**context** context_id: a string of 1 to 79 alphanumeric characters to identify the specific context associated with the end-point address.

**bind**

Activates (binds) the end-point.



**Important** Only use **bind** after you have configured other parameters.

**port port_number**

Identifies the M3UA's SCTP port associated with this end-point.

port_number: must be an integer fom 1 to 65535. Default is 2905.

**no**

Removes the end-point configuration or deactivates the end-point.



**Caution** Entering this command will terminate all current subscriber sessions for associated peers.

## Usage Guidelines

Use this command to manage the ASP end-point. Once the ASP end-point is bound the end-point configuration can not be changed until it is unbound.

### Example

Activate the end-point with the following command:

```
end-point bind
```

Deactivate or unbind the end-point with the following command:

```
no end-point bind
```

Set the end-point port to default for ASP 1 with the following command:

```
default asp instance 1 end-point port
```

# exit

Exits the current mode and returns to the previous mode.

**Product**

SGSN

**Privilege**

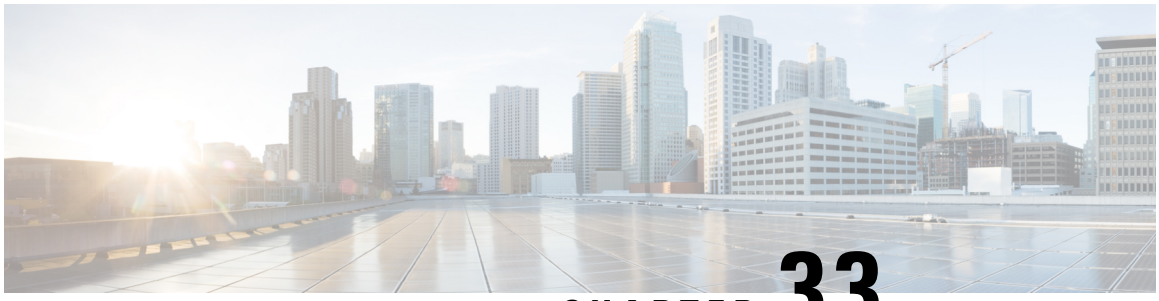
Security Administrator, Administrator

**Syntax Description**

**exit**

**Usage Guidelines**

Returns to the previous mode.



CHAPTER 33

# SGSN Congestion Action Profile Configuration Mode

- active calls
- new calls
- SM messages

For more information about the SGSN's MTC congestion control functionality, refer to the *MTC Congestion Control* section in the *SGSN Administration Guide.*

**Command Modes**

This mode provides the commands to configure the congestion-action-profile, which incorporates the actions to be taken by the SGSN during specified congestion scenario as part of the SGSN's machine type communications (MTC) congestion control reponses for the call/messages events.

Exec > Global Configuration > SGSN Global Configuration > Congestion Control Configuration > Congestion Action Profile Configuration

configure > sgsn-global > congestion-control > congestion-action-profile *act_prof_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-cong-act-prof-act_prof_name)#`

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


- active-call-policy, on page 300
- do show, on page 301
- end, on page 301
- exit, on page 302
- new-call-policy, on page 302
- sm-messages, on page 303

# active-call-policy

This command instructs the SGSN to drop or reject any active call messages when congestion occurs during an active call. The active call instructions in the congestion-action-profile can be refined to only drop or reject active call messages with LAPI.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration > Congestion Control Configuration > Congestion Action Profile Configuration

configure > sgsn-global > congestion-control > congestion-action-profile *act_prof_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-cong-act-prof-`*`act_prof_name`*`)#`

**Syntax Description**

```
active-call-policy { rau | service-req } { drop | reject } [
low-priority-ind-ue ]
no active-call-policy { rau | service-req }
```

**no**

When this filter is added to the command, the SGSN deletes the active call policy definitions from the congestion-action-profile.

**rau**

Defines the action, either drop or reject, to be taken when the SGSN receives a Routing Area Update (RAU) message during congestion.

**service-req**

Defines the action, either drop or reject, to be taken when the SGSN receives a Service Request message during congestion.

**drop**

Instructs the SGSN to drop the defined message type as the congestion control response.

**reject**

Instructs the SGSN to reject the defined message type as the congestion control response.

**low-priority-ind-ue**

Instructs the SGSN to only take defined action if messages from the UE include a low priority access indicator (LAPI). This keyword can be use with either message type: RAU or Service Request.

**Usage Guidelines**

Use the **show sgsn-mode** command to display the SGSN's congestion control configuration defined with the command listed above. .

This command defines some of the congestion responses for the congestion-action-profile. These responses are a part of the overall SGSN machine type communication (MTC) congestion control functionality. For more information about the SGSN's MTC congestion control functionality, refer to the *MTC Congestion Control* section in the *SGSN Administration Guide.*

### Example

Use a command similar to the following to instruct the SGSN to drop RAU Requests received during an active call if LAPI is set in the request:

```
active-call-policy rau drop low-priority-ind-ue
```

Use a command similar to the following to remove all active-call congestion response definitions, for Service Requests, from the congestion-action-profile :

```
no active-call-policy service-req
```

# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`end`**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`exit`**

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

# new-call-policy

This command instructs the SGSN to drop or reject any new calls (Attach Request messages or new Inter SGSN RAU messages) if new call messages are received during congestion. The new call instructions in the congestion-action-profile can be refined to only drop or reject new call messages with low access priority indicator (LAPI).

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > SGSN Global Configuration > Congestion Control Configuration > Congestion Action Profile Configuration

configure > sgsn-global > congestion-control > congestion-action-profile *act_prof_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-cong-act-prof-`*`act_prof_name`*`)#`

**Syntax Description** **`new-call-policy { drop | reject } [ apn-based ] [ low-priority-ind-ue ]`**
**`no new-call-policy`**

**no**

When this filter is added to the command, the SGSN deletes the new call policy definitions from the congestion-action-profile.

**drop**

Instructs the SGSN to drop the any new call messages (Attach Request or new RAU ) if the new call messages are received during congestion.

#### reject

Instructs the SGSN to reject any new call messages (Attach Request or new RAU ) if the new call messages are received during congestion.

#### apn-based

Instructs the SGSN to reject a new call request based on the APN if congestion control is configured for that APN under an applicable Operator Policy.

#### low-priority-ind-ue

Instructs the SGSN to only take defined action if messages from the UE include a low priority access indicator (LAPI).

### Usage Guidelines

Use the **show operator-policy full name** *policy_name* command to display whether congestion control has been implemented for a specific APN.

Use the **show sgsn-mode** command to display the SGSN's congestion control configuration defined with the command listed above. .

This command defines some of the congestion responses for the congestion-action-profile. These responses are a part of the overall SGSN machine type communication (MTC) congestion control functionality. For more information about the SGSN's MTC congestion control functionality, refer to the *MTC Congestion Control* section in the *SGSN Administration Guide.*

#### Example

Use a command similar to the following to instruct the SGSN to drop new call messages that include LAPI :

```
new-call-policy drop low-priority-ind-ue
```

Use a command similar to the following to instruct the SGSN to reject new call messages only if the messages includes a LAPI and the APN is configured for congestion-control in an applicable operator policy :

```
new-call-policy reject apn-based low-priority-ind-ue
```

Use a command similar to the following to remove all new-call congestion response definitions from the congestion-action-profile :

```
no new-call-policy
```

# sm-messages

This command instructs the SGSN to reject any SM signaling messages (activation or modification) as a response to congestion. This congestion-action-profile parameter can be refined to only reject SM signaling messages when the low access priority indicator (LAPI) is included in the message.

### Product

SGSN

### Privilege

Security Administrator, Administrator

## Command Modes

Exec > Global Configuration > SGSN Global Configuration > Congestion Control Configuration > Congestion Action Profile Configuration

configure > sgsn-global > congestion-control > congestion-action-profile *act_prof_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-cong-act-prof-act_prof_name)#
```

## Syntax Description

```
sm-messages reject [ apn-based] [ low-priority-ind-ue ]
no sm-messages
```

### no

When this filter is added to the command, the SGSN deletes the sm-messages definition from the congestion-action-profile.

### reject

Instructs the SGSN to reject any sm-messages received during congestion.

### apn-based

Instructs the SGSN to reject sm-messages only if congestion control is configured for that APN under an applicable Operator Policy.

### low-priority-ind-ue

Instructs the SGSN to reject sm-messages from the UE only if the messages includes a low priority access indicator (LAPI).

## Usage Guidelines



**Important** For SM congestion to work, the **apn-based** option must be configured with the **sm-messages reject** command.

If both the LAPI and APN-based options are included in the action-profile, then the sm-messages will only be rejected if both conditions are matched.

Use the **show operator-policy full name** *policy_name* command to display whether congestion control has been implemented for a specific APN.

Use the **show sgsn-mode** command to display the SGSN's congestion control configuration defined with the command listed above. .

This command defines some of the congestion responses for the congestion-action-profile. These responses are a part of the overall SGSN machine type communication (MTC) congestion control functionality. For more information about the SGSN's MTC congestion control functionality, refer to the *MTC Congestion Control* section in the *SGSN Administration Guide.*

### Example

Use a command similar to the following to instruct the SGSN to reject sm-messages that include LAPI :

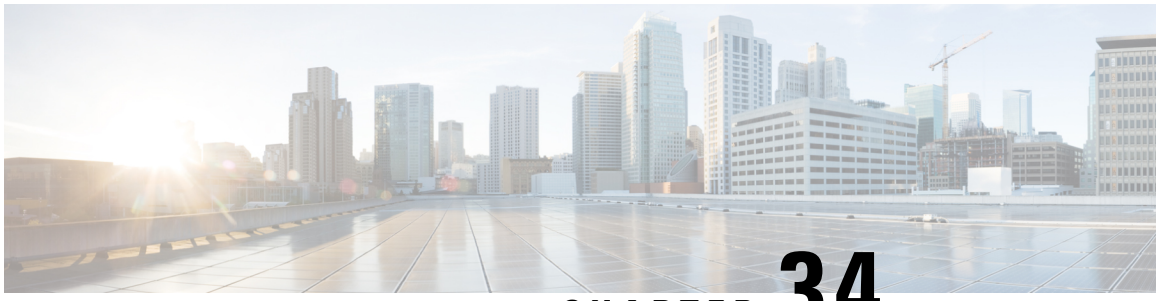
**sm-messages reject low-priority-ind-ue**

Use a command similar to the following to instruct the SGSN to reject sm-messages only if the messages includes a LAPI and the APN is configured for congestion-control in an applicable operator policy :

**sm-messages reject apn-based low-priority-ind-ue**

Use a command similar to the following to remove all congestion response definitions related to sm-messages from the congestion-action-profile :

**no sm-messages**



CHAPTER 34

# SGSN Congestion Control Configuration Mode

[this paragraph is needed as a minimum and must be completed as a continuation of the shortdesc]

**Command Modes**

The SGSN Congestion Control configuration mode provides the commands to access and configure the congestion control for the SGSN globally.

Exec > Global Configuration > SGSN Global Configuration > Congestion Control Configuration

**configure > sgsn-global > congestion-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-congestion-ctrl)#
```

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


- congestion-action-profile, on page 307
- do show, on page 308
- end, on page 309
- exit, on page 309


# congestion-action-profile

Creates an instance of a congestion-action-profile, which defines action to be take during congestion control scenario. Command also provides access to the Congestion Action Profile configuration mode commands.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration > Congestion Control Configuration

**configure > sgsn-global > congestion-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-congestion-ctrl)#
```

**Syntax Description** **`[ no ] congestion-action-profile`** *`action_profile_name`*

**no**

When this filter is added to the command, the SGSN deletes the congestion-control-profile from the SGSN-Global configuration.

**congestion-action-profile *action_profile_name***

Create or identify a congestion-action-profile.

*action_profile_name*: Enter a string of 1 to 64 alphanumeric characters.

**Usage Guidelines** This command provides access to the Congestion-Action-Profile configuration mode commands which define the SGSN's congestion responses for:

- active calls
- new calls
- SM messages

Use the **show sgsn-mode** command to display the SGSN's congestion-control configuration defined with the command listed above.

**Example**

Use a command similar to the following to gain access to the commands to modify an existing congestion-action-profile named *sgsnCongActProf1*:

```
congestion-action-profile sgsnCongActProf1
```

# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`do show`**

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`end`**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

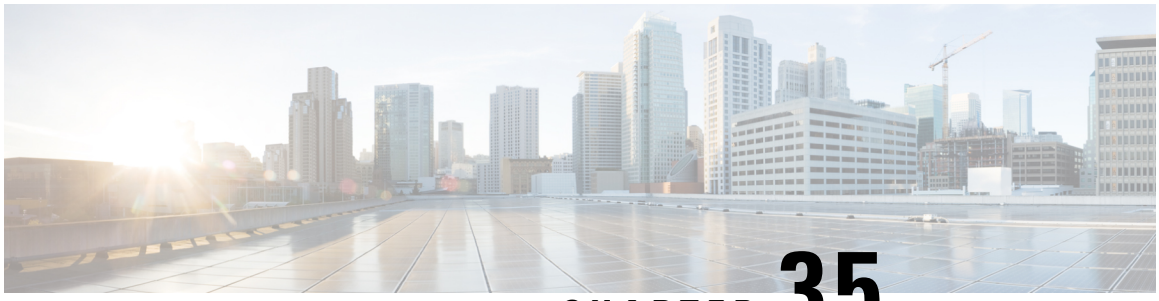
**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`exit`**

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

exit



CHAPTER 35

# SGSN Global Configuration Mode Commands

**Command Modes**

The commands in this mode configure parameters that impact the entire SGSN and that are independent of the GPRS or the IuPS services.

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

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


- aggregate-ipc-msg, on page 312
- apn-resolve-dns-query snaptr, on page 314
- bssgp-message dl-unitdata, on page 315
- bssgp-message ms-flow-control-from-unknown-ms , on page 316
- bssgp-message ptp-bvc-reset, on page 317
- bssgp-timer, on page 318
- bvc-unblock, on page 319
- canonical-node-name, on page 320
- common-ra-paging, on page 320
- congestion-control, on page 321
- do show, on page 322
- dscp-template, on page 322
- dual-address-pdp, on page 324
- ec-gsm, on page 325
- eir-profile, on page 325
- end, on page 326
- exit, on page 326
- gmm-message, on page 327
- gmm-sm-statistics, on page 327
- gprs-mocn, on page 328
- interface-management, on page 328

- ipms-suppress, on page 329
- imsi-range, on page 330
- location-services, on page 332
- map-message, on page 333
- max-pending-attaches, on page 334
- msisdn-group, on page 335
- msisdn-range, on page 336
- old-tlli invalidate tlli, on page 337
- old-tlli hold-time, on page 338
- pdp-deactivation-rate , on page 339
- qos-arp-rp-map-profile, on page 340
- ranap excess-len ignore, on page 341
- ran-information-management, on page 342
- target-offloading, on page 342
- tlli-cb-audit, on page 343
- umts-aka-r99, on page 344


# aggregate-ipc-msg

Configures the number of inter-process communication (IPC) messages that can be aggregated in the various managers and defines the frequency of flushing the messages.

**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

**Product**

SGSN

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

**aggregate-ipc-msg { gbmgr | linkmgr | sessmgr } { auto-num-msgs | flush-frequency***frequency* **| num-msgs** *number_msgs* **}**
**default aggregate-ipc-msg { gbmgr | linkmgr | sessmgr }**

**default**

Resets the managers to default values for flushing.

**gbmgr**

Selects the Gb manager to configure the number of IPC messages to be aggregated and frequency of flushing messages to the Session Manager that have been aggregated at the Gb Manager.

**linkmgr**

Selects the linkmgr to configure the number of IPC messages to be aggregated and frequency of flushing.

**sessmgr**

Selects the sessmgr to configure the number of IPC messages to be aggregated and frequency of flushing.

**auto-num-msgs**

Enables the automated aggregation of messages sent from LinkMgr or GbMgr to the SessMgr.

Default is Disabled.

**flush-frequency *frequency***

Configure the frequency, in 100-millisecond intervals, that the aggregated IPC messages will be flushed. Flushing limits the number of messenger calls between managers to transfer the received packets.

*frequency* : Enter an integer from 1 to 3. Default is 1.

**num-msgs *number_msgs***

Configure the number of IPC messages to aggregate before flushing.

*number_msgs* : Enter the integer 1 (to disable aggregation) or an integer from 2 to 164 to define the number of messages. Default is 10.



**Important** Setting **num-msgs** to a value of 1 will disable message packet aggregation.

## Usage Guidelines

Use this command to enable/disable aggregation of IPC messages in the linkmgr and/or the sessmgr. This command includes options to configure the frequency of aggregated message flushing and the number of packets to be buffered before the flush. This command provides a solution for reducing latency while sending the IPC messages towards the core network (CN).

The flushing limit will be based on either desired flush-frequency or maximum number of messages to be aggregated. Repeat the command to engage multiple limits.

By default, the link manager buffers packets and then send them over the SCCP link if there are events to be sent via SCCP Connection Request (SCCP CR) towards the core node. The HNB-GW/SGSN aggregate packets for 100 msec and send them with whatever aggregation has been done during those 100 msecs.

At the HNB-GW/SGSN, this command can be used to reduce the processing involved in sending every event individually towards the core node in the following manner:

- If aggregation is enabled, then there could be a time delay for sending SCCP CRs depending on configuration of the HNB-GW or SGSN.
- If aggregation is reduced to 1, then there will be no delay for aggregation and events are sent via SCCP CR without delay. This reduces the SCCP connection setup time.

To view aggregate IPC message statistics, use command **show config | grep aggregate-ipc-msg**.

### Example

Configure the linkmgr to buffer *45* messages before flushing the linkmgr IPC messages:

```
aggregate-ipc-msg linkmgr flush-frequency 45
```

The following command configures the *linkmgr* to flush the IPC messages towards the CN without aggregation:

```
aggregate-ipc-msg linkmgr1
```

The following command configures the *sessmgr* to flush the IPC messages towards the CN without aggregation:

```
aggregate-ipc-msg sessmgr1
```

# apn-resolve-dns-query snaptr

Enable/disable sending of SNAPTR DNS query to resolve an APN for a subscriber with an EPS (evolved packet system)-capable handset.

**Important** This command is no longer available in all 12.0 and 12.2 releases. If you do not see this command in your release, look for the **apn-resolve-dns-query snaptr** command in the APN Profile configuration mode to accomplish the same task.

## Product

SGSN

## Privilege

Security Administrator, Administrator

## Command Modes

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

## Syntax Description

```
[ no ] apn-resolve-dns-query snaptr
default apn-resolve-dns-query
```

### default

Resets the default, the ability to send SNAPTR DNS query is disabled.

### no

Disables the ability to send SNAPTR DNS query.

**Usage Guidelines**

By default, sending the SNAPTR DNS query is disabled. Use this command to send SNAPTR DNS query when resolving an APN for an EPS-capable subscriber.

At PDP context activation, the SGSN will use the UE capabilitly as input to select either a GGSN or a P-GW for the EPS-capable subscriber. The SNAPTR DNS query will be used for P-GW resolution. Enabling this feature will give priority to P-GW selection for E-UTRAN-capable UEs.

### Example

Use the following command to enable sending of SNAPTR DNS query for APN resolution:

```
apn-resolve-dns-query
```

Use the following command to disable the use of SNAPTR DNS query for APN resolution:

```
no apn-resolve-dns-query
```

# bssgp-message dl-unitdata

Configure this command to exclude or include RAT/Frequency Selection Priority (RFSP ID) in BSSGP DL-Unitdata messages to the BSC.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

```
bssgp-message dl-unitdata rfsp-id exclude
default bssgp-message dl-unitdata rfsp-id
```

### default

By default, the RFSP-ID IE is included in BSSGP DL-Unitdata message.

### dl-unitdata rfsp-id exclude

Use this keyword to exclude RFSP-ID IE in BSSGP DL-Unitdata message.

**Usage Guidelines**

The SGSN can control sending of RAT/Frequency Selection Priority (RFSP ID) from subscription or a local overridden value towards BSC.

### Example

Use this command to exclude the RFSP ID in BSSGP DL-Unitdata message:

```
bssgp-message dl-unitdata rfsp-id exclude
```

Use this command to include the RFSP ID in BSSGP DL-Unitdata message:

**default bssgp-message dl-unitdata rfsp-id**

# bssgp-message ms-flow-control-from-unknown-ms

This command determines the SGSN response to MS-Flow-Control messages received from an unknown MS.

## Product

SGSN

## Privilege

Security Administrator, Administrator

## Command Modes

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

## Syntax Description

**bssgp-message ms-flow-control-from-unknown-ms { discard-message | send-ack | send-status }**
**default bssgp-message ms-flow-control-from-unknown-ms**

### default

Including **default** with the command configures the SGSN to use default behavior so that the SGSN sends BSSGP-Status messages whenever the SGSN receives an MS-Flow-Control message from an unknown MS.

### discard-message

This keyword instructs the SGSN to discard the received BSSGP message. With this option, the SGSN does not send any response to the MS after discarding the received BSSGP message.

### send-ack

This keyword instructs the SGSN to send an acknowledgement message (MS-Flow-Control-ACK) after receiving an MS-Flow-Control message.

### send-status

Default

This keyword instructs the SGSN to send a BSSGP-Status message to the MS whenever the SGSN receives an MS-Flow-Control message from an unknown MS.

## Usage Guidelines

This command allows the operator to specify the action the SGSN needs to take whenever the SGSN receives an MS-Flow-Control message from an unknown mobile station. This configuration determines the response for the SGSN globally.

The list of possible actions are:

- send a BSSGP-Status response message

- send an ACK message (MS-Flow-Control-ACK)
- discard the BSSGP message

To see the statistics for the number of MS-Flow-Control messages that have been discarded, use the **show bssgp statistics** command from the Exec mode.

### Example

Change the default configuration and have the SGSN acknowledge receipt of the MS-Flow-Control message:

```
bssgp-message ms-flow-control-from-unknown-ms send-ack
```

# bssgp-message ptp-bvc-reset

This command determines the SGSN response, per BVCI, to receipt of a peer-to-peer BVC Reset.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

```
bssgp-message ptp-bvc-reset { frc-subscriber-standby | retain-current-state }
default bssgp-message ptp-bvc-reset
```

### default

Including **default** with the command configures the SGSN to use default behavior so that the SGSN continues with the current state once a peer-to-peer BVC Reset is received.

### frc-subscriber-standby

This keyword instructs the SGSN to change the state of the subscribers to standby when the peer-to-peer BVC Reset is received.

### retain-current-state

Default

This keyword instructs the SGSN to continue the current state of the subscribers when the BVC Reset message is received.

**Usage Guidelines**

This command allows the operator to specify the action the SGSN needs to take whenever the SGSN receives a peer-to-peer BVC Reset message for a specific BVCI.

To confirm the configuration for the response to the BVC Reset, use the **show sgsn-mode** command from the Exec mode.

### Example

Change the default configuration and have the SGSN change subscriber states to standby:

```
bssgp-message ptp-bvc-reset frc-subscriber-standby
```

# bssgp-timer

Configures the T2 and TH timers for the BVCs (BSSGP virtual connections) of the NSE (network service entities).

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

```
bssgp-timer { t2 T2_time | th TH_time }
default bssgp-timer { t2 | th }
```

#### default

Resets the specified timers to default settings.

#### t2 *T2_time*

Configures the BVC reset guard timer (at the BSSGP layer) in units of 1 second.

*T2_time* : Enter an integer from 1 to 120. Default is 30 seconds.

#### th *TH_time*

Configures, at the BSSGP layer, the MS flow control parameter validity timeouts in units of 1 second.

*TH_time* : Enter an integer from 6 to 5999. Default is 500 seconds.

**Usage Guidelines**

Use this command to configure timer timeout values for MS flow control and BVC reset timers that control BVCs for the NSEs.

### Example

Set the TH timeout for *20* seconds:

```
bssgp-timer th 20
```

# bvc-unblock

This command enables (disabled by default) or disables the SGSN to unblock blocked BVCs based on the receipt of uplink packets from the BSC.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

**bvc-unblock { data-or-flow-control | flow-control | ul-data }**
**[ default | no ] bvc-unblock**

**default**

Include **default** with the command to disable the function.

**no**

Include **no** with the command to disable this function.

**data-or-flow-control**

Enables the BVC-Unblock function when the SGSN receives either a FLOW-CONTROL-BVC packet or a UL-UNITDATA packet.

**flow-control**

Enables the BVC-Unblock function when the SGSN receives a FLOW-CONTROL-BVC packet.

**ul-data**

Enables the BVC-Unblock function when the SGSN receives a UL-UNITDATA packet.

**Usage Guidelines**

Configurations defined with this command are common to all NSE defined for the SGSN.

This command is useful if there is a BVC status mismatch across different SGSN managers (such as the sessmgr and the linkmgr) when the BSC sends BVC-Block (SGSN should move to BLOCKED) followed by a BVC-Reset (SGSN should move to UNBLOCKED). Such mismatches can easily occur, particularly on Gb-IP network connection, when one link receives the BVC-Block and a different link receives the BVC-Reset with little delay between the two.

If BVC-Unblock function is enabled, the SGSN ensures that BVCs which are in the BLOCKED state move to the UNBLOCKED state upon receipt of the configured packet type(s).

### Example

Instruct the SGSN to perform BVC-Unblock when a mismatch occurs and the SGSN receives a FLOW-CONTROL-BVC packet:

```
bvc-unblock flow-control
```

# canonical-node-name

Defines the SGSN's canonical node name.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

**[ no ] canonical-node-name** *canonical_node_name*

**no**

Erases the specified canonical node name definition from the SGSN Global configuration.

**Usage Guidelines**

*canonical_node_name* is a fully or properly qualified domain name; for example sgsn.div.bng.kar.3gppnetwork.org.

In order for the Gn/Gp-SGSN to support the topological gateway selection feature, the SGSN's canonical node name must be defined in the SGSN's configuration. (This is not needed for the S4-SGSN). For additional information about this feature, refer to the *Topology-based Gateway Selection* section in the *SGSN Administration Guide*.

### Example

Define the SGSN's canonical node name as *sgsn.div.bng.kar.3gppnetwork.org*:

```
canonical-node-name  sgsn.div.bng.kar.3gppnetwork.org
```

# common-ra-paging

This command enables paging across common Routing Area (RA) for 2G and 3G.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

**`[ default | no ] common-ra-paging`**

**default**

Returns the SGSN to the default state: paging across commong Routing Area (RA) is disabled for 2G and 3G.

**no**

Disables paging across common Routing Area (RA) for 2G and 3G after it has been enabled using the **common-ra-paging** command

**Usage Guidelines**

When this CLI is enabled, the SGSN supports paging initiation in both the RATs (2G and 3G) if paging has to be done in RA which is common across the RATs. SGSN also accepts power-off detach from the MS, which is different from the RAT when the MS is attached.

**Example**

Use the following command to enable paging across common Routing Area (RA) for 2G and 3G.

**`common-ra-paging`**

# congestion-control

Sets up the environment on the SGSN to support Machine Type Communications (MTC) congestion control and opens a new SGSN Global Congestion Control command configuration mode.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

**`congestion-control`**

**Usage Guidelines**

Provides access to the congestion-action-profile configuration command.

### Example

Open the SGSN Global Congestion Control configuration mode.

```
congestion-control
```

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character | is only available if the command is valid in the Exec mode.



**Caution**

There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# dscp-template

Creates and/or deletes DSCP templates that can be configured for use for all GPRS services on the SGSN and provides access to the DSCP Template configuration mode. This command is also supported on HNB-GW service to create a DSCP template.



**Important**

In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

**Product**

SGSN

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

## Syntax Description

**dscp-template** *template_name* **[ -noconfirm ]**
**no dscp-template** *template_name*

**no**

Deletes the template instance from the SGSN Global configuration.

***template_name***

Enter 1 to 64 alphanumeric characters, including dots (.), dashes (-), and forward slashes (/). to identify a unique instance of a DSCP template.

There is no known limit to the number of templates that can be created.

## Usage Guidelines

This command enables the operator to create or delete an instance of a DSCP template and access the DSCP Template configuration mode. The DSCP templates are used to define the DSCP configuration for control packets and data packets for the GPRS services.

**Related commands:**

- This command provides access to the mode containing all the configuration commands used to define DSCP markings for the control packets and data packets for a particular GPRS service (see the *DSCP Template Configuration Mode Commands* section).
- To associated a specific DSCP template with a specific GPRS service configuration, for builds prior to release 14.0 use the **associate-dscp-template downlink** command and for builds in releases 14.0 and higher use the **associate dscp-template downlink**command. Both commands are documented in the *GPRS Service Configuration Mode Commands* section.
- To check the list of DSCP templates configured, use the **show sgsn-mode** command documented in the *Exec Mode Commands* section.

This command is also supported on HNB-GW service to create a DSCP template.

**Related commands for HNB-GW:**

- This command provides access to the mode containing all the configuration commands used to define DSCP markings for the control packets and data packets for a particular HNB-GW service (see the *DSCP Template Configuration Mode Commands* chapter).
- To associated a specific DSCP template with a system for a PSP instance in SS7 routing domain, use the **associate-dscp-template downlink** documented in the *SGSN PSP Configuration Mode Commands* chapter.

### Example

Use a command similar to the following to create a DSCP template with ID *dscp_london* that can be used specifically for Gb/IP calls from subscribers in London:

```
dscp-template dscp_london
```

Following command creates a DSCP template with ID *dscp_hnb1* that can be used specifically for HNB-GW services on a chassis:

```
dscp-template dscp_hnb1
```

# dual-address-pdp

This command makes it possible for the operator to enable (default) / disable SGSN support for MS requests for dual PDP type (IPv4v6) addressing.

## Product

SGSN

## Privilege

Security Administrator, Administrator

## Command Modes

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

## Syntax Description

```
[ default | no ] dual-address-pdp
```

**default**

Enables dual PDP type address support.

**no**

Disables the default behavior so that the SGSN does not honor requests for dual PDP type addresses.

## Usage Guidelines

With release 12.2 and in accordance with 3GPP Release 9.0 specifications, by default the SGSN honors the MS/UE request for dual PDP type addressing (IPv4v6) for PDP context association with one IPv4 address and one IPv6 address/prefix. This support can be disabled by configuration.



**Important** For the dual PDP addressing feature to function, **common-flags** must be enabled with the **gptc send** command in the SGTP service configuration mode *prior* to enabling the feature with the **dual-address-pdp** command.

With this default behavior, the operator has multiple options to refine the level of support for dual PDP type addressing through the use of several related commands.

- **dual-address-pdp** command in the RNC configuration mode disables SGSN support for dual PDP type addressing for a specific RNC that either does or does not support this type of addressing..
- **pdp-type-ipv4v6-override** in the APN profile configuration mode allows the SGSN to override the MS/UE request for dual PDP type addressing.
- Using the **dual-ipv4v6** keyword with the **wildcard-apn pdp-type** command in the APN remap table configuration mode enables the operator to configure a default APN with a wildcard subscription with PDP type IPv4v6.

### Example

Use the following command to disable support for dual PDP type addressing (IPv4v6):

```
no dual-address-pdp
```

If dual PDP addressing has been disabled, to renable the feature, move to the SGTP service configuration mode, in the appropriate context, to perform the following as the *first* command needed to re-enable support for dual PDP type addressing in the configuration:

```
gtpc send common-flags
```

Now in the SGSN global configuration mode, use the following as the second command required to re-enable support for dual PDP type addressing in the configuration:

```
dual-address-pdp
```

# ec-gsm

This command enables extended coverage class support on the SGSN.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

### Syntax

```
[ no ] ec-gsm
```

#### no

Disables EC-GSM support on the SGSN.

**Usage Guidelines**

Use this command to enable EC-GSM for all GPRS services on the SGSN.

# eir-profile

Creates an EIR profile and provides access to the EIR profile configuration mode commands that define the parameters of the profile.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

**eir-profile** *profile_name*
**no eir-profile** *profile_name*

**no**

Deletes an EIR profile from the SGSN Global configuration.

***profile_name***

Enter a unique name for the profile, upto 64 alphanumeric characters in length.

**Usage Guidelines**

This command creates up to 16 instances of EIR profiles and provides access to the EIR Profile configuration mode for the commands to configure the EIR profile parameters.

**Example**

Remove the 'testing' EIR profile from the SGSN Global configuration mode:

**no eir-profile testing**

# end

Exits the current mode and returns to the Exec Mode.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**end**

**Usage Guidelines**

Change the mode back to the Exec Mode.

# exit

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

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**end**

**Usage Guidelines** Change the mode to the Global Configuration Mode.

# gmm-message

This command configures the SGSN to discard (drop) the Attach-Request message received with a random TLLI already in use.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

```
[ default ] gmm-message attach-with-tlli-in-use discard-message
```

**default**

Resets the default function allowing multiple MS, using the same random TLLI, to attempt to Attach simultaneously and disables discarding the Attach-Request message for random TLLI already in use.

**Usage Guidelines** Working with the two related commands (noted below), this command is part of a procedure for handling multiple MS Attaches all with the Same Random TLLI. Use this command to configure the SGSN to allow only one subscriber at a time to attach using a fixed random TLLI.

**Related Commands**:

- The **old-tlli invalidate tlli** command configures a list of random TLLI to be invalidated from the GMM after the invalidate old-TLLI timer expires.
- The **old-tlli hold-time** command configures the old-TLLI expiry timer.

**Example**

Configure the SGSN to drop Attach Request containing TLLI already in use:

```
gmm-message attach-with-tlli-in-use discard-message
```

# gmm-sm-statistics



**Important** This command has been deprecated.

**Product** SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

```
gmm-sm-statistics attach-rejects cause network-failure only-internal
no gmm-sm-statistics attach-rejects
```

# gprs-mocn

Enables or disables General Packet Radio Service (GPRS) Multi-Operator Core Network (MOCN). With 2G MOCN, the radio network is shared among different operators, while each operator maintains its separate core network.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

```
[ no ] gprs-mocn
```

**no**

Disables GPRS MOCN when it has been previously enabled.

**Usage Guidelines**

Use this command to enable 2G MOCN, which is disabled by default.

For complete information about the 2G (GPRS) MOCN feature and its configuration, refer to the *MOCN for 2G SGSN* feature section in the *Serving GPRS Support Node Administration Guide*

**Example**

The following command enables GPRS MOCN support for SGSN:

```
gprs-mocn
```

# interface-management

This command creates an interface management configuration and provides access to the SGSN Interface Management configuration mode.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description** **`interface-management`**

**Usage Guidelines** Use this command to access the SGSN Interface Management configuration mode to map NSE-ID and NSE-name to the Gb interface and/or to lock and unlock interface by the NSE/BSC identifier.

**Example**

Access the SGSN Interface Management configuration mode:

**`interface-management`**

# ipms-suppress

This command enables suppressing of the specified RAT related ipms event reporting.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

```
ipms-suppress [ gprs | umts ]
no ipms-suppress [ gprs | umts ]
```

**no**

Disables suppressing of the specified RAT related ipms event reporting.

**gprs**

This keyword enables suppressing of 2G related ipms-event reporting to the Intracer.

**umts**

This keyword enables suppressing of 3G related ipms-event reporting to the Intracer.

**Usage Guidelines**

This command is configured to suppress or allow the IPMS-event reporting to Intracer for the specified RAT. This CLI command helps the operator to change the IPMS-event reporting and manage network load or congestion on the fly.

**Note**

- At a time only service (either gprs or umts service) related ipms event reporting to the Intracer server (IPMS server) can be suppressed using the CLI command, provided there is a valid IPMS-context and server address.
- When no **ipms-suppress [gprs | umts]** is configured then regardless of the service provided the suppression enabled on the service (configured through **ipms-suppress [gprs | umts]**) will be disabled. There is no one-to-one mapping of the **ipms-suppress** and **no ipms-suppress**.
  - For example, if ipms-suppress on gprs is configured using the command **ipms-suppress gprs**. To remove ipms suppress, either of the commands **no ipms-suppress gprs** or **no ipms-suppress umts** can be used. However the command **no ipms-suppress gprs** is recommended in such a scenario.
- By default the IPMS event reporting will be done by both the services, provided there is a valid IPMS-context and IPMS-server configured.
- IPMS suppression can be enabled on both the services (GPRS and UMTS service) at the same time. This provides independent control on the suppression of ipms-events from the GPRS and UMTS services.

### Example

Use this command to enable suppressing of 2G related ipms-event reporting to the Intracer:

```
ipms-suppress gprs
```

# imsi-range

Configure an IMSI range with an optional PLMN ID to associate with an Operator Policy.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

```
imsi-range mcc mcc_num mnc mnc_num { msin first start_number last stop_number [
 operator-policy policy_name [ description description ] ] | plmnid plmn_id
operator-policy policy_name [ description description ] } +
no imsi-range mcc mcc_num mnc mnc_num { msin first start_number last stop_number
 | plmnid plmn_id }
```

**no**

Using **no** in the command deletes the definition from the SGSN Global configuration.

**mcc *mcc_num***

**mcc** defines the mobile country code (MCC) of an IMSI.

*mcc_num:* Enter a 3-digit number from 100 to 999 - 000 to 099 are reserved.

**mnc *mnc_num***

**mnc** defines the mobile network code (MNC) of an IMSI.

*mnc_num:* Enter a 2 or 3-digit number from 00 to 999.

**msin**

MSIN (mobile subscriber international number) portion of the IMSI.

first *start_num:* Defines first MSIN prefix number in a range

last *stop_num:* Defines the last or final MSIN prefix number in a range.

**operator-policy *policy_name* description *description***

Identify the operator policy that the IMSI range definition and/or the PLMN-ID is to be associated.

*policy_name* : Enter a string of 1 to 64 alphanumeric characters.

*description*: Enter a string of 1 to 100 alphanumeric characters to provide range clarification for converted Release 9.0 configurations.

Description is just an information field. From release 19.0 onwards the length of the string supported for this field has been reduced, the supported range is now "1" up to "50" alphanumeric characters. The reduction of the supported string size results in improvement in boot up time.

If a PLMN-ID is to be included in the definition, enter the **plmnid** before entering the operator policy name.

**plmnid *plmn_id***

The 5-6 digit PLMN-ID consists of the MCC (mobile country code) plus the MNC (mobile network code) to identify the public land mobile network (PLMN) for a specific operator. This keyword associates a specific PLMN with this specific SGSN operator policy.

*plmn_id* : Enter 5 to 6 digits.

**+**

This symbol indicates that command can be repeated to create repeated definitions.

## Usage Guidelines

An IMSI = maximum of 15 digits. An IMSI consists of the MCC (3 digits) + the MNC (2 or 3 digits) + the MSIN (the remaining 10 or 9 digits depending on the length of the MNC ).

MCC and MNC are the minimum amount of information required to identify a unique operator policy with IMSI filtering. The MCC and MNC combine uniquely to identify the country and the network operator, for example: Cingular Wireless in the United States = **mcc** *311***mnc** *180*

To improve the granularity of call handling, an operator policy with additional IMSI filtering parameters can be defined, to include filtering based on the MSIN, by defining a MSIN range - first (or start-of-range) MSIN and last (or end-of-range) MSIN. The range numbers do not include the maximum allowed for the MSIN but should include a sufficient number to enable the operator policy to filter effectively.

For the most efficient IMSI filter, the operator policy should include all of the above parameters and the PLMN ID which defines the current location of the MS -- this parameter is particularly useful for highlighting which calls are roaming.

And if none of the operator policies contain useful filtering information, then the default operator policy will be applied as the information in this command is never defined for the default operator policy.

The following table will illustrate how these filtering parameters determine which operator policy will govern a call:

| Operator Policy ID | MCC | MNC | MSINfirst | MSINlast | PLMN ID |
|---|---|---|---|---|---|
| OpPol-1 | 123 | 45 | 67890 | 67898 | |
| OpPol-2 | 123 | 45 | | | |
| OpPol-3 | 123 | 45 | 67890 | 67898 | 23232 |
| OpPol-4 | 123 | 45 | | | 23232 |
| OpPol-5 | 123 | 45 | 6789012 | 6789019 | |
| OpPol-6 | 123 | 45 | 6789012 | 6789019 | 23232 |
| default | | | | | |

The filtering selects which operator policy will be used to determine how a call is handled - the operator policy that best matches the IMSI. So, a call with IMSI 123456789012345 PLMNID 23232 is best matched with OpPol-6.

In most cases, the operator policy with the most information defined will be used as a combination of PLMNID and IMSI provides the best match. But OpPol-6 won't always be the best match. Using the table above:

OpPol-1 is the best match for IMSI 123456789011111

OpPol-2 is the best match for IMSI 123456789099999

OpPol-5 is the best match for IMSI 123456789012345 if the PLMNID is 12344

### Example

The following associates operator policy *oppol1* with country code *310*, mobile network code of *33*, and IMSI range *1231234* - *1231244*:

```
imsi-range mcc 310 mnc 33 msin first 1231234 last 1231244 operator-policy
 oppol1
```

# location-services

Enable or 'start' Location Services (LCS) on the SGSN.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

```
location-services
no location-services
```

**no**

Disables or 'stops' LCS on the SGSN.

**Usage Guidelines** By default, Location Services is not enabled on the SGSN. This command is mandatory to enable the SGSN to support LCS, which is a license-controlled feature. Multiple other commands are required to configure LCS functionality. For more information about the operation and configuration of LCS on the SGSN, refer to the *Location Services* section of the *SGSN Administration Guide*.

**Example**

Use the following command to disable Location Services once they have been enabled:

```
no location-services
```

# map-message

This command instructs the SGSN to ignore the CAMEL subscription when there is no CAMEL service associated or in existence.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

```
map-message insert-subscriber-data csi-handling when-camel-not-associated
 ignore-subscription
default map-message insert-subscriber-data csi-handling
```

**default**

Resets the SGSN's default behavior. By default, the SGSN validates the CAMEL subscription and rejects an Attach Request when there is no CAMEL service association.

**Usage Guidelines**

By default, the SGSN updates the the CAMEL subscription included in the INSERT-SUBSCRIBER-DATA (ISD) messages received from the HLR. While processing the ATTACH request from the CAMEL subscriber, the SGSN checks whether it has a CAMEL service associated with the corresponding service (either GPRS service or SGN service). It drops the ATTACH request if there is no CAMEL service associated with a corresponding service.

Also by default, the SGSN does not allow establishment of a Direct Tunnel (DT) for a CAMEL subscriber. It strictly validates the subscriber against the CAMEL subscription during the Direct Tunnel setup procedure.

This command enables the operator to control the behavior of the SGSN by configuring the SGSN to ignore the CAMEL subscription. This allows the SGSN to successfully complete an ATTACH procedure when there is an ATTACH Request from a CAMEL subscriber and there is no CAMEL service association in the SGSN. As well, during the Direct Tunnel establishment, validation of the CAMEL subscription is ignored to allow the DT to setup when there is no CAMEL service association in the SGSN.

**Example**

Instruct the SGSN to validate the CAMEL subscription:

```
default map-message insert-subscriber-data csi-handling
```

# max-pending-attaches

Configure the maximum length of the pending attach queue.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

```
max-pending-attaches limit
default max-pending-attaches
```

**default**

Resets the SGSN's Attach queue to a maximum pending value of 10,000.

***limit***

Set the a maximum limit to the pending Attach/RAU messages queue in the LinkMgr. When the limit is reached a message is sent to the IMSIMgr.

*limit* : Enter an integer from 5000 - 50000. Default is 10000.

**Usage Guidelines**

With this command, configure the maximum limit to the pending ATTACH/RAU messages queue in the LinkMgr. When the limit is reached, the LinkMgr sends the Query/Forward messages to the IMSIMgr.

As the IMSIMgr gets busier and does not responded to Query/Forward requests, the response to the requests will get slower and slower and the queue size continues inflating if the incoming message rate is high. To avoid this situation, set the **max-pending-attaches** for the pending queue for Attach and RAU messages. All other messages from the HLR will be added to the queue as they cannot be dropped. High and low watermarks are set to the queue at 80% of **max-pending-attaches "** and 60% of **max-pending-attaches** respectively.

Once a high watermark is reached, the new Attach and RAU requests are dropped and relevant statistics are incremented. Once a low watermark is hit, the new Attach/RAU requests are accepted and added to the pending queue. The entries are added to the pending queue only when the window-size between IMSIMgr and LinkMgr becomes zero. This is a very rare occurrence and will not affect the current behavior in normal circumstances.

### Example

Set the queue length to a maximum of *15000* requests:

```
max-pending-attaches 15000
```

# msisdn-group

This command configures the Mobile Subscriber Integrated Services Digital Network (MSISDN) group to which the operator policy should be associated.

**Product**

SGSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

**msisdn-group** *group_name* **operator-policy** *policy_name*
**no msisdn-group** *group_name*

### no

Deletes the configured MSISDN group.

### msisdn-group *group_name*

Specifies the MSISDN group name to which the operator policy should be associated. *group_name* must be an alphanumeric string of 1 through 64 characters. It can have a maximum of 50 groups.

**operator-policy *policy_name***

Specifies the operator policy to which the IMSI range should be associated with.

*policy_name* must be an alphanumeric string of 1 through 64 characters.

**Usage Guidelines** Use this command to specify the MSISDN group to which the operator policy should be associated.

# msisdn-range

This command configures the MSISDN range to which operator policy should be associated.

**Product** SGSN

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

**msisdn-range cc** *cc_value* **number first** *start_range* **last** *end_range* **operator-policy** *policy_name*

**no msisdn-range cc** *cc_value* **number first** *start_range* **last** *end_range* **operator-policy** *policy_name*

**no**

Deletes the specified MSISDN numbers.

**cc *cc_value***

**cc** is the country code of MSISDN. *cc_value* is a 1 to 3 digit number.

**number first *start_range* last *end_range***

Specifies the start and end of MSISDN (combination of Country Code (CC), National Destination Code (NDC) or Number Planning Area (NPA), and Subscriber Number (SN)).

**operator-policy *policy_name***

Specifies the operator policy to which the IMSI range should be associated with.

*policy_name* must be an alphanumeric string of 1 through 64 characters.

**Usage Guidelines** Use this command to configure the MSISDN range to which operator policy should be associated.

**Example**

The following command configures the MSISDN with CC as *334* and MSISDN range as *918369110173* and *918369110184*, and then associates with operator policy *OP1*:

```
msisdn-range cc 334 number first 918369110173 last 918369110184
operator-policy op1
```

# old-tlli invalidate tlli

This command configures a list of random TLLI to be invalidated (removed) from the GMM after the invalidate old-TLLI timer expires.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

`[local]host_name(config-sgsn-global)#`

**Syntax Description**

**`[ no ] old-tlli invalidate tlli`** *`< hexadecimal >`*

**no**

Removes a single random TLLI from the configured list.

***< hexadecimal >***

Identifies a single random TLLI to be removed from the GMM after the old-TLLI timer expires.

**Usage Guidelines**

Use this command to create a list of up to 50 random TLLI to be dropped from the GMM after the old-TLLI timer expires. This command also starts the invalidate old-TLLI timer.

**Important** If the old-TLLI expiry timer is not configured with the **old-tlli hold-time** command, then the SGSN will only drop second Attach Requests using the same random TLLI already in use.

**Related Commands**:

- The **gmm-message** configures the SGSN to discard (drop) the Attach-Request message received with a random TLLI already in use
- The **old-tlli hold-time** command configures the old-TLLI expiry timer.

### Example

Add random TLLI *0x7f05a30a* to the Invalidate List:

```
old-tlli invalidate tlli 0x7f05a30a
```

# old-tlli hold-time

This command configures the old-TLLI expiry timer to be started in GMM when anyone of the listed random TLLI are received.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

**[ default ] old-tlli hold-time** *< seconds >*

**default**

Resets the timer to 5 seconds

***< seconds >***

Sets the numbers of seconds before the timer expires; range 1 to 125.

**Usage Guidelines**

Use this command to configure the old-TLLI expiry timer to be started in GMM when anyone of the listed random TLLI are received. If the timer expires prior to receiving Attach-Complete then the SGSN invalidates (removes) the TLLI from the GMM.

**Important** For this configuration to work, the list of random TLLI to be removed (invalidated) from the GMM must be defined with the **old-tlli invalidate tlli** command.

**Related Commands**:

- The **gmm-message** configures the SGSN to discard (drop) the Attach-Request message received with a random TLLI already in use
- The **old-tlli invalidate tlli** command configures the random invalidate TLLI list.

**Example**

Set the timer for *2* seconds:

```
old-tlli hold-time 2
```

# pdp-deactivation-rate

Set the rate the SGSN deactivates PDP connections per second per SessMgr when GPT-C path failure is detected. Beginning with release 15.0, this command is also supported on the S4-SGSN.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

**pdp-deactivation-rate { connected-ready** *rate* **| idle-standby** *rate* **}**
**default pdp-deactivation-rate { connected-ready | idle-standby }**

**default**

If this keyword is used with the command, then the default deactivation rates are used.

**connected-ready *rate***

Subscribers that are in the PMM-Connected / GPRS-Ready state and actively using the SGSN service need to be deactivated at a faster rate to facilitate the deactivation/re-activation process.

*rate* -sets the number of subscribers to be deactivated per second per SessMgr and the valid range is 1 to 1000 and the default is 760 connected-ready subscribers deactivated per second.

**idle-standby *rate***

Subscribers that are in the PMM-Idle / GPRS-Standby state are not actively using the SGSN service and can be deactivated at a slower rate. The deactivation process for idle-standby subscribers includes paging before the Deactivate Request is sent.

*rate* - sets the number of subscribers to be deactivated per second per SessMgr and the valid range is 1 to 1000 and the default is 240 idle-standby subscribers deactivated per second.

**Usage Guidelines**

Use this command to define a rate at which the SGSN processes PDP deactivations when a GTP-C path failure is detected (and confirmed according to the SGSN's default behavior). The operator can use this command to set a deactivation rate that ensures radio network congestion is avoided.

**Related commands:**

- **max-remote-restart-counter-change** - allows the operator to set a maximum variance between stored and received values for restart counter changes coming from the GGSN. For details, refer to the SGSN Global configuration mode documentation.
- **disable-remote-restart-counter-verification** - allows the operator to disable the default behavior. For details, refer to this command in the SGSN Global configuration mode documentation.

### Example

Use the following command to deactivate PDP connections for *600* PMM-Connected / GPRS-Ready subscribers per second:

```
pdp-deactivation-rate connected-ready 600
```

Use the following command to deactivate PDP connections for *320* PMM-Idle / GPRS-Standby subscribers per second:

```
pdp-deactivation-rate idle-standby 320
```

Use the following command to reset the default *760* per second deactivation rate for PMM-Connected / GPRS-Ready subscribers:

```
default pdp-deactivation-rate connected-ready
```

# qos-arp-rp-map-profile

This command creates an instance of an ARP-RP Mapping Profile and/or access the ARP-RP Mapping Profile configuration mode commands.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

**qos-arp-rp-map-profile** *arp-rp_prof_name*
**no qos-arp-rp-map-profile** *arp-rp_prof_name*

**no**

Removes the specified ARP-RP Map Profile from the SGSN Global configuration.

***arp-rp_prof_name***

Enter a string of 1 to 64 alphanumeric characters to identify the mapping profile and moves into the ARP-RP mapping profile configuration mode. The ARP-RP Map Profiles need to be associated with the SGSN and/or GPRS Services.

**Usage Guidelines**

Using the ARP to RP mapping, the SGSN can choose a preferred radio priority according to the ARP values sent by the GGSN and HLR. As well, these mappings will be used by corresponding 2G and/or 3G services to choose the radio priority value while triggering messages (such as those listed below) towards the MS/UE:

- Activate PDP Accept.
- Modify PDP Request during network-initiated PDP modification procedure.

- Modify PDP Accept during MS-initiated PDP modification procedure provided the ARP has been changed by the network.

The profiles will be populated via the **arp** command under the ARP-RP Map Profile configuration mode.

### Example

Create an ARP-RP Map Profile named *arprpmap1* using the following command:

```
qos-arp-rp-map-profile  arprpmap1
```

# ranap excess-len ignore

Configure the SGSN to ignore excess length of received RANAP messages.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

```
[ default | no ] ranap excess-len ignore
```

### default

Resets the default behavior - a decode error is generated when received RANAP messages are more than an extra octet in length.

### no

Disables the configuration to ignore overly long RANAP messages.

**Usage Guidelines**

By default, the SGSN issues a decode error when the RANAP messages include extra octets. Use this command to ignore RANAP messages that have excess octets.

### Example

Use the following command to enable the SGSN to ignore overly long RANAP messages:

```
ranap excess-len ignore
```

Use the following command to disable ignoring of RANAP messages that are excessive in length:

```
no ranap excess-len ignore
```

# ran-information-management

Enable/disable RAN information management (RIM) support for the SGSN.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

**`[ default | no ] ran-information-management`**

**default**

Resets the default so RIM is disabled.

**no**

Disables the RIM support in the configuration file.

**Usage Guidelines**

By default, handling of RAN information management (RIM) messages is disabled. This command enables the SGSN to handle RIM messages. When this command is enabled and RIM message handling is enabled on the destination node, then RIM PDUs will be forwarded to the BSC/RNC. If RIM message handling is not enabled on both nodes, then the RIM PDUs will be dropped silently.

Confirm RIM configuration with the **show sgsn-mode** command in the Exec mode.

**Example**

Use the following command to enable RIM support:

**`ran-information-management`**

Use the following command to disable RIM support that has been added to the configuration:

**`no ran-information-management`**

# target-offloading

Selects the subscriber offloading algorithm to be applied to the SessMgr and the IMSIMgr.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

```
target-offloading algorithm [ optimized-for-speed |
optimized-for-target-count ]
default target-offloading algorithm
```

**default**

Resets the configuration to default values.

**optimized-for-speed**

Enables faster algorithm to achieve the target count.

**optimized-for-target-count**

Enables a reliable algorithm to achieve the target count.

Default.

**Usage Guidelines**

With the SGSN's distributed architecture, there are many SessMgrs and offloading will happen in parallel at all SessMgrs. This command enables the operator to control the total number of subscribers being offloaded.



**Important** The value for this command can not be altered once dynamic offloading has begun - refer to the command description for the **sgsn-offload** command in the *Exec Mode* chapter..

**Example**

Set the SGSN to use the faster algorithm for offloading:

```
target-offloading algorithm optimized-for-speed
```

# tlli-cb-audit

This command enable (default is disabled) or disables a periodic (hourly) audit of TLLI-CBs in the BSSGP layer.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

```
tlli-cb-audit
[ default | no ] tlli-cb-audit
```

**default**

Include **default** with the command to disable the audit function.

**no**

Include **no** with the command to disable the audit function.

**Usage Guidelines**

This command is used to clean-up hanging or unassociated TLLI in the BSSGP layer. This configuration defined with this command will be common to all NSE configured for this SGSN.

Independent of this command configuration, the SGSN triggers and audit when the number of TLLI-CBs reaches 35,000.

**Example**

Use the following command to enable the hourly audit for unassociated TLLl-CBs:

```
tlli-cb-audit
```

# umts-aka-r99

This command enables the operator to authenticate mobile equipment (MEs) with R99+ USIMs and capable of UMTS AKA.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration

**configure > sgsn-global**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax Description**

```
umts-aka-r99
no umts-aka-r99
```

**no**

Including **no** with the command disables the authentication.

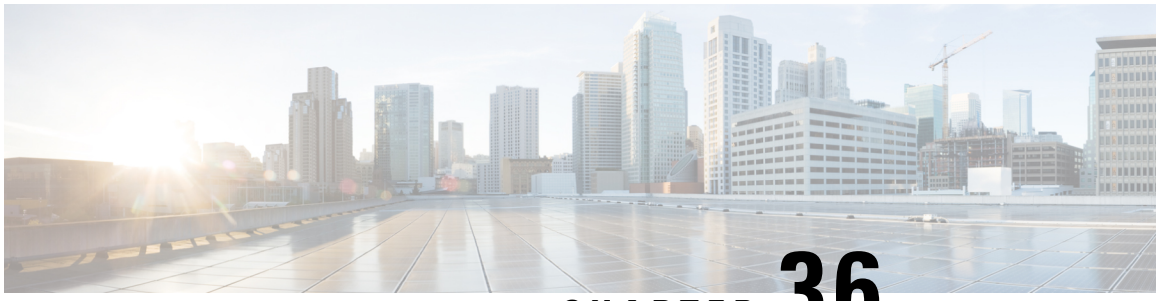
## Usage Guidelines

This command enables operators to authenticate MEs that are attempting to connect to a 2.5G network with R99+ USIMs if the MEs are UMTS AKA capable. For R99 mobiles, the SGSN will continue to perform GSM AKA even if quintuplets are received fromthe HLR.

### Example

Use the following command to disable UMTS AKA authentication for MEs with R99+ USIMs:

```
no umts-aka-r99
```



CHAPTER 36

# SGSN Interface Management Configuration Mode

**Command Modes**

The interface management commands, accessed via the SGSN Global configuration mode, are applicable to the SGSN on a global level. They map the NSC/BSC to the SGSN's Gb interface and enable the operator to quickly configure lock or unlock for the BSC interface on the basis of the NSE's ID or name.

Exec > Global Configuration > SGSN Global Configuration > Interface Management Configuration

**configure > sgsn-global > interface-management**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-interface-mgmt)#
```

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


- do show, on page 347
- end, on page 348
- exit, on page 348
- interface, on page 348
- lock-interface, on page 350
- paging-rlf-template, on page 351


# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character | is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Return to the Exec mode.

# exit

Exits the current configuration mode and returns to the SGSN Global configuration mode.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

**Usage Guidelines** Returns to the SGSN Global configuration mode.

# interface

Maps the Gb interface to an NSE-ID and an NSE-name to facilitate the identification of the peer NSE/BSC.This command also allows the SGSN to configure the mapping between RNC-ID and RNC-NAME which allows the operator to associate rlf-template either by NAME or ID.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > SGSN Global Configuration > Interface Management Configuration

**configure > sgsn-global > interface-management**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-interface-mgmt)#
```

## Syntax Description

**interface { gb peer-nsei id | iu peer-rnc id } { name** *<value>* **| id** *<value>* **}**
**no interface{ gb peer-nsei id | iu peer-rnc id } { name** *<value>* **| id** *<value>* **}**

### no

Removes the interface mapping from the configuration.

The "No" option removes the mapping and action configuration from the SGSN and it resets the behavior to default for that RNC. By default, no throttling is done.

### gb peer-nsei id *id*

Maps a specific peer NSE/BSC to the Gb interface by the NSEI.

*id* - Enter an integer from 0 to 65535.

### gb peer-nsei *name*

Identifies a BSC by name assigned to the NSEI, which is stored in the SCT.

*name* - Enter an alphanumeric string of 1 to 64 characters.

### iu peer-rnc id *id*

Maps a specific peer RNC-ID .

*id* - Enter an integer from 0 to 65535.

### iu peer-rnc *name*

Maps a specific peer RNC-Name.

*name* - Enter an alphanumeric string of 1 to 64 characters.

## Usage Guidelines

This command configures mapping between an NSE-ID and an NSE name and the SGSN's Gb interface. The mapping allows the operator to use the **lock-interface** command (also in this mode) to more easily configure locking or unlocking of the interface to the BSC by identifying the network service entity by ID or by name.

This command provides a configuration option to create a mapping for RNC to the interface name for the interface identifier which allows the operator to associate rlf-template either by using name or identifier.

**Related Commands:**

**lock-interface**

### Example

Map NSE with ID of *422* and the name *Dover* to the Gb interface:

```
interface gb peer-nsei id 422 name Dover
```

The following example disables the mapping for NSEI *2321*:

```
no interface gb peer-nsei id 2321
```

# lock-interface

This command enables the operator to configure the SGSN's Gb interface, toward the peer NSE/BSC, as locked or unlocked on the basis of the NSE's name or identifier.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration > Interface Management Configuration

**configure > sgsn-global > interface-management**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-interface-mgmt)#
```

**Syntax Description**

**[ no ] lock-interface gb peer-nsei { id** *nse-id* **| name** *nse_name* **}**

**no**

Disables a previously configured lock on the interface to the NSE/BSC.

**peer-nsei id *nsei_id***

Specifies the numeric identifier of the network service entity mapped to the Gb interface.

*nse_id* - Enter an integer from 0 to 65535.

**peer-nsei *nsei_name***

Specifies the name of the NSE associated with the BSC, which is stored in the SCT.

*nse_id* - Enter an alphanumeric string of 1 to 64 characters.

**Usage Guidelines**

This command allows the operator to lock/unlock the interface, towards the NSE/BSC, based on the NSE name or NSE identifier.

Lock is configured primarily to avoid the high CPU usage the SGSN can experience when BSCs attempt to reconnect after an SGSN reboot or reload. The lock stops the auto-learn procedure for the locked BSC connected via Gb over IP.

The auto-learn facility can be enabled in a staggered manner for each BSC after reboot/reload by unlocking the BSCs one-by-one.

The NSE unlock state is the default state and the NSE can accept or send any uplink and downlink data.

**Related Commands:**

**interface**

### Example

Lockout NSE/BSC ID *319* from the SGSN:

```
lock-interface gb peer-nsei id 319
```

# paging-rlf-template

This command allows the SGSN to associate the RLF template either at global level which limits the paging messages initiated across both 2G (NSE level) and 3G (RNC level) access or at per entity level either at RNC level for 3G access or at NSE level for 2G access.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration > Interface Management Configuration

**configure > sgsn-global > interface-management**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-interface-mgmt)#
```

**Syntax Description**

**`[no] paging-rlf-template {template-name` *`<template-name>`*`} {gb peer-nsei | iu peer-rnc} {name` *`<value>`* `| id` *`<value>`*`}`**

#### no

The "No" option removes the association of the rlf-template against the global level or at particular NSE/RNC.

#### template-name *<template-name>*

Specifies the template name.

#### gb peer-nsei *id*

Maps a specific peer NSE/BSC to the Gb interface by the NSEI.

*id* - Enter an integer from 0 to 65535.

#### gb peer-nsei *name*

Identifies a BSC by name assigned to the NSEI, which is stored in the SCT.

*name* - Enter an alphanumeric string of 1 to 64 characters.

#### iu peer-rnc *id*

Maps a specific peer RNC-ID .

*id* - Enter an integer from 0 to 65535.

**iu peer-rnc *name***

Maps a specific peer RNC-Name.

*name* - Enter an alphanumeric string of 1 to 64 characters.

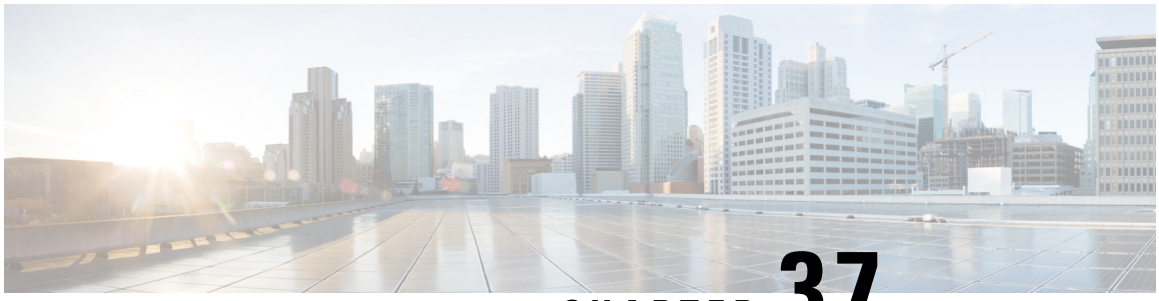
## Usage Guidelines

This command helps to limit the paging load sent out from the SGSN as it consumes more bandwidth in the radio interface. The NSE/RNC level rlf-template association overrides the globally associated rlf-template which throttles the paging messages initiated from that NSE/RNC with the configured message rate. The actual RLF template can be configured under the global configuration mode which provides the option to configure the message-rate, burst-size, threshold and delay-tolerance for throttling or rate-limiting.

### Example

Use the following command to associate a RLF template with name "rlf1":

**paging-rlf-template template-name** *rlf1*



CHAPTER 37

# SGSN Pool Area Configuration Mode Commands

**Command Modes**

The Pool Area configuration mode configures the parameters used to setup the VLRs to use with a pool area in a Gs service.

Exec > Global Configuration > Context Configuration > Gs Service Configuration > Pool Area Configuration

**configure > context** *context_name* **> gs-service** *service_name* **> pool-area** *pool_area_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-gs-pool-area)#`

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


- do show, on page 353
- end, on page 354
- exit, on page 354
- hash-value, on page 354
- lac, on page 356


# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Return to the Exec mode.

# exit

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

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

**Usage Guidelines** Return to the previous configuration mode.

# hash-value

This command configures the load distribution for the VLRs that service this pool area.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Gs Service Configuration > Pool Area Configuration

**configure > context** *context_name* **> gs-service** *service_name* **> pool-area** *pool_area_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gs-pool-area)#
```

## Syntax Description

**hash-value { *hash_value* | non-configured-values | range *start_value* to *end_value* } use-vlr *vlr_name***
**no hash-value { *hash_value* | non-configured-values | range *start_value* to *end_value* }**

### no

Removes the configured Gs procedures from this Gs service.

### *hash_value*

Specifies the specific hash value for VLR(s).

*hash_value* must be an integer value from 0 through 999.

### range *start_value* to *end_value*

Specifies the range of hash values for a VLR.

*start_value* specifies the start value for range of hash and is an integer value from 0 through 999. *start_value* must be lower than *end_value.*

*end_value* specifies the end value for range of hash and is an integer value from 0 through 999. *end_value* must be higher than *start_value*.

### non-configured-values

This keyword assign all non-configured hash values to use the named VLR.

### use-vlr *vlr_name*

Specifies the name of the VLR to be associated with this pool area.

*vlr_name* is the name of VLR and must be an alpha and/or numeric string of 1 to 63 characters.

## Usage Guidelines

Use this command to command configures the load distribution for the VLRs that service this pool area as defined in TS 23.236.

The algorithm for selection of VLR from a pool area is based on the hash value computed on the IMSI digits. The SGSN derives a hash value (V) using procedure as defined in TS 23.236. Every hash value from the range 0 to 999 corresponds to a single MSC/VLR node. Typically many hash values may point to the same MSC/VLR node.

This command can be entered multiple times for different hash value.

### Example

Following command configure the all non configured hash values to use VLR named *starvlr1* in this pool area:

**hash-value non-configured-values use-vlr** *starvlr1*

# lac

This command defines a set of location area code (LAC) values for a pool area.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Gs Service Configuration > Pool Area Configuration

**configure > context** *context_name* **> gs-service** *service_name* **> pool-area** *pool_area_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gs-pool-area)#
```

**Syntax Description**

**lac** *lac_id* **+**
**no lac** *lac_id*

**no**

Removes the configured LAC value from this pool area configuration.

**lac *lac_id***

Specifies the subscribers' location area code (LAC) to be associated with this pool area and a specific VLR. This LAC is obtained from the radio area identity (RAI).

*lac_id:* Must be an integer from 1 through 65535.

**+**

More than one *lac_id*, separated by a space, can be entered within a single command.

**Usage Guidelines**

Use this command to specify a set of LACs to use for a pool area.

This command can be entered multiple times, subject to a limit of 32 LAC definitions (total for **non-pool-area** and **pool-area** configuration) per Gs service.

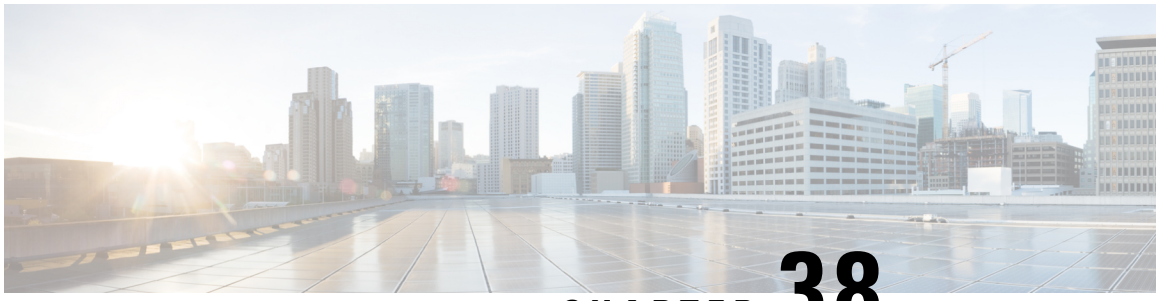


**Important** LAC values across multiple pool areas and non-pool-areas must be unique within the Gs service.

### Example

The following command configures LACs *101*, *301*, and *222* for the pool area.

**lac** *101 301 222*



CHAPTER 38

# SGSN PSP Configuration Mode Commands

## Command Modes

The Peer-Server Process (PSP) configuration mode provides the commands to create, configure, bind, and manage a specific PSP instance included in an SS7 routing domain configuration.

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-ss7-rd-`*`ss7rd_id`*`-ps-peer-`*`server_id`*`-psp-`*`psp_instance`*`)#`

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


- associate, on page 358
- do show, on page 360
- end, on page 360
- end-point, on page 360
- exchange-mode, on page 361
- exit, on page 362
- psp-mode, on page 363
- routing-context, on page 364
- sctp-alpha, on page 365
- sctp-beta, on page 366
- sctp-checksum-type, on page 367
- sctp-cookie-life, on page 368
- sctp-init-rwnd, on page 369
- sctp-max-assoc-retx, on page 370
- sctp-max-data-chunks, on page 371
- sctp-max-in-strms, on page 372
- sctp-max-init-retx, on page 372
- sctp-max-mtu size, on page 373
- sctp-max-out-strms, on page 374

- sctp-max-path-retx, on page 375
- sctp-parameter , on page 376
- sctp-rto-initial, on page 377
- sctp-rto-max, on page 378
- sctp-rto-min, on page 379
- sctp-sack-frequency, on page 380
- sctp-sack-period, on page 381
- sctp-suppress-alarm, on page 382
- shutdown, on page 383
- timeout, on page 384


# associate

Defines an association between the PSP instance and an application server process (ASP) instance and/or a DSCP marking template.

**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

**Product**

SGSN

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#`

**Syntax Description**

**associate { asp instance** *asp_num* **| dscp-template downlink** *template_name* **}**
**no associate [ asp | dscp-template downlink ]**

**no**

Removes the association, between the PSP and the ASP or the DSCP marking template, from the routing domain configuration.

**Important** Using the **no associate** command will most likely result in the termination of all current subscriber sessions active through the peer-server.

**asp instance *asp_num***

Identifies a specific ASP configuration. Up to four ASP instances can be configured for a single SS7 routing domain.

*asp_num* is a digit from 1 to 4.

**dscp-marking downlink *template_name***

Identifies a specific DSCP marking template to associate with this PSP configuration.

*template_name* is a string of 1 to 64 characters, including letters, digits, dots (.), dashes (-), and forward slashes (/), to identify a unique instance of a DSCP template. For more information about DSCP marking templates, refer to the *DSCP Template Configuration Commands Mode* chapter.

The DSCP marking template provides a mechanism enabling the SGSN to perform differentiated services code point (DSCP) marking of control packets and signaling messages at the SGSN's M3UA level on the Gb interface. This DSCP marking feature enables the SGSN to perform classifying and managing of network traffic and to determine quality of service (QoS) for the interfaces to an IP network

While enabling DSCP marking of SCTP (control packets) on HNB-GW only **associate dscp-template downlink** *template_name* command is applicable. This command is used to provides a mechanism enabling the HNB-GW to perform differentiated services code point (DSCP) marking of control packets and signaling messages at the HNB-GW. This DSCP marking feature enables the HNB-GW to perform classifying and managing of network traffic and to determine quality of service (QoS) for the interfaces to an IP network

## Usage Guidelines

Use this command to create an association between a specific peer-server process (PSP) and a specific application server process (ASP) instance or a specific differentiated services code point (DSCP marking template).

Before using the **associate** command, the values for the **psp-mode** and **end-point** commands must be configured.

Before using the **associate** command, the M3UA end-point of the ASP must be configured. Use the commands defined in the *ASP Configuration Mode* chapter of the *Command Line Interface Reference.*

While enabling DSCP marking of SCTP (control packets) on HNB-GW only **associate dscp-template downlink** *template_name* command is applicable. For more information about DSCP marking templates, refer to the *DSCP Template Configuration Commands Mode* chapter.

### Example

Associate this PSP instance with ASP configuration instance *2* :

```
associate asp instance 2
```

Use the following command to terminate all associations with this PSP instance:

```
no associate
```

Associate this PSP instance with a DSCP marking template identified as *dscptemp1* :

```
associate dscp-template downlink dscptemp1
```

# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

Exits the configuration mode and returns to the Exec mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
end
```

**Usage Guidelines** Change the mode back to the Exec mode.

# end-point

This command defines or deletes the IP address to be associated with the local SCTP end-point for the application server process (ASP).



**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

**Product** SGSN

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-ss7-rd-`*`ss7rd_id`*`-ps-peer-`*`server_id`*`-psp-`*`psp_instance`*`)#`

**Syntax Description**

**`end-point { address`** *`ip_address`* **`| port`** *`port_number`* **`}`**
**`no end-point [ address`** *`ip_address`* **`]`**

**no**

Removes the ASP end-point association configuration from the PSP configuration.

**Important** This command can not be used as long as the PSP and the ASP are associated. Use the **no associate** command when entering any form of this command, including **no end-point**. When the change is made, re-enter the ASP association with the **association** command.

**address *ip_address***

Specifies the IP address for the ASP end-point.

*ip_address:* Must be defined using the standard IPv4 dotted decimal notation or the colon notation of IPv6.

**port *port_number***

Configures the M3UA's SCTP port number for the end-point.

*port_number:* Must be an integer from 1 to 65535.

Default: 2905.

**Usage Guidelines**

Use this command to manage the ASP end-point. At least one address needs to be configured for the ASP before the end-point can be associated with the PSP.

**Example**

Set the ASP end-point to IP address *192.168.1.1* with the following command:

**`end-point address 192.168.1.1`**

# exchange-mode

Configures the exchange-mode for the PSP communication.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#`

**Syntax Description** **exchange-mode [ double-ended | single-ended ]**

**double-ended**

A double exchange of ASPTM and ASPSM messages would typically be needed to change the IPSP states. Either end can request the change and the state changes if the other end acknowledges.

With this configuration, the connections in each direction are managed independently so one could be closed while the other remains active.

**single-ended**

Only a single exchange of ASPTM and ASPSM messages is needed to change the IPSP state. Either end can request the change and the state changes if the other end acknowledges.

**Usage Guidelines**

**Important** Before using this command to set a value or reset the default, you must disassociate the PSP instance with the **no associate** command. When you have modified your configuratioin with this command, then use the **associate** command to setup a new ASP association.

Use this command to toggle the exchange modes for the PSP to match the exchange mode supported by the ASP. The exchange mode specifies what type of ASP messages exchange is used in an IPSP communication.

The **exchange-mode** must be configured for 'single-ended' if the **psp-mode** has been configured for 'client'.

**Example**

Change the exchange mode from the standard double-ended to single-ended:

**exchange-mode single-ended**

# exit

Exits the current configuration mode and moves to the previous configuration mode.

**Product** All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**exit**

**Usage Guidelines**

Return to the Peer-Service configuration mode.

# psp-mode

Configures either client-mode or server-mode as the PSP's operational mode.

**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

**Product**

SGSN

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-ss7-rd-`*`ss7rd_id`*`-ps-peer-`*`server_id`*`-psp-`*`psp_instance`*`)#`

**Syntax Description**

**psp-mode { client | server }**

**client**

The PSP operates as a client.

**server**

The PSP operates as a server.

**Usage Guidelines**

**Important** Before using this command to change the configuration, you must disassociate the PSP instance with the **no associate** command. When you have modified your configuratioin with this command, then use the **associate** command to setup a new ASP association.

Instruct the peer-server process to operate in either client or server mode.

### Example

Configure the PSP to operate in server mode:

```
psp-mode server
```

# routing-context

Configures the behavior of the routing context in M3UA messages.

**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

**Product**

SGSN

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#
```

**Syntax Description**

```
routing-context { discard-inbound | process-inbound | m3ua-data {
insert-outbound | suppress-outbound } }
default routing-context
```

#### default

Include this keyword with the command, to reset the configuration to the system default for routing-context which is a combination of process-inbound and insert-outbound.

#### discard-inbound

Sets the routing context received in M3UA messages to be discarded.

#### process-inbound

Sets the routing context received in M3UA messages to be processed.

#### m3ua-data

This keyword controls the insertion of routing context in outbound M3UA data messages. The default behavior is to insert routing context in management messages and suppress routing context in data messages.

### insert-outbound

Sets the routing context so that it is added in the M3UA messages.

### suppress-outbound

Sets the routing context so that it is suppressed in the M3UA messages.

## Usage Guidelines

**Important** Before using this command to change the configuration or reset the default, you must disassociate the PSP instance with the **no associate** command. When you have modified your configuratioin with this command, then use the **associate** command to setup a new ASP association.

In PSP (singled-ended) configuration mode, the settings for both the local routing context (the SGSN's routing context) and the peer routing context (the RNC's routing context) should be the same. If the routing contexts created at the SGSN and on the peer are different then this can cause the M3UA link to fail.

Routing context is an optional parameter when an M3UA association has only one associated peer-server.

### Example

If the peer does not support routing context, then disable the routing context feature:

```
routing-context discard-inbound suppress-outbound
```

# sctp-alpha

This stream control transmission protocol (SCTP) retransmission time out (RTO) parameter defines the RTO-Alpha value.

## Product

SGSN

## Privilege

Security Administrator, Administrator

## Command Modes

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#
```

## Syntax Description

**sctp-alpha** *value*
**default sctp-alpha**

***value***

Defines a percentage (%) that represents the RTO portion of the round-trip time (RTT) calculation. This percentage value must be an integer between 0 and 65535.

**default**

Resets the **sctp-alpha** to the default value of 5%.

**Usage Guidelines**

**sctp-alpha** is used in conjunction with other commands, such as the **sctp-beta** command, to determine the round-trip time (RTT) calculations. The Alpha parameter is used to manage load balancing within the SS7 environment for multi-homed peers.



**Important** Before using this command to set a value or reset the default, you must disassociate the PSP instance with the **no associate** command. When you have modified your configuratioin with this command, then use the **associate** command to setup a new ASP association.

**Example**

Set the SCTP RTO-Alpha value to *256%* of the RTT calculation:

```
sctp-alpha 256
```

# sctp-beta

This stream control transmission protocol (SCTP) retransmission time out (RTO) parameter defines the RTO-Beta value.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#
```

**Syntax Description**

```
sctp-beta value
default sctp-beta
```

***value***

Defines a percentage (%) that represents the RTO portion of the round-trip time (RTT) calculation. This percentage value must be an integer between 0 and 65535.

**default**

Resets the **sctp-beta** to the default value of 10%.

**Usage Guidelines**

Use this command in conjunction with other commands, such as the **sctp-alpha** command, to determine the round-trip time (RTT) calculations. The Beta parameter is used to manage load balancing within the SS7 environment for multi-homed peers.



**Important**

Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

**Example**

Set the SCTP RTO-Alpha value to *512%* of the RTT calculation:

```
sctp-beta 512
```

# sctp-checksum-type

This command selects the type of checksum algorithm to be used.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#
```

**Syntax Description**

```
sctp-checksum-type { adler32 | crc32 }
default sctp-checksum-type
```

**adler32**

Selects the Adler-32 type of algorithm as a faster checksum function.

**crc32**

Selects the CRC-32, a slower but more reliable 32-bit cyclic redundancy check.

**default**

Resets the **sctp-checksum-type** to the default of CRC-32.

**Usage Guidelines** Use this command to set which type of checksum algorithm the SGSN is to use to validate SCTP packets.



**Important** Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

### Example

Set the checksum type for *CRC32*:

```
sctp-checksum-type crc32
```

# sctp-cookie-life

This command sets the SCTP valid cookie life.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#
```

**Syntax Description**

```
sctp-cookie-life value
default sctp-cookie-life
```

#### *value*

Sets the valid cookie life value in increments of 100 milliseconds. The range is 50 to 1200 .

#### default

Resets the **sctp-cookie-life** value to the default, 600 (= .6 seconds).

**Usage Guidelines** Use this command to set the SCTP cookie life.



**Important** Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

### Example

Set the SCTP cookie life to 1 second (*1000* milliseconds):

```
sctp-cookie-life 1000
```

# sctp-init-rwnd

This command sets the size of the SCTP receiver window .

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#
```

**Syntax Description**

**sctp-init-rwnd** *window_size*
**default sctp-init-rwnd**

#### *window_size*

Sets an integer to configure the window size. The range is 32768 to 1048576.

#### default

Resets the **sctp-init-rwnd** window size to the default, 1048576.

**Usage Guidelines**

Use this command to set the receiver window size in the configuration. Configuring this parameter enables the SCTP client to send configured 'sctp-init_rwnd' as a_rwnd parameter in the INIT message. For the SCTP server, the INIT ACK will be populated with sctp-init_rwnd as a_rwnd parameter per RFC 4960.

The command enables the operator to configure a reduced priority for LinkManager Control messages, thereby giving Timer messages the highest priority. The Timer messages are retained at the highest priority and Data messages are kept at a lower priority.



**Important** Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

### Example

Use the following command to set the SCTP window size to *32786*:

```
sctp-init-rwnd 32768
```

# sctp-max-assoc-retx

This command sets the maximum number of datagram retransmissions to be associated with this peer server configuration.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#
```

**Syntax Description**

**sctp-max-assoc-retx** *value*
**default sctp-max-assoc-retx**

#### *value*

Defines the maximum number of datagram retransmissions for an association. The value must be an integer between 0 and 255.

#### default

Resets the default for **sctp-max-assoc-retx** to 10.

**Usage Guidelines**

Use this command to configure the maximum number of datagram retransmissions for an association. The endpoint will be declared unreachable after **sctp-max-assoc-retx** number of consecutive retransmissions to an endpoint on any transport address.



**Important** Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

### Example

Set the maximum number to *3* datagram retransmissions:

```
sctp-max-assoc-retx 3
```

# sctp-max-data-chunks

This command sets the operator-preferred limit to the number of data chunks that can be bundled in an SCTP message.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-ss7-rd-`*`ss7rd_id`*`-ps-peer-`*`server_id`*`-psp-`*`psp_instance`*`)#`

**Syntax Description**

**`sctp-max-data-chunks ( limit`** *`max_chunks`* **`| mtu-limit )`**
**`default sctp-max-data-chunks`**

**default**

Resets the default for **sctp-max-data-chunks** to the limit set for the MTU with the **sctp-max-mtu-size** command.

**limit *max_chunks***

Sets the operator-preferred maximum number of data chunks that can be bundled into SCTP messages. Enter an integer from 1 to 65535.

**mtu-limit**

Instructs the SGSN to bundle only as many data chunks for the SCTP streams as defined by for the maximum transmission unit (MTU) size configured with the **sctp-max-mtu-size** command.

**Usage Guidelines**

Use this command to override the default MTU-limit for data chunk bundling and configure a preferred maximum number of data chunks that can be bundled into an SCTP message.

**Important** Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

**Example**

Set *1024* as a maximum number of data chunks to bundled:

```
sctp-max-data-chunks limit 1024
```

# sctp-max-in-strms

Configures the maximum number of incoming SCTP streams

**Product**

SGSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-ss7-rd-`*`ss7rd_id`*`-ps-peer-`*`server_id`*`-psp-`*`psp_instance`*`)#`

**Syntax Description**

**`sctp-max-in-strms`** *`value`*
**`default sctp-max-in-strms`**

**default**

Returns the configuration to the default of 16.

***value***

Default: 16.

Specifies the maximum number of incoming SCTP streams as an integer from 1 to 16. The SGSN restricts the allowable range to 2 to 16. If a value of 1 is entered, a value 2 will be applied for any SGSN service associated with this SCTP parameter template.

**Usage Guidelines**

Use this command to configure the maximum number of incoming SCTP streams.

**Example**

The following command configures the maximum number of incoming SCTP streams to *5*:

**sctp-max-in-strms 5**

# sctp-max-init-retx

This command sets the maximum number of retries to send the INIT datagram.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#`

**Syntax Description**

**sctp-max-init-retx** *value*
**default sctp-max-init-retx**

***value***

Sets the maximum number of retries. This value must be an integer between 0 and 255.

**default**

Resets the default for **sctp-max-init-retx** to 5.

**Usage Guidelines**

Use this command to set the maximum number of retries the SCTP layer should make to send the INIT datagram to the peer to open an association.



**Important** Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

**Example**

**sctp-max-init-retx** *3*

# sctp-max-mtu size

This command sets the number of bytes that comprise the maximum MTU size.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#`

**Syntax Description**

**sctp-max-mtu-size** *value*
**default sctp-max-mtu-size**

***value***

Sets the maximum number of bytes for the SCTP MTU size. This value must be an integer between 508 and 65535.

**default**

Resets the default for **sctp-max-mtu-size** to 1500 bytes.

**Usage Guidelines**

Use this command to configure the size of the MTU.

**Important** Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

**Example**

Set the maximum size of the MTU to 3000 bytes:

**sctp-max-mtu-size** *3000*

# sctp-max-out-strms

This command sets the maximum number of outgoing streams through the PSP going towards the peer server.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-ss7-rd-`*`ss7rd_id`*`-ps-peer-`*`server_id`*`-psp-`*`psp_instance`*`)#`

**Syntax Description**

**sctp-max-out-strms** *max#_out_streams*
**default sctp-max-out-strms**

**default**

Resets the SGSN's **sctp-max-out-strms** value to the default of 2.

***max#_out_streams***

The value must be an integer between 1and 16. The value should match the peer node's (STP/SG/RNC/HLR) number of in-bound streams.



**Important** For releases prior to 14.0, the value range was 1 to 65535. However, the system always capped at 16 so in Release 14.0 the range has been decreased to reflect that fact.

**Usage Guidelines** Use this command to balance the stream throughput from the PSP to the peer server. The value for this command is used to validate the incoming packets in the SCTP layer.

If the user tries to configure the value of **sctpmax-out-strms** less than "2", a message is displayed and the default value is set.



**Important** Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

**Example**

Set a maximum SCTP out streams to *12*:

```
sctp-max-out-strms 12
```

Set a maximum SCTP out streams to the default of *2* streams:

```
default sctp-max-out-strms
```

# sctp-max-path-retx

This command sets the maximum number of datagram retransmissions for this path.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#`

**Syntax Description**

**sctp-max-path-retx** *value*
**default sctp-max-path-retx**

***value***

Sets the maximum number of datagram retransmission to a destination transport address. This value must be an integer from 0 to 255.

**default**

Resets the **sctp-max-path-retx** default to 5.

**Usage Guidelines**

Use this command to set the maximum number of datagram retransmissions to a destination transport address. The destination transport address will be declared unreachable after the SGSN exhausts the **sctp-max-path-retx** number of consecutive retransmissions to a destination transport address.

Depending upon network conditions, lower values typically means faster detection of SCTP-Path failure.



**Important** Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

**Example**

```
sctp-max-path-retx 10
```

# sctp-parameter

This command enables the SGSN administrator to alter the contents of the Optional Address Parameter IE.

**Product**

SGSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#
```

**Syntax Description**

```
[ default | no ] sctp-parameter ipv4-address suppress single-ended
```

**[ default | no ]**

Either command prefix resets the default behavior to repeat the source IP address in the IE.

**Usage Guidelines**

In situations when the endpoint is uni-homed (that is, single transport layer address), this command enables the SGSN administrator to override the default behavior and to configure the SGSN to suppress (not repeat)

the source IP address which is typically included as part of the Optional Address Parameter IE in the INIT/INIT-Ack chunk.

### Example

Enable suppression of sending repeated IP address in the OAP IE with this command:

**sctp-parameter ipv4-address suppress single-ended**

Repeat sending the source IP address in the OAP IE with the following command:

**no sctp-parameter ipv4-address suppress single-ended**

# sctp-rto-initial

This command sets the initial retransmission timeout for the SCTP.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-ss7-rd-`*`ss7rd_id`*`-ps-peer-`*`server_id`*`-psp-`*`psp_instance`*`)#`

**Syntax Description**

**`sctp-rto-initial`** *`value`*
**`default sctp-rto-initial`**

#### default

Resets the system to the **sctp-rto-initial** default of 30 (3 seconds).

#### *value*

The value must be an integer between 1 and 50.

**Usage Guidelines**



**Important** Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

Use this command to define the initial retransmission timer.

The value set for **sctp-rto-initial** should be greater than or equal to the minimum value set with **sctp-rto-min** (**sctp-rto-initial**=> **sctp-rto-min**).

The value set for **sctp-rto-initial** should be less than or equal to the maximum value set with **sctp-rto-max** (**sctp-rto-initial** <= **sctp-rto-max**).

### Example

**sctp-rto-initial** *240*

# sctp-rto-max

This command sets the maximum retransmission timeout value for the SCTP.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

`[local]`*host_name*`(config-ss7-rd-`*ss7rd_id*`-ps-peer-`*server_id*`-psp-`*psp_instance*`)#`

**Syntax Description**

**sctp-rto-max** *value*
**default sctp-rto-max**

#### default

Resets the system to the **sctp-rto-max** default of 600 (60 seconds).

#### *value*

Set the maximum retransmission timeout value in increments of 100 milliseconds (0.1 seconds) and the value must be an integer between 5 and 1200.

**Usage Guidelines**



**Important** Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

Use this command to configure the maximum time for retransmissions.

The value set for **sctp-rto-max** should be greater than or equal to the value set for **sctp-rto-initial** (**sctp-rto-max** => **sctp-rto-initial**).

### Example

The following sets the timeout for 45 seconds:

```
sctp-rto-max 450
```

# sctp-rto-min

This command sets the minimum retransmission timeout (RTO) value for the SCTP.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#
```

**Syntax Description**

```
sctp-rto-min [ units-10ms ] value
default sctp-rto-min
```

#### default

Resets the **sctp-rto-min** to the default of 10 (1 second).

#### units-10ms

Including this keyword, before entering a value, enables configuration with finer granuality - in 10 millisecond units.

#### *value*

If the **units-10ms** keyword is included, then set the timeout in increments of 10 milliseconds. The value must be an integer between 1 and 500.

If the **units-10ms** keyword is not included then set the timeout in increments of 100 milliseconds. The value must be an integer between 1 and 50.

**Usage Guidelines**

**Important** Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

Use this command to set the minimum time for retransmission before timeout.

The value set for **sctp-rto-min** should be less than or equal to the value set for **sctp-rto-initial** (**sctp-rto-min** <= **sctp-rto-initial**)

### Example

The following sets the timeout for 2 seconds:

```
sctp-rto-min 20
```

# sctp-sack-frequency

This command sets the frequency of transmission of SCTP selective acknowledgements (SACK).

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#
```

**Syntax Description**

```
sctp-sack-frequency [ units-10ms ] value
default sack-frequency
```

#### units-10ms

Including this keyword, before entering a value, enables configuration with finer granuality - in 10 millisecond units.

#### *value*

Sets the maximum number of datagrams to be received prior to sending a SACK to the peer. The value must be an integer between 1 and 5.

#### default

Resets the **sctp-sack-frequency** default value of 2.

**Usage Guidelines**



**Important** Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

Use this command to set the maximum number of datagrams to be received before a SACK must be sent to the peer. The **sctp-sack-frequency** is used in conjunction with the **sctp-sack-period** to control the generation of SACK, depending on which one occurs first.

### Example

```
sctp-sack-frequency 3
```

# sctp-sack-period

This command sets the delay before sending an SCTP selective acknowledgement (SACK).

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#
```

**Syntax Description**

```
sctp-sack-period [ units-10ms ] value
default sack-period
```

#### units-10ms

Including this keyword, before entering a value, enables configuration with finer granuality - in 10 millisecond units.

#### *value*

If the **units-10ms** keyword is included, then set the timeout in increments of 10 milliseconds. The value must be an integer between 0 and 50.

If the **units-10ms** keyword is not included then set the timeout in increments of 100 milliseconds. The value must be an integer between 0 and 5.

#### default

Resets the system to the **sctp-sack-period** default value, 2 (=200 milliseconds).

**Usage Guidelines**

Use this command to set the time the SCTP waits to send a SACK.

**Important** Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

**Example**

```
sctp-sack-period 3
```

# sctp-suppress-alarm

This command enables/disables the suppression of alarms for SCTP path failure between two peer endpoints.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#
```

**Syntax Description**

```
[ no ] sctp-suppress-alarm path-failure self-end-point-address
orig_ipv4_addresspeer-end-point-address peer_ipv4_address
```

**no**

Disables the pre-configured alarm suppression for SCTP path failure.

**path-failure**

This keyword specifies that the alarm suppression is for SCTP path failure between two peer nodes.

**self-end-point-address *orig_ipv4_address***

This keyword specifies the IP address of the originating endpoint.

*orig_ipv4_address* is the IP address of originating endpoint in IPv4 dotted decimal notation.

**peer-end-point-address *peer_ipv4_address***

This keyword specifies the IP address of the peer endpoint.

*peer_ipv4_address* is the IP address of peer endpoint in IPv4 dotted decimal notation.

**Usage Guidelines** Use this command to configure the path failure alarm suppression. This command ignores the alarms generated on SCTP path failure.



**Important** Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

### Example

The following command suppresses the path failure alarms occurred in SCTP path between originating peer address *209.165.200.228* and peer endpoint *209.165.200.233*:

**sctp-suppress-alarm path-failure self-end-point-address** *209.165.200.228* **peer-end-point-address** *209.165.200.233*

# shutdown

This command brings down and locks the SCTP association.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

`[local]`*host_name*`(config-ss7-rd-`*ss7rd_id*`-ps-peer-`*server_id*`-psp-`*psp_instance*`)#`

**Syntax Description** **[no] shutdown**

***no***

On configuring **no shutdown**, the PSP is marked unlocked and the SGSN initiates an association establishment towards the peer, if the SGSN is a client and it honors messages from the peer for association establishment, if SGSN is server. This is the default configuration for a PSP.

The default is **no shutdown**.

**Usage Guidelines** On configuring **shutdown**, the PSP is brought down via a SCTP Shutdown procedure (if association is already ESTABLISHED) or Abort (any other association state) and it is marked LOCKED. The SGSN does not initiate any messages towards the peer and any message from the peer will be responded with a SCTP Abort, when the PSP is in a LOCKED state.

### Example

The following command brings down and locks the SCTP association:

**shutdown**

# timeout

This command sets the times for various timeout timers.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type* **> peer-server id** *id* **> psp instance** *psp_instance*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#`

**Syntax Description**

**timeout { m3ua-periodic-dest-audit** *dest_timeout* **| sctp-bundle [ units-10ms ]** *timer* **| sctp-heart-beat** *hrt_bt_timeout* **}**
**[ default | no ] timeout { m3ua-periodic-dest-audit | sctp-bundle | sctp-heart-beat }**

#### default

Resets the specified command to the default value.

#### no

Removes the selected configuration.

#### m3ua-periodic-dest-audit *dest_timeout*

Sets the period (in increments of seconds) between the DAUD messages while auditing a destination state.

*dest_timeout:* Must be an integer from 1 to 65535. Default is 2.

#### sctp-bundle [ units-10ms ] *timer*

Specifies that SCTP data chunks are to be queued until this timer expires at which time the data chunks are bundled and committed for transmission. SCTP bundling provides better bandwidth utilization and less traffic, however, there is a packet transmission delay.

*timer* is an integer from 1 through 65535, in 100ms increments (10 = 1000ms or 1 second).

**[ units-10ms ]**: Including this optional keyword specifies that the integer *timer* is to be calculated using 10ms increments (instead of 100ms increments) to allow for finer granularity.

**Important** Peer end should also be configured to support SCTP bundling.

Default: SCTP bundling is disabled.

**sctp-heart-beat *hrt_bt_timeout***

Sets the number of seconds in the SCTP heart-beat timer

*hrt_bt_timeout*: This value is an integer between 1 and 300. Default is 30.

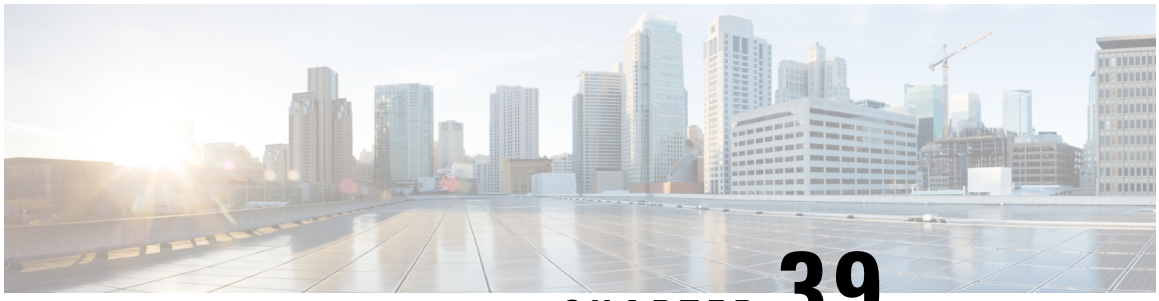
## Usage Guidelines

Use this command to configure timers. Repeat the command with each of the keywords to set values for each.

**Important** Before using this command to set a value, you must disassociate the PSP instance with the **no associate** command. When you have set the value with this command, then use the **associate** command to setup a new association.

### Example

```
timeout m3ua-periodic-dest-audit 120
```



CHAPTER 39

# SGSN Service Configuration Mode Commands

SGSN Service works with MAP Service, SGTP Service, GTPP Group, and IuPS Service. All five of these services must be configured to enable a 3G SGSN to communicate with other elements within a UMTS network.

## Command Modes

The SGSN Service configuration mode is used within the global configuration mode to specify the 3G operations of the SGSN and the available SGSN services for a specific context.

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

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

**Important** The commands should be added or removed in the startup config only and not when the node is live.


- accounting, on page 388
- admin-disconnect-behavior, on page 389
- associate, on page 391
- cc profile, on page 394
- check-imei, on page 396
- check-imei-timeout-action , on page 397
- core-network, on page 397
- disable/enable super-charger, on page 397
- dns israu-mcc-mnc-encoding, on page 398
- dns mcc-mnc-encoding, on page 399
- do show, on page 400
- end, on page 400
- exit, on page 401
- gmm, on page 401

- gs-service, on page 406
- lac, on page 407
- max-pdp-contexts, on page 408
- mobile-application-part, on page 409
- network-sharing cs-ps-coordination, on page 410
- nri length, on page 411
- override-lac-li, on page 413
- override-rac-li, on page 414
- qos-modification, on page 415
- rac, on page 416
- ran-protocol, on page 417
- reporting-action event-record, on page 417
- s4-overcharge-protection, on page 418
- sgsn-number, on page 419
- sgtp-service, on page 420
- sm, on page 421


# accounting

This command defines the accounting context name and enables/disables specific types of CDR generation for the accounting in the SGSN service.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure** > **context** *context_name* > **sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax Description**

```
accounting ( cdr-types { mcdr | scdr | sms { mo-cdr | mt-cdr }  | lcs {
mt-cdr  | mo-cdr  } | smbmscdr }+ | context  cntx_name  }
default accounting cdr-types
no accounting ( cdr-types | context }
```

**default**

Returns the system to default settings for the selected type of CDR.

**no**

Removes the pre-configured type of CDR generation for accounting from the SGSN service.

**cdr-types { mcdr | scdr | sms { mo-cdr | mt-cdr } | lcs { mt-cdr | mo-cdr }| smbmscdr }**

Default: enabled

Defines the types of CDRs to be generate:d within the specified SGSN service for accounting:

- **mcdr** Enables generation of M-CDRs.
- **scdr** : Enables generation of S-CDRs.
- **sms** : Enables generation of SMS-type CDRs based on one of the following:
  - **mo-cdr:** : SMS CDRs orignates from the mobile.
  - **mt-cdr:** SMS CDRs terminates at the mobile.
- **smbmscdr:** This CDR type is currently under development and should not be included in configuration for this release.
- **lcs:** Enables the generation of LCS CDRs, based on:
  - **mt-cdr:** Mobile terminated location request CDR
  - **mo-cdr:** Mobile originated location request CDR

**+**

Specifies that the specified keywords with in the group can be entered multiple times with a single command.

**context *cntx_name***

Specifies an accounting context to be associated with the SGSN service.

*cntx_name*: Define a string of 1 to 79 alphanumeric characters.

**Usage Guidelines**

Use this command to define the type of CDRs to generate for SGSN service. By default all type of CDRs are generated. Note that change of this configuration will be applied to new call and/or to new PDP contexts only.

By default, the generation of all CDR types is enabled.

**Example**

The following command configures the system to generate CDRs of M-CDR type for accounting in the current SGSN service:

```
accounting cdr-types mcdr
```

# admin-disconnect-behavior

This command defines some of the actions the SGSN will take during an Admin-Disconnect procedure.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

## Syntax Description

```
admin-disconnect-behavior { clear-subscription | detach-type {
reattach-not-required | reattach-required } }
[ default | no ] admin-disconnect-behavior { clear-subscription |
detach-type }
```

### clear-subscription

Including this keyword in the configuration instructs the SGSN to clear subscriber contexts and the subscription data database whenever the **clear subscribers all** command is issued (from the Exec mode) for attached subscribers. As well, the SGSN will issue an appropriate Map-Purge-MS-Req to the HLR if needed.

Default: disabled

### detach-type

Including this keyword defines which type of detach instruction to include in the Detach-Request message during an Admin-Disconnect procedure. One of the following options must be included when this command is entered:

- **reattach-not-required**
- **reattach-required**

Default: reattach-required

### default | no

Including either **default** or **no** keyword in the command, instructs the SGSN to use the default value for the specified parameter.

## Usage Guidelines

Include the **clear-subscription** keyword with this command configuration to ensure that more than attached MM-context and active PDP-contexts are cleared when the clear **subscribers all** command is issued for attached subscribers.

To clear subscription data for detached subscribers, refer to the **sgsn clear-detached-subscriptions** command described in the *Exec* mode chapter.

Including the **detach-type** keyword with this command instructs the SGSN to include either a 'reattach-required' or a 'reattach-no-required' instruction in the Detach-Request message.

### Example

Configure the SGSN to clear data such as PTMSI allocated, auth-vectors received, and NGAF flag values stored in the subscriber database for attached subscribers:

```
admin-disconnect-behavior clear-subscription
```

# associate

Associates or disassociates supportive services and policies, such as an Evolved GPRS Tunnelling Protocol (eGTP) service, an HSS peer service, or a MAP service.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax Description**

```
associate { { camel-service camel_svc_name [ context context_name ] |
egtp-service egtp_svc_name [ context context_name ] | gs-service gs_svc_name [
context context_name ] | hss-peer-service hss_svc_name [ context context_name ]
| map-service map_svc_name [ context context_name  ] |
network-global-mme-id-mgmt-db | sgtp-service sgtp_svc_name [ context
context_name ] | tai-mgmt-db database_name }
no associate { camel-service | egtp-service | gs-service | hss-peer-service
 | map-service | network-global-mme-id-mgmt-db  | sgtp-service |
tai-mgmt-db database_name }
```

**no**

Disassociates a previously associated service with this SGSN service.

**camel-service *camel_svc_name***

Associates a CAMEL service with SGSN service.

*camel_svc_name* specifies the name for a pre-configured CAMEL service to associate with the SGSN service.

**egtp-service *egtp_svc_name***

Associates an eGTP service with SGSN service.

*egtp_svc_name* specifies the name for a pre-configured eGTP service to associate with the SGSN service. For more information on the eGTP service, refer to the **egtp-service** command in the *Context Configuration Mode Commands* chapter.



**Important** Only one eGTP service can be associated with a SGSN service. The eGTP service should be configured prior to issuing this command.

**gs-service *gs_svc_name***

Associates a GS service with this SGSN service.

*gs_svc_name* specifies the name for a pre-configured GS service to associate with the SGSN service.



**Important** Only one Gs service can be associated with a SGSN service. The Gs service should be configured prior to issuing this command.

**hss-peer-service *hss_svc_name***

Associates an HSS peer service with this SGSN service.

*hss_svc_name* specifies the name for a pre-configured HSS peer service to associate with the SGSN service as an alphanumeric string of 1 through 63 characters. For more information about the HSS peer service, refer to the **hss-peer-service** command in the *Context Configuration Mode Commands* chapter and the *HSS Peer Service Configuration Mode Commands* chapter.



**Important** Only one HSS peer service can be associated to a service in this release. The HSS peer service should be configured prior to issuing this command.

**map-service *map_svc_name***

Associates a MAP service with this SGSN service.

*map_svc_name* specifies the name for a pre-configured MAP service to associate with the SGSN service.

The MAP service is created with the **map-service** command in the *Context Configuration Mode Commands* chapter. The MAP service provides Mobile Application Part (MAP) protocol support for the interface between the SGSN and the HLR. For more information on the MAP service, refer to the *MAP Service Configuration Mode Commands* chapter.



**Important** Only one MAP service can be associated with a SGSN service. The MAP service should be configured prior to issuing this command.

**network-global-mme-id-mgmt-db**

On the S4-SGSN, associates a pre-configured network global MME ID management database with the SGSN service. This enables operators to associate a single custom list of MME Group IDs for use in UMTS to E-UTRAN handovers on the S4-SGSN. The global MME ID management database must be configured on the S4-SGSN using the the **network-global-mme-id-mgmt-db**command in *LTE Policy Configuration Mode* before it can be associated with an SGSN service.

This command is available on the SGSN only if the *SGSN S4 Interface* license is enabled.

**sgtp-service *sgtp_svc_name***

Associates an SGTP service with this SGSN service.

*sgtp_svc_name* specifies the name for a pre-configured SGTP service to associate with the SGSN service as an alphanumeric string of 1 through 64 characters. For more information on the SGTP service, refer to the

**sgtp-service** command in the *Context Configuration Mode Commands* chapter and/or the *SGTP Service Configuration Mode Commands* chapter.



**Important** The SGTP service should be configured prior to issuing this command. Only one SGTP service can be associated with an SGSN service. When co-locating an SGSN and an MME, the SGSN Service cannot be associated with the same SGTP Service that is used by the MME.

**context *ctx_name***

Identifies a specific context name where the named service is configured. If this keyword is omitted, the named service must exist in the same context as the SGSN service.

*ctx_name* is name of the configured context of the named service expressed as an alphanumeric string of 1 through 63 characters that is case sensitive.

**tai-mgmt-db *database_name***

Associates this SGSN service with a pre-configured TAI Management Database.

*database_name* specifies the name of a pre-configured TAI Management Database to associate with the SGSN service as alphanumeric string of 1 through 64 characters. For more information, refer to the **tai-mgmt-db** command in the *LTE Policy Configuration Mode Commands* chapter and the *LTE TAI Management Database Configuration Mode Commands* chapter.

This command is available on the SGSN only if the *SGSN S4 Interface* license is enabled.

## Usage Guidelines

Use this command to associate a pre-configured service or policy with an SGSN service.

The eGTP service provides eGTP-C protocol interface support between EPS nodes. For more information on the eGTP service and the supported interface type, refer to the *eGTP Service Configuration Mode Commands* chapter.



**Important** Only one eGTP service can be associated with a service. The eGTP service should be configured prior to issuing this command.

The HSS peer service provides S6d and S13-prime interface support via the Diameter protocol between the SGSN and an HSS (S6d) or EIR (S13-prime). For more information on HSS peer service and other parameters, refer to the *HSS Peer Service Configuration Mode Commands* chapter.



**Important** Only one HSS peer service can be associated to a service in this release. The HSS peer service should be configured prior to issuing this command.



**Caution** This is a critical configuration. The SGSN service cannot be started without this configuration. Any change to this configuration would lead to restarting the SGSN service. Removing or disabling this configuration will stop the SGSN service.

### Example

The following command associates a pre-configured eGTP service called *egtp1* in the *dst_ctx* context to an SGSN service:

```
associate egtp-service egtp1 context dst_ctx
```

The following command associates a pre-configured HSS peer service called *hss1* in the same context as SGSN service to an SGSN service:

```
associate hss-peer-service hss1
```

# cc profile

Configures the charging characteristic (CC) profile with the triggers for generating various types of CDR as defined with the **accounting** command.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax Description**

**cc profile** *profile_bits* **[ buckets** *number* **| interval** *time* **| tariff time1** *mins hours* **[ time2** *mins hours* **] [ time3** *mins hours* **] [ time4** *mins hours* **] | volume { downlink** *down_vol* **uplink** *up_vol* **| total** *total_vol* **} ] +**
**[ no | default ] cc profile** *profile_bits* **[ buckets | interval | tariff | volumne ]**

#### no

Removes a previously configured CC profile.

#### default

Returns the specified CC profile to the original default system settings.

#### *profile_bits*

Defines the value of the profile bits for the SGSN service.

*index* can be configured to any integer value from 0 to 15. Some of the values have been predefined according to 3GPP standard:

- 1 for hot billing
- 2 for flat billing

- 4 for prepaid billing
- 8 for normal billing

**buckets *number***

Specifies the number of statistics container changes in the CDR due to QoS changes or tariff times that can occur before an accounting record (CDR) is closed

Default: 4

*number* : Must be integer from 1 to 4.

**interval *time***

Specifies the normal time duration (in seconds) that must elapse before closing an accounting record (CDR) provided that any or all of the following conditions occur:

*time* : Enter any integer from 60 to 40000000.

**tariff time1 *mins hours* [ time2 *mins hours* time3 *mins hours* time4 *mins hours* ]**

Specifies the time-of-day (based on a 24-hour clock) to close the current statistics container in the CDR, but not necessarily the CDR itself. One tariff time must be defined and up to four tariff times can be specified.



**Important** The system assumes that the billing system uses the day/date to determine if the statistics container represents an actual tariff period.

- *mins*: The minutes of the hour. Enter an integer from 0 to 59.
- *hours*: The hour of the day. Enter an integer from 0 to 23.

**volume { downlink *down_vol* uplink *up_vol* | total *total_vol* }**

Specifies the downlink, uplink, and total volumes octet counts that must be met for the closure of the CDR.

*down_vol* : Enter any integer from 100000 to 1345294336.

*up_vol* : Enter any integer from 100000 to 400000000.

*total_vol* : Enter any integer from 100000 to 400000000.

## Usage Guidelines

Charging characteristics consist of a profile index and behavior settings. This command configures the profile index for the SGSN's charging characteristics. The SGSN supports up to 16 profile indexes.

### Example

The following command configures a profile index of 10 with tariff times of 7:00 AM and 7:30 PM:

```
cc profile 10  tariff time1 0 7 time2 30 19 time3 0 7 time4 30 19
```

# check-imei

This command configures the action the SGSN will take if the route towards the EIR is down.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax Description**

```
check-imei { gf-failure-action | gf-timeout-action } { continue | reject
 }
default check-imei { gf-failure-action | gf-timeout-action }
```

#### default

Resets the default function to reject the Attach.

#### gf-failure-action

Coupled with either **continue** or **reject**, this keyword instructs the SGSN to take action if a valid EIR configuration exists under the MAP service and if the EIR is temporarily unreachable due to associated DPC/SSN inaccessible/out-of-service.

#### gf-timeout-action

Coupled with either **continue** or **reject**, this keyword instructs the SGSN to take action if a valid EIR configuration exists under the MAP service and the route to the EIR is available, but no response is received from the EIR.

#### continue

Instructs the SGSN to continue the Attach process.

#### reject

Instructs the SGSN to reject the Attach process.

**Usage Guidelines**

Typically, the Attach process will be continued when there is an IMEI check timeout based on the configuration under the SGSN service configuration and/or the GPRS service configuration. But this works only if the route towards the EIR is UP and the IMEI request timer expires. This command configures the SGSN to allow the Attach process to continue in the case the route towards the EIR is down, that is the DPC / SSN is out-of-service.

#### Example

Use the following command to reset the default and reject Attach:

```
default check-imei gf-failure-action
```

# check-imei-timeout-action

In Releases 12.0 and higher, this command has been replaced with enhanced functionality in the **check-imei** command, also available in this configuration mode.

# core-network

This command specifies the numeric ID for a core network to identify which CN is to be used by the SGSN service.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax Description**

**core-network id** *cn_id*
**no core-network id**

**no**

Removes the currently configured core network ID from the current SGSN configuration.

**id *cn_id***

This number identifies the core network to connect the SGSN service.

*cn_id* : Must be an integer from 0 through 4095.

**Usage Guidelines**

Use this command to set a global ID to identify this SGSN in the core network.

**Example**

The following command sets the core network ID for the current SGSN service to 127:

**core-network id** *127*

# disable/enable super-charger

This command has been deprecated and replaced by the **super-charger** command. For the commands to configure the SuperCharger feature, refer to the *Call-Control Profile Configuration Mode* chapter.

# dns israu-mcc-mnc-encoding

Configures either decimal or hexadecimal format for the MCC and MNC values in the DNS query which is sent during the ISRAU.

This command is deprecated from release 16.0 onwards, it is replaced by the **dns mcc-mnc-encoding** command. See the **dns mcc-mnc-encoding** command for more information.

## Product

SGSN

## Privilege

Security Administrator, Administrator

## Command Modes

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

## Syntax Description

```
dns israu-mcc-mnc-encoding { decimal | hexidecimal }
default dns israu-mcc-mnc-encoding
```

### default

Resets the SGSN to send the MCC and MNC values in decimal format for DNS queries.

### decimal

Default.

Instructs the SGSN to send the MCC and MNC in decimal format in the DNS query.

### hexadecimal

Instructs the SGSN to send the MCC and MNC in hexadecimal format in the DNS query.

## Usage Guidelines

Use this command to determine the type of encoding for the MCC and MNC to be included in the DNS query sent during the inter-SGSN RAU (ISRAU). The choice must match the format of the DNS server. For example:

In decimal, the MNC/MCC in a DNS query would appear like:

```
rac0017.lac42e3.mnc310.mcc722.gprs
```

In hexadecimal, the MNC/MCC in a DNS query would appear like:

```
rac0017.lac42e3.mnc0136.mcc02d2.gprs
```

### Example

Use hexadecimal values for the MCC/MNC in the DNS query.

```
dns israu-mcc-mnc-encoding hexadecimal
```

# dns mcc-mnc-encoding

Configures the encoding format for the MCC and MNC values in the DNS query.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax Description**

```
dns mcc-mnc-encoding  { apn-fqdn | mmec-fqdn | rai-fqdn| rnc-fqdn|
tai-fqdn }* { a-query | snaptr-query }*  { decimal | hexadecimal }
default dns mcc-mnc-encoding
```

**default**

Resets the SGSN to send the MCC and MNC values in decimal format for DNS queries.

**apn-fqdn**

This keyword is used for PGW/GGSN selection during PDP activation.

**mmec-fqdn**

This keyword is used for Peer MME selection during MME to SGSN ATTACH/RAU procedure and Suspend procedure.

**rai-fqdn**

This keyword is used for SGW selection, Peer SGSN selection during RAU/Attach procedure, Suspend procedure and RIM procedure.

**rnc-fqdn**

This keyword is used for Peer SGSN selection during SRNS re-location.

**tai-fqdn**

This keyword is used for Peer MME selection during SGSN to MME SRNS re-location and RIM procedure.

**a-query**

This keyword is used to control the DNS A/AAAA query MCC/MNC encoding format.

**snaptr-query**

This keyword is used to control the DNS SNAPTR query MCC/MNC encoding format.

**decimal**

Default

Instructs the SGSN to send the MCC and MNC in decimal format in the DNS query.

**hexadecimal**

Instructs the SGSN to send the MCC and MNC in hexadecimal format in the DNS query.

**Usage Guidelines**

In order to provide effective control on DNS queries for particular type of procedures, existing CLI commands in GPRS and SGSN services have been deprecated and replaced with new enhanced commands. The command **dns israu-mcc-mnc-encoding [hexadecimal | decimal]** has been deprecated and this new CLI command is introduced. New keyword options **snaptr-query** and **a-Query** are provided to control different types of queries.

**Example**

Use the following command to configure hexadecimal encoding in the DNS query:

```
dns mcc-mnc-encoding rai-fqdn apn-fqdn mmec-fqdn rnc-fqdn tai-fqdn a-query
 hexadecimal
```

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution**

There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Return to the Exec mode.

# exit

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

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

**Usage Guidelines** Return to the context configuration mode.

# gmm

This command defines the GPRS mobility management parameters for the SGSN service.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-sgsn-service)#`

**Syntax Description**

**gmm { [ Extended-T3312-timeout { value** *exT3312_minutes* **| when-subscribed }** **[ low-priority-ind-ue ] ] | T3302-timeout** *t3302_dur* **| T3312-timeout** *t3312_dur* **| T3313-timeout initial** *t3313_init* **[ decrease** *t3313_decrement* **| increase** *t3313_increment* **] | T3322-timeout** *t3322_dur* **| T3323-timeout** *T3323_dur* **| T3350-timeout** *t3350_dur* **| T3360-timeout** *t3360_dur* **| T3370-timeout** *t3370_dur* **|** **implicit-detach-timeout** *secs* **| max-auth-retransmission** *auth_retrans* **|** **max-identity-retransmission** *id_retrans* **| max-page-retransmission** *page_retrans* **| max-ptmsi-reloc-retransmission** *ptmsi_reloc_retrans* **|** **mobile-reachable-timeout** *ms_reach_dur* **| paging-failure-action** **downlink-data-lockout-timer** *seconds* **[ repeat** *number_repeats* **] |** **perform-identity-on-auth-failure | purge-timeout** *minutes* **| t3346 min** *minimum* **max** *maximum* **| trau-timeout** *trau_dur* **}**
**default gmm { T3302-timeout | T3312-timeout | T3313-timeout | T3322-timeout | T3323-timeout | T3350-timeout | T3360-timeout | T3370-timeout |**

```
implicit-detach-timeout | max-auth-retransmission |
max-identity-retransmission | max-page-retransmission |
max-ptmsi-reloc-retransmission | mobile-reachable-timeout |
perform-identity-on-auth-failure | purge-timeout | trau-timeout }
no gmm  {Extended-T3312-timeout | implicit-detach-timeout |
max-auth-retransmission | max-identity-retransmission |
perform-identity-on-auth-failure | t3346 }
```

**default**

Sets the default value for the specified parameter.

**Extended-T3312-timeout**

This keyword enables the operator to determine how the SGSN handles Extended T3312 timer values in a 3G UMTS network environment.

- **value** : This keyword instructs the SGSN to send the defined Extended T3312 timer value in Attach or RAU Accept messages to the MS if the subscriber has a subscription for the Extended T3312 timer (Subscribed Periodic RAU/TAU Timer in ISD) and indicates support for the extended periodic timer via the MS Network Feature Support.
- *exT3312_minutes* : Enter an integer from 0 to 18600 to identify the number of minutes for the timeout; default is 186 minutes.
- **when-subcribed**: This keyword instructs the SGSN to only send the extended T3312 period RAU timer value in Attach or RAU Accept messages if the SGSN receives the timeout value in an ISD when the MS has indicated support in MS Network Feature Support.
- **low-priority-ind-ue**: This keyword instructs the SGSN to include the extended T3312 timer value only if the Attach/RAU Request messages include a LAPI (low access priority indicator) in the "MS Device Properties".
- **no**: This command filter instructs the SGSN to remove the extended T3312 configuration from the SGSN Service configuration.

**T3302-timeout *t3302_dur***

Default: 10

Specifies the retransmission timer value to guard the GPRS attach or RAU procedure on MS side.

*t3302_dur* is the waiting duration in minutes before retransmitting the specific message and must be an integer from 1 through 186.

**T3312-timeout *t3312_dur***

Default: 54

Specifies the retransmission timer value to guard the RAU procedure initiation on network side.

*t3312_dur* is the waiting duration in minutes before retransmitting the specific message and must be an integer from 1 through 186.

**T3313-timeout initial *t3313_init* [ decrease *t3313_decrement* | increase *t3313_increment* ]**

Default: 5

Specifies the retransmission timer value to guard the for paging request procedure initiation on network side.

**initial** *t3313_init* - Specifies the initial wating duration in seconds before retransmitting the specific message. *t3313_init* must be an integer from 1 through 60.

**decrease** *t3313_decrement* - Specifies the decrement of the initial timer value in seconds. *t3313_decrement* must be an integer from 1 through 5.

**increase** *t3313_increment* - Specifies the increment of the initial timer value in seconds. *t3313_decrement* must be an integer from 1 through 5.

#### T3322-timeout *t3322_dur*

Default: 6

Specifies the retransmission timer value to guard the GPRS detach request procedure on network side.

*t3322_dur* is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 20.

#### T3323-timeout *T3323_dur*

Default: 54

Specifies that the S4-SGSN Idle Mode Signaling Reduction T3323-timeout deactivation timer will be sent to the UE in Attach Accept and Routing Area Update Accept Messages.

*T3323_dur*specifies the amount of time, in minutes, that will transpire before the UE deactivates the ISR feature if the UE is no longer in the UMTS coverage area and has not completed a Routing Area Update with the S4-SGSN within the specified time duration. Once the timer expires, the S4-SGSN waits an additional four minutes before beginning an Implicit Detach for the UE and sends a Detach Notification message (cause = local detach) to the MME across the S3 interface. The MME will then deactivate ISR for the UE since it now also is aware that the UE is no longer in the UMTS coverage area. Valid entry is an integer from 1 to 186.

This command is available only if the *Idle Mode Signaling Reduction* license is enabled on the S4-SGSN and the Idle Mode Signaling Reduction feature has been activated via the **idle-mode-signaling-reduction** command in *Call Control Profile Configuration Mode*.

#### T3350-timeout *t3350_dur*

Default: 6

Specifies the retransmission timer value to guard the GPRS attach accept/RAU accept/realloc request procedure sent with P-TMSI and/or TMSI on network side.

*t3350_dur* is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 20.

#### T3360-timeout *t3360_dur*

Default: 6

Specifies the retransmission timer value to guard the authentication and cipher request procedure on network side.

*t3360_dur* is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 20.

**T3370-timeout *t3370_dur***

Default: 6

Specifies the retransmission timer value to guard the identity request procedure on network side.

*t3370_dur* is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 20.

**implicit-detach-timeout *secs***

Default: 3600

Specifies the implicit detach timer (IDT) timeout value for any 3G calls (not specific to ISR activated calls) as part of the implicit detach procedure on the network side. The IDT starts after expiry of the mobile reachable timer (MNR). Soon after IDT expiry, the subscriber is implicitly detached from the SGSN.

*secs* value must be an integer from 1 to 86400.



**Important** From R15.0 release onwards the lowest configurable limit of the IDT timeout is modified to "240" seconds.

**max-auth-retransmission *auth_retrans***

Default: 4

Specifies the maximum retransmission of authentication requests allowed.

*auth_retrans* is the number of retries before declaring the authentication failure and must be an integer from 1 through 10.

**max-identity-retransmission *id_retrans***

Default: 4

Specifies the maximum retransmission of identity requests allowed.

*id_retrans* is the number of retries before declaring the identity failure and must be an integer from 1 through 10.

**max-page-retransmission *page_retrans***

Default: 5

Specifies the maximum retransmission of page requests allowed.

*id_retrans* is the number of retries before declaring the paging request failure and must be an integer from 1 through 5.

**max-ptmsi-reloc-retransmission *ptmsi_reloc_retrans***

Default: 5

Specifies the maximum retransmission for P-TMSI relocation procedure allowed.

*id_retrans* is the number of retries before declaring the P-TMSI relocation procedure failure and must be an integer from 1 through 10.

**mobile-reachable-timeout *ms_reach_dur***

Default: 58

Specifies the timeout duration for the mobile reachable timer (MNR) for the mobile reachable procedure on network side.

*impli_detach_dur* sets the waiting duration in minutes before retransmitting the specific message and must be an integer from 4 through 1440.

**paging-failure-action downlink-data-lockout-timer *seconds* [ repeat *number_repeats* ]**

Default: 1000 seconds.

Enables and configures the downlink data lockout timer, for the SGSN services, to reduce the frequency of mobile-initiated keep alive messages.

*seconds* set the number of seconds before timer expire, range of 0 to 10000.

**repeat** *number_repeats* optionally sets the number of times (1 to 10) that the timer restarts after paging failure. **Note**: If repeat is not configured then paging proceeds endlessly until the MR timer expires.

**[ default | no ] gmm paging-failure-action** disables the downlink data lockout timer.

**perform-identity-on-auth-failure**

Default: Enabled

Configures the SGSN service to perform an identity check to ascertain the IMSI after an authentication failure on a PTMSI-based message.

Beginning with Release 19.2, a new default behavior has the SGSN initiate the Identity Procedure

- (1) on receiving authentication failure with cause "GSM Authentication Unacceptable" from a 3G subscriber during an Attach/RAU, or
- (2) on receiving authentication failure with cause "MAC failure" during 2G ISRAU.

**purge-timeout *minutes***

Default: 10080 (7 days)

The purge timer defines the MM-context lifetime, part of the MM-context procedure on the network side. The configured value sets the duration (number of minutes) the SGSN holds the detached subscriber's MM-context profile. If the subscriber does not reattach to the SGSN during this time, then the SGSN purges this detached subscriber's MM-context information from its database and sends a MAP purge request towards the HLR to indicate that the subscribers profile is gracefully purged from SGSN's database.

*minutes* must be an integer from 1 through 20160.

**t3346**

This keyword enables the mobility management (MM) T3346 back-off timer for the 3G service. When the SGSN is confronted by a situation involving congestion, the SGSN can assign the back-off timer value to the UEs and requests the UEs not to access the network for a given period of time.

**min** *minimum*: Enter an integer from 1 to 15 to identify the minimum number of minutes that the timer will run; default is 15 minutes.

**max** *maximum*: Enter an integer from 1 to 30 to identify the maximum number of minutes the timer can run; default is 30 minutes.

- If an Attach Request or RAU Request or Service Request is rejected due to congestion, then the T3346 value will be included in the reject message with GMM cause code 22 (congestion). The MM back-off timer value sent will be chosen randomly from within the configured T3346 timer value range.
- The timer will be ignored if an Attach Request or RAU Request is received after congestion has cleared.
- If T3346 timer value is configured in a Call-Control Profile then that value will override the back-off timer values defined for this SGSN Service configurations.

**trau-timeout *trau_dur***

This timer is available in releases 9.0 and higher.

Default: 30

Specifies the number of seconds the "old" 3G SGSN waits to purge the MS's data. This timer is started by the "old" SGSN after completion of the inter-SGSN RAU.

*trau_dur* : Must be an integer from 5 to 60.

**Usage Guidelines**

Repeat this command as needed to configure multiple parameters for GPRS mobility management in a UMTS network. This command provides the configuration of timers for mobility procedures and retries for different messages. GMM layer is defined in the 3GPP TS 24.008 (Release 7).

**Example**

Following command configures the timer to wait for *5* mins before retransmitting the message for GPRS attach or RAU procedure on MS side with maximum number of retries as *6* for authentication:

```
gmm T3302-timeout 5 max-auth-retransmission 6
```

# gs-service

This command associates a previously defined Gs service configuration, for the Gs interface to an MSC/VLR, with this SGSN service.



**Important** This command is used in Releases 12.0 and 12.2. For Release 14.0 refer to the **associate** command.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax Description**

**gs-service** *gs_srvc_name* **context** *ctx_name*
**no gs-service** *gs_srvc_name*

**no**

Removes/disassociates the named Gs service from this SGSN service.

***gs_srvc_name***

Specifies the name of a specific Gs service for which to display information.

*svc_name* is the name of a configured Gs service and can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

**context *ctx_name***

Specifies the specific context name where Gs service is configured. If this keywork is omitted, the named Gs service must be exist in the same context as the SGSN service.

*ctx_name* is name of the configured context of Gs service. This can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

**Usage Guidelines**

Use this command to associate a specific Gs service interface with this SGSN service instance.

**Important** A single Gs service can be used with multiple SGSN and/or GPRS service.

**Example**

Following command associates a Gs service instance named *stargs1*, which is configured in context named *star_ctx*, with an SGSN service:

**gs-service** *stargs1* **context** *star_ctx*

# lac

This command defines the location area code (LAC) in hexadecimal format.

**Note** This command is new in releases 8.1 and higher.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure** > **context** *context_name* > **sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax Description**

**lac** *hex*
**no lac**

**no**

Erases the **lac** configuration statement.

***hex***

Enter a hexadecimal number between 0x0 and 0xFFFF

# max-pdp-contexts

Configures the maximum number of PDP contexts for a MS (mobile station) that will be supported on this SGSN service.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax Description**

**max-pdp-contexts per-ms** *number*
**default max-pdp-contexts per-ms**

**default**

Resets the maximum number of PDP contexts per mobile station to the default of 11 for the Gs service configuration

**per-ms *number***

Default: 11

Defines the combined total number of primary and secondary PDP contexts for the SGSN service.

*number* can be an integer from 2 to 11.

**Usage Guidelines**

The following example defines 5 as the maximum number of primary and secondary PDP contexts that this SGSN will support for any connected MS.

### Example

```
max-pdp-contexts per-ms 5
```

# mobile-application-part

This command identifies an already defined MAP service (Mobile Application Part service) to associate with the SGSN service. Although the MAP service does not need to be defined in the same context as the SGSN service, there is a one-to-one relationship between a MAP service and an SGSN service.

**Important** This command is used in Releases 12.0 and 12.2. For Release 14.0 refer to the **associate** command.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax Description**

**mobile-application-part service** *map_srvc* **[ context** *ctx_name* ]
**no mobile-application-part service**

#### no

Remove the MAP service association from the SGSN service configuration.

#### service *map_srvc*

Specifies the name of the MAP service to be associated with this SGSN service.

*map_srvc* must be the name of a MAP service previously configured on the system.

#### context *ctx_name*

Specifies the name of the context where the MAP service is configured. If the MAP service is not configured in the current context, then the context where it is configured must be specified to enable the SGSN to reach the MAP service.

If this keyword is not specified, the current context is used.

*ctxt_name:* Must be the name of the context where the specified MAP service is configured.

**Usage Guidelines**

Use this command to identify the MAP service configuration to be used by the SGSN service configuration. Also use this command to specify the context in which the MAP service configuration was created.

If the MAP service is not identified or if the correct context is not identified, then the SGSN service will not START.

### Example

The following command specifies a MAP service named map1 that is configured in the same context as the current SGSN service:

**mobile-application-part service** *map1*

# network-sharing cs-ps-coordination

Enables/disables the SGSN service to perform a CS-PS coordination check.

**Important** This command is no longer available in all 12.0 and 12.2 releases. If you do not see this command in your release, look for the **network-sharing cs-ps-coordination** command in the IuPS Service configuration mode to accomplish the same task. Configuring in the IuPS Service configuration mode allows for the possibility of multiple IuPS services with network-sharing and differing CS-PS coordination requirements.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

*[context_name]host_name*(config-sgsn-service)#

**Syntax Description**

**network-sharing cs-ps-coordination**
**default network-sharing cs-ps-coordination**
**no network-sharing cs-ps-coordination**

#### default

Including this keyword resets the SGSN service to allow the check to be performed.

#### no

Disables this feature for the SGSN service.

**Usage Guidelines**

Use this command to facilitate the network sharing functionality. With this command, the SGSN can be instructed to perform a check to determine if CS-PS coordination is needed.

3GPP TS 25.231 section 4.2.5 describes the functionality of the SGSN to handle CS-PS (circuit-switching/packet-switching) coordination for attached networks not having a Gs-interface. In compliance with the standard, the SGSN rejects an Attach in a MOCN configuration with cause 'CS-PS coordination

required', after learning the IMSI, to facilitate the RNC choosing the same operator for both CS and PS domains.

### Example

Use the following syntax to disable the CS-PS coordination check:

```
no network-sharing cs-ps-coordination
```

# nri length

This command defines the Network Resource Identifier (NRI) of the SGSN that is stored in the P-TMSI (bits 23 to 18).

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax Description**

```
nri length  nri_length [ nri-value nri_value | null-nri-value null_nri_value
non-broadcast mcc mcc mnc mnc lac lac_id rac rac_id nri-value value
non-pooled-nri-value value ]
default nri
no nri
```

### default

Release 14.0 and higher.

Resets the nri configuration to **nri length** 6 and **nri-value** 0.

### no

Deprecated in Release 14.0

Releases prior to 14.0, this command removes the configured NRI value and location information in the P-TMSI that would be retrieved by this SGSN.

### nri length *nri_length*

Specifies the number of bits to be used in the P-TMSI, bits 23 to 18. to define the network resource identifier (NRI). The NRI length configuration also sets the maximum size of the pool. If not configured, the NRI length will be of zero length.

*nri_length* : Must be an integer from 1 to 6 to identify the number of bits.

**null-nri-value *null_nri_value***

This keyword is only available in releases 8.1 and higher.

Configures the null NRI value which must be unique across the pool areas. This keyword is used for the offloading procedure for SGSN pooling (enabled with the **sgsn offloading** command, see the Exec Mode chapter).

*null_nri_value* is an integer 0 (zero) to 63 which identifies the SGSN to be used for the offloading procedure for SGSN pooling. There is no default value for this parameter.

**non-broadcast mcc *mcc* mnc *mnc* lac *lac_id* rac *rac_id***

This keyword set is only available in releases 8.1 and higher.

Defines the non-broadcast LAC/RAC to be used in combination with the null-NRI for the offloading procedure. Including the MCC and MNC to specify the PLMN because the Iu-Flex feature supports multiple IuPS Services.

*mcc* identifies the mobile country code, the first part of the PLMN ID. Must be an integer between 100 and 999.

*mnc* identifies the mobile network code portion of the PLMN ID. Must be a 2- or 3-digit integer between 01 and 999.

*lac_id* defines a location area code associated with an RNC. Must be an integer between 1 and 65535.

*rac_id* defines the remote area code to be associated with an RNC. Must be an integer between 1 and 255.

**nri-value *nri_value***

Specifies the MS-assigned value of the NRI to retrieve from the P-TMSI. This value must not exceed the maximum possible value specified by the NRI length. The NRI value must be unique across the pool or across all overlapping pools.

*nri_value* must be an integer from 1 to 63 to identify a specific SGSN in a pool. Use of 0 (zero) value is not recommended.

Multiple NRI values can be identified by providing multiple nri-values separated by a blank space for example: **nri length** *6* **nri-value** *29 43 61*

The NRIs configured using this keyword will be used only in pooled area if the keyword **non-pooled-nri-value** is configured, else the NRIs configured using the **nri-value** keyword will be used for both pooled and non-pooled areas.

**non-pooled-nri-value *value***

If pooling is supported (the **null-nri-value** keyword is configured) use this keyword to configure values of NRIs to be used for non-pooled area. If the NRI CLI is configured as **nri length** *length_value* **nri-value** *values* **non-pooled-nri-value** *values* (null-nri-value is not configured, that is pooling not supported at SGSN) , NRIs will be used from "non-pooled-nri-value" irrespective of RNC/BSC being pooled or non-pooled.

**Note** The same NRI can be configured using both the keywords **nri-value** and **non-pooled-nri-value**, this implies the NRI can be used either in pooled area or non-pooled area. If an NRI is configured for both pooled and non-pooled areas, then the SGSN re-uses the same NRI when moving from pooled to non-pooled areas and vice versa.

**Usage Guidelines**

Use this command to identify the SGSN identified with the NRI in the MS generated P-TMSI.

This command adds or removes the Iu Flex configuration for this SGSN service. When using Iu Flex, all keywords must be defined. The command can be repeated to specify different values for any of the keyword parameters. If more than one NRI is configured, the SGSN service will round-robin between the available NRIs when new subscribers (re)connect.

Use this command to retrieve the NRI (identity of an SGSN) stored in in bits 23 to 18 of the packet-temporary mobile subscriber identity (P-TMSI). If more than one NRI value is configured, the SGSN service will round-robin between the available NRIs when new subscribers (re)connect.

When using MOCN mode for network sharing without SGSN pooling, the NRI length and the NRI value should both be used.

**Important** In Releases prior to 14.0, selection of one of the keywords (**nri-value** or **null-nri-value**) was manadatory. With Release 14.0 use of the keywords is optional.

### Example

The following command specifies the the NRI length as *5* bits, identifies SGSN *23* with MCC *123* and MNC *22* and LAC *222* and RAC *12* for offloading procedure with NRIs *6* and *41*:

```
nri length 5 null-nri-value 34 non-broadcast mcc 123 mnc 22 lac 222 rac
12 nri-value 6 41
```

# override-lac-li

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

# LI-specific

This command defines the override routing area code needed for the lawful intercept function.

**Note** This command is available in releases 8.1 and higher.

**Product**

SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-sgsn-service)#`

**Syntax Description**

**rac** *hex*
**no rac**

**no**

Erases the routing area code configuration statement.

***hex***

Enter a hexadecimal number between 0x0 and 0xFFFF

# override-rac-li

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

# Li-specific

This command defines the override routing area code needed for the lawful intercept function.

**Note** This command is only available in 8.0 releases.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-sgsn-service)#`

**Syntax Description**

**override-rac-li** *hex*
**no override-rac-li**

**no**

Erases the override routing area code for this GGSN service from the configuration.

***hex***

Enter a hexadecimal number between 0x0 and 0xFFFF

# qos-modification

This command provides the operator the flexibility to control RAB setup and negotiations based on the RNC.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax Description**

```
qos-modification { inform-rnc-before-ue | allow-s4-rab-negotiation
[inform-pgw]}
no qos-modification [ inform-rnc-before-ue | allow-s4-rab-negotiation
[inform-pgw]]
```

**no**

The SGSN uses the default behavior

- to inform the UE before the RNC or
- to reject PDP Context Activation (in compliance with TS 23.00 section 9.2.2.1A), if the RNC negotiates QoS in the RAB assignment response when the S4 interface is used for the PDP context.

**inform-rnc-before-ue**

When this keyword is used the SGSN informs the RNC of new QoS before informing the UE. On execution of the command with this keyword, the SGSN initiates a RAB assignment to inform the RNC followed by UPCQ towards the GGSN / Modify towards the UE based on whether or not the RNC downgrades the QoS.

**allow-s4-rab-negotiation**

With this keyword used as part of the configuration, if the S4 interface is used for PDP activation then the SGSN locally accepts what the RNC sends as QoS in the RAB Assigment Response and sends that QoS in the Activate Response.

This CLI is applicable only for PDP activation. For any other scenario, if the RNC negotiates the QoS then the SGSN ignores this configuration and locally accepts the change and continues with the call.

**inform-pgw**

This CLI option is used to enable or disable sending of Modify Bearer Command to the PGW. By default this option is disabled. When this option is enabled, the S4-SGSN triggers a Modify Bearer Command if QoS is downgraded by the RNC in RAB Assignment Procedure. To avoid looping of messages between S4-SGSN and PGW, PCRF should be configured to "NOT" upgrade QoS when RAT-Type is 3G.

**Usage Guidelines**

This command enables the operator the flexibility to accommodate legacy RNCs that don't meet the parameters set by TS 23.060.

With **allow-s4-rab-negotiation**, this keyword is needed for activation cases only as the default behaviour, per 3GPP spec, is to reject activation, which is service impacting. Hence to avoid such service impacts a configuration is added to control the behavior

**Example**

Use this command to override the SGSN default behavior during the PDP modification procedure.

**qos-modification inform-rnc-before-ue**

Use this command to override the SGSN default behavior and accept PDP activation with legacy RNCs using the S4 interface for context activation:

**qos-modification allow-s4-rab-negotiation**

# rac

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

# LI-specific

This command defines the override routing area code needed for the lawful intercept function.



**Note** This command is available in releases 8.1 and higher.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-sgsn-service)#`

**Syntax Description**

**rac** *hex*
**no rac**

**no**

Erases the routing area code configuration statement.

***hex***

Enter a hexadecimal number between 0x0 and 0xFFFF

# ran-protocol

This command specifies the IuPS service for the SGSN service to use for communication with the RAN.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax Description**

```
ran-protocol iups-service iups_srvc [ context ctx_name ]
no ran-protocol iups-service
```

**no**

Removes the IuPS service information from the SGSN service configuration.

**iups-service *iups_srvc***

Specifies the name of an IuPS service already configured on the system.

*iups_srvc* : Enter an alphanumeric string of 1 to 63 characters.

***ctx_name***

*ctx_name* : Enter the name of the IuPS context, an alphanumeric string of 1 to 63 characters.

**Usage Guidelines**

Use this command to configure the IuPS service context that the current SGSN service will use to communicate with the RAN. Up to 8 definitions can be defined for a single SGSN service to allow for multiple PLMNs support.

**Example**

The following command configures the SGSN service to use an IuPS service named **iups1** that has been configured. in the same context as the SGSN service:

```
ran-protocol iups-service iups1
```

# reporting-action event-record

This command enables the SGSN to log GMM/SM events in EDR files for 3G services.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax Description**

```
reporting-action event-record
[ default | no ] reporting-action event-record
```

**default**

Disables the logging function.

**no**

Removes the logging function from the configuration file.

**Usage Guidelines**

This command is one of the steps needed to enable the SGSN to create a log for events such as Attach, RAU, and Activations. The log is an EDR (event data record) in CSV format. For details about how this feature works, refer to the *GMM-SM Event Logging* chapter in the *SGSN Administration Guide*.

**Related Commands:**

- To enable GMM/SM event logging for 2G services, the **reporting-action event-record** command must be configured in the GPRS service configuration.
- To enable a log to be generated in an EDR file, the **edr-module active-charging-service** command must be enabled in the Context configuration mode.
- To configure parameters for the logging file characteristics and for file transfer, use the commands in the EDR Module Configuration Mode.

**Example**

Enable GMM/SM event logging for 3G services:

```
reporting-action event-record
```

# s4-overcharge-protection

This command enables or disables Subscriber Overcharging Protection functionality for the S4-SGSN in the 3G network *and* associates a RANAP cause code group with the SGSN Service configuration.

**Product**



**Important** We recommend that you enable Release Access Bearer, with the **release-access-bearer command** in the Call-Control Profile configuration mode, *before* this **s4-overcharge-protection** command is used to enable Subscriber Overcharging Protection.

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax Description**

**s4-overcharge-protection ranap-cause-code-group** *group_name*
**no s4-overcharge-protection**

**no**

Disables Subscriber Overcharging Protection functionality for 3G. Disabled is the default.

**ranap-cause-code-group *group_name***

Associates a RANAP cause code group with the SGSN Service configuration. You can enter a group's name before the cause code group is actually created but the names must match.

*group_name*Enter an alphanumeric string up to 16 characters long to identify the cause code group.

**Usage Guidelines**

The cause code group is created with the **cause-code-group** command in the LTE Policy configuration mode.

To see the name of the defined cause code group(s) or the configuration of the RANAP cause code groups, use the **show lte-policy cause-code-group [ name | summary ]** command in Exec mode.

To see the status of the Subscriber Overcharging Functionality and the associated RANAP cause code group, use Exec command **show gprs-service name** *service_name*.



**Important** If Release Access Bearer is enabled and going out of the S4-SGSN, the ARRL bit will be included if this CLI is enabled and if LORC (loss of radio coverage) is detected.

**Example**

Enable Subscriber Overcharging Protection and associated cause code group *3Gccgp1* with a command similar to the following:

```
s4-overcharge-protection bssgp-cause-code-group 3Gccgp1
```

Disable Subscriber Overcharging Protection and automatically disassociate the cause code group with the SGSN Service configuration by using a command similar to the following:

```
no s4-overcharge-protection
```

# sgsn-number

This command defines the E.164 number that identifies this particular SGSN service context.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax Description**

**sgsn-number** *E.164_number*
**no sgsn-number**

**no**

Removes the SGSN number configuration from the SGSN service configuration.

***E.164_number***

Enter a maximum of 15 digits to define the 'phone' number associated with this SGSN service in the specified context.

**Usage Guidelines**

The SGSN supports multiple SGSN numbers – different numbers in the 2G GPRS service configuration and the the 3G SGSN service configuration. If an HLR-initiated dialog is received, the SGSN will perform a lookup based on the IMSI and find the correct SGSN number with which the MS is associated. Subsequent messaging will use this address.

**Example**

To delete the sgsn-number associated with this SGSN service context, enter:

**no sgsn-number**

# sgtp-service

This command creates an instance of an SGTP service and associates the SGTP service instance with this SGSN service.

**Important** This command is used in Releases 12.0 and 12.2. For Release 14.0 refer to the **associate** command.

**Product**

SGSN

PDG/TTG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure > context** *context_name* **> sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax Description**

```
sgtp-service sgtp_srvc_name
no sgtp-service
```

***sgtp_srvc_name***

Enter the name of an SGTP service that will be used by this SGSN service

*sgtp_srvc_name* : Enter a string of 1 to 63 alphanumeric characters.

**Usage Guidelines**

Use this command to access the SGTP Service configuration mode to configure SGTP parameters.

**Example**

```
sgtp-service sgtp1
```

# sm

This command configures session management parameters for this SGSN service. This command can be repeated multiple times to configure each parameter individually.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

**configure** > **context** *context_name* > **sgsn-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax Description**

```
sm { T3385-timeout time | T3386-timeout time | T3395-timeouttime |
guard-timer guard_seconds | ignore-asi | max-actv-retransmission number |
max-deactv-retransmission number | max-modf-retransmission number |
radio-priority from-arp arp-rp_prof_name | t3396 min minimum max maximum cause
 cause_code | ue-3gpp-compliance-unknown restrict-16mbps }
default sm { T3385-timeout | T3386-timeout | T3395-timeout | guard-timer
 | max-actv-retransmission | max-deactv-retransmission |
max-modf-retransmission }
no sm { ignore-asi | radio-priority from-arp | t3396  |
ue-3gpp-compliance-unknown [restrict-16mbps] }
```

**default**

Resets the selected timer to the system default value.

**no**

Removes the specified parameter configuration from this SGSN service configuration.

**T3385-timeout**

Retransmission timer for network-initiated Activate Request.

Default is 8 sec

**T3386-timeout**

Retransmission timer for network-initiated Modify Request.

Default is 8 sec

**T3395-timeout**

Retransmission timer for network-initiated Deactivate Request.

Default is 8 sec

**guard-timer *guard_seconds***

Sets the number of seconds before the session manager resources are cleared.

*guard_seconds* is an integer from 30 to 150.

Default: 80 seconds

**ignore-asi**

Enables the operator to modify the SGSN service default configuration and instructs the SGSN to ignore the ASI bit in the SGSN Context Response during RAU-based handovers over Gn interfaces and to ignore establishing a RAB for any PDPs.

**radio-priority from-arp**

This keyword associates an ARP-RP Mapping Profile with the SGSN service. The profile is created and configured via the ARP-RP Mapping Profile configuration mode under the SGSN-Global configuration mode.

*arp-rp_prof_name* - Enter a string of 1 to 64 alphanumeric characters to identify the mapping profile and moves into the ARP-RP mapping profile configuration mode.

Use the **show configuration** command to display the association.

**max-actv-retransmission**

Configures maximum retries for activate PDP ctxt request.

Default is 4

**max-deactv-retransmission**

Configures maximum retries for deactivate PDP ctxt request.

Default is 4

**max-modf-retransmission**

Configures maximum retries for modify PDP ctxt request.

Default is 4

#### t3396

This keyword enables the session management (SM) T3396 back-off timer for the 3G service. When the SGSN is confronted by a situation involving congestion, the SGSN can assign the back-off timer value to the UEs and reques the UEs not to access the network for a given period of time.

**min** *minimum*: Enter an integer from 1 to 15 to identify the minimum number of minutes that the timer will run; default is 15 minutes.

**max** *maximum*: Enter an integer from 1 to 30 to identify the maximum number of minutes the timer can run; default is 30 minutes.

**cause** *cause_code*: Enter an integer from 1 to 255 to identify the appropriate rejection cause code. The default is 26. During congestion, the configured value is ignored and 26 is sent.

- During congestion, the SGSN randomly chooses a T3396 value from the configured range and sends that timer value to the UE in the Reject message with the cause code #26.
- The command can be repeated to define a maximum of 16 cause codes.

#### ue-3gpp-compliance-unknown restrict-16mbps

If this keyword is configured, the SGSN caps the APN-AMBR for non-GBR bearers to "16" Mbps and rejects the activation of GBR bearers with GBR higher than "16" Mbps.

If the **no** form of this keyword is configured, the APN-AMBR and GBR higher than "16" Mbps are allowed.

By default, the SGSN does not cap APN-AMBR or reject GBR bearer activation with bitrates higher than "16" Mbps.

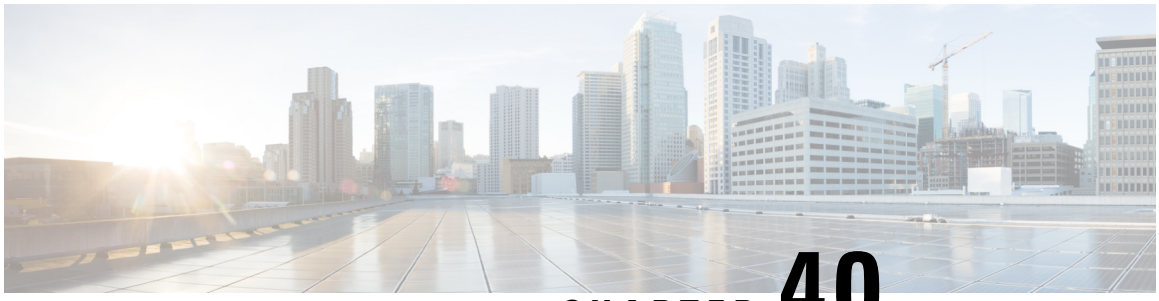
### Usage Guidelines

Repeat the command to configure multiple session management parameters for the SGSN service.

#### Example

Use a command similar to the following to set the expiry for 5 seconds for the session manager's T3385-timeout:

```
sm T3385-timeout 5
```



CHAPTER 40

# SGTP Service Configuration Mode Commands

**Command Modes**

The SGSN GPRS Tunneling Protocol (SGTP) Service configuration mode provides the configuration of GTP-C and GTP-U related parameters.

Exec > Global Configuration > Context Configuration > SGTP Service Configuration

**configure > context** *context_name* **> sgtp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgtp-service)#
```

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


- direct-tunnel-disabled-ggsn, on page 425
- disable-remote-restart-counter-verification, on page 427
- do show, on page 428
- end, on page 428
- exit, on page 429
- ggsn-fail-retry-timer, on page 429
- gn-delay-monitoring , on page 430
- gtpc, on page 431
- gtpu, on page 436
- ignore-remote-restart-counter-change, on page 438
- max-remote-restart-counter-change, on page 438
- mbms, on page 439
- path-failure, on page 440
- pool, on page 440


# direct-tunnel-disabled-ggsn

This command makes it possible for the operator to disable direct tunneling on the basis of a GGSN.

**Product**

SGSN

## Privilege

Security Administrator, Administrator

## Command Modes

Exec > Global Configuration > Context Configuration > SGTP Service Configuration

**configure > context** *context_name* **> sgtp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgtp-service)#
```

## Syntax Description

**direct-tunnel-disabled-ggsn** *ipv4/ipv6_address*
**no direct-tunnel-disabled-ggsn [** *ipv4/ipv6_address* **]**

### no

Deletes the direct-tunnel-disabled-ggsn configuration which results in re-enabling direct tunneling to the GGSN.

- Including an IPv4 or IPv6 address for a specific GGSN, re-enables direct tunneling for that specific GGSN.
- Excluding any IPv4 or IPv6 address from this command removes all direct-tunnel-disabled-ggsn definitions from the SGTP service configuration.

## Usage Guidelines

By default, GGSNs and RNCs are assumed to be capable of direct tunneling.

This command disables direct tunneling for a specified GGSN. The command can be repeated to disable direct tunneling for multiple GGSNs, thereby creating a 'disabled GGSN' list. Checking for a direct-tunnel-disabled GGSN is actually the last step in the PDP Activation procedure.

Restricting direct tunneling by a GGSN for an entire APN would be configured with the appropriate command in the APN profile configuration mode.

Restricting direct tunneling at the RNC level would be configured with the appropriate command in the IuPS service configuration mode.

This command can only be used if:

- The Direct Tunnel license has been purchased and applied.
- The Direct Tunnel feature is appropriately enabled via configurations of the IMEI profile and/or the Call-Control and APN profiles.
- The RNC does not restrict direct tunnel.
- The subscriber is not requesting CAMEL services.

### Example

Use the following command to disable direct tunnel for the GGSN with the IP address of *141.21.4.20*:

**direct-tunnel-disabled-ggsn 141.21.4.20**

# disable-remote-restart-counter-verification

This command disables the SGSN's default behavior for verification of the remote peer's (GGSN) restart counter change values.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGTP Service Configuration

**configure > context** *context_name* **> sgtp-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-sgtp-service)#`

**Syntax Description**

**`[ default | no ] disable-remote-restart-counter-verification`**

**default**

Enables the default behavior for verification of the GGSN's restart counter change values.

**no**

Disables the command configuration and enables the default behavior of verification.

**Usage Guidelines**

This command disables the default behavior used to minimize PDP deactivations resulting from path failure detection due to erroneous restart counter change messages.

With the execution of this command, the SGSN stops verifying restart counters received in Create PDP Context Response or Update PDP Context Response or Update PDP Context Request (CPCR, CPCR, and UPCQ) messages. When the SGSN detects GTP-C path failure between the SGSN and the GGSN, the SGSN assumes PDP sessions at the GGSN are lost and the SGSN deactivates those PDP sessions towards the UE with an indication that the UE should activate the PDP session again. Potentially, this scenario could cause unnecessary traffic increases within the operator's network.

The SGSN default behavior provides the ability to manage GTP-C path failures detected as a result of spurious restart counter change value messages received from the GGSN. With the default behavior, path failure detection is based on receipt of restart counter change values in CPCR, CPCR, and UPCQ messages. The session manager informs the SGTPC manager about a changed restart counter value. The SGTPC manager verifies the PDP context status by performing an echo request and echo response with the GGSN. Only then is the path failure confirmed if the echo response contains a new restart counter value. Then the SGTPC manager informs all session managers about the path failure and the session managers begin deactivation of the PDP contexts.

**Related commands**:

- **max-remote-restart-counter-change**, also part of the SGTP service configuration mode, allows the operator to set a maximum variance between stored and received values for restart counter changes coming from the GGSN.
- **pdp-deactivation-rate**, in the SGSN Global configuration mode, allows the operator to modify the rate the SGSN deactivates PDP connections when GPT-C path failure is detected.

- **ignore-remote-restart-counter**, also part of the SGTP service configuration mode.

### Example

Disable the default behavior and stop verification with echo request/response process:

```
disable-remote-restart-counter-verification
```

Use either of the following commands to enable the default verification behavior:

```
no disable-remote-restart-counter-verification
default disable-remote-restart-counter-verification
```

# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

Exits the configuration mode and returns to the Exec mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
end
```

**Usage Guidelines** Changes the mode to the Exec mode.

# exit

Exits the SGTP Service configuration mode and returns to the Context configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**exit**

**Usage Guidelines**

Return to the previous mode.

# ggsn-fail-retry-timer

This command sets the amount of time that a GGSN will be unavailable.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGTP Service Configuration

**configure > context** *context_name* **> sgtp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgtp-service)#
```

**Syntax Description**

**ggsn-fail-retry-timer** *value*
**no ggsn-fail-retry-timer**

**no**

Removes the timer setting and disables the Local DNS feature.

***value***

Defines the amount of time, in seconds, that the GGSN is to be considered unavailable.

Enter an integer from 60 to 600. Default is 300.

**Usage Guidelines**

Setting this timer to a valid value enables the Local DNS feature - described in the ***SGSN Administration Guide***. Setting this timer marks a GGSN in the primary GGSN pool as unavailable for PDP context creation and causes the SGSN to forward a PDP Context Activation Request to a remote pool GGSN, identified via a local (on the SGSN) DNS check. Marking a GGSN unavailable can be done if there is a reason to believe the GGSN is unavailable; for example, lack of response to GTP messages. Marking a GGSN as unavailable is usually done for a limited period to allow the GGSN time to recover.

### Example

Enable the Local DNS feature and mark the GGSNs in the primary pool as unavailable for 4 minutes (*240 seconds*):

```
ggsn-fail-retry-timer 240
```

# gn-delay-monitoring

This command configures monitoring of Gn/Gp interface to check for the delay of packets between the SGSN and the GGSN.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGTP Service Configuration

**configure > context** *context_name* **> sgtp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgtp-service)#
```

**Syntax Description**

```
gn-delay-monitoring [ num-delay number_delayed | num-no-delay-for-clear
number_normal | tolerance-seconds number_seconds ]
default gn-delay-monitoring [ num-delay | num-no-delay-for-clear |
tolerance-seconds ]
no gn-delay-monitoring
```

#### default

Resets the specified parameter to the default value.

#### no

Disables Gn/Gp monitoring for delayed GTP-C packets.

#### num-delay *number_delayed*

Defines the number of response messages, coming from the GGSN, that can be delayed (delay time defined by tolerance-seconds parameter) before the delay is flagged to generate an SNMP trap.

*number_delayed*: Enter an integer from 1 to 500, default is 30.

#### num-no-delay-for-clear *number_normal*

Defines the number of consecutive response messages, coming from the GGSN, that must be received without delay (in normal response time) to clear the flag towards the GGSN.

*number_normal*: Enter an integer from 1 to 500, default is 15.

**tolerance-seconds *number_seconds***

Defines the 'normal' number of seconds the SGSN should wait for a response from the GGSN. After this time, the response would be considered 'delayed'.

*number_seconds*: Enter an integer from 1 to 20, default is 4 seconds.



**Important** The value for this parameter should be less than the value set for the **retransmission-timeout** parameter of the **gtpc** command, also in this configuration mode.

**Usage Guidelines**

With this command, the SGSN can monitor the control plane packet delay for GTP-C signaling messages on the SGSN's Gn/Gp interface towards the GGSN. If the delay crosses this configurable threshold, an alarm will be generated to prompt the operator.

A delay trap is generated when the GGSN response to an ECHO message request is delayed more than a configured amount of time and for a configured number of consecutive responses. When this occurs, the GGSN will be flagged as experiencing delay.

A clear delay trap is generated when successive ECHO Response (number of successive responses to detect a delay clearance is configurable), are received from a GGSN previously flagged as experiencing delay.

This functionality can assist with network maintenance, troubleshooting, and early fault discovery.

**Example**

Enable Gn/Gp monitoring for GTP-C packets that arrive from the GGSN with a delay greater than *5* seconds:

```
gn-delay-monitoring tolerance-seconds 5
```

# gtpc

Configure the GPRS Tunneling Protocol Control (GTP-C) settings for the SGTP service.

**Product**

eWAG

MME

PDG/TTG

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGTP Service Configuration

**configure > context** *context_name* **> sgtp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgtp-service)#
```

## Syntax Description

**gtpc { bind address** *ipv4_address* **| dns-sgsn context** *context_name* **| echo-interval** *interval_seconds* **| echo-retransmission { exponential-backoff [ [ min-timeout** *timeout_seconds* **] [ smooth-factor** *smooth_factor* **] + ] | timeout** *timeout_seconds* **} | guard-interval** *interval_seconds* **| ignore response-port-validation | ip qos-dscp** *dscp_marking* **| max-retransmissions** *max_retransmissions* **| retransmission-timeout** *timeout_seconds* **| send { common flags | rab-context | target-identification-preamble } | sync-echo-with-peer }**
**no gtpc { bind address | dns-sgsn context | echo-interval | send { common-flags | rab-context | target-identification-preamble } | sync-echo-with-peer }**
**default gtpc { echo-interval | echo-retransmission | guard-interval | ignore response-port-validation | ip qos-dscp | max-retransmissions | retransmission-timeout | send { common-flags | rab-context | target-identification-preamble } | sync-echo-with-peer }**

**no**

Disables the configured GTP-C setting.

**default**

Resets the specified parameter to its default value.

**bind address *ipv4_address***

Binds SGTP service to the IP address of the interface.

The bind address for the **gtpc** and **gtpu** commands should be the same.

*ipv4_address* must be a standard IPv4 address.

**dns-sgsn context *context_name***

Identify the context where the DNS client is configured to send the DNS query to get the peer SGSN address. If nothing is configured, the system assumes the DNS client is configured in the same context where the SGTP service is configured.

*context_name*: Enter a string of 1 to 79 alphanumeric characters to identify the context.

There is a dns-sgsn command option in the call-control profile, which, if configured, would override the configuration in this SGTP service configuration.

**echo-interval *interval_seconds***

Configures the duration between echoes.

*seconds* Enter an integer from 0 through 3600.

Default: 60

**echo-retransmission { exponential-backoff [ [ min-timeout *timeout_seconds* ] [ smooth-factor *smooth_factor* ] + ] | timeout *timeout_seconds* }**

Configures the retransmission parameters for GTP-C echo messages. The operator can choose to use either an "exponential-backoff" timers or a "fixed-retransmission" timer:

- The **exponential-backoff** timer uses an exponential backoff algorithm to better manage the GTP-C path during periods of network congestion and to perform exponential-backoff echo timing. The exponential-backoff timer uses a calculated round-trip time (RTT), as well as a configurable factor or a multiplier to be applied to the RTT statistic. Different paths can each have a different RTT, so the exponential-backoff timer can be configured for multiple paths. One or both of the following parameters can be configured to refine the exponential-backoff timer configuration:
  - **min-timeout** *timeout_seconds*: Specifies the minimum time period (in seconds) for the exponential-backoff echo timer. If the RTT multiplied by the smooth factor is less than this minimum timeout value, then the node uses the value set with this keyword. Range is 1-20. Default is 5.
  - **smooth-factor** *smooth_factor*: Specifies the multiplier that the exponential-backoff echo timer uses when calculating the time to wait to send retries, when the gateway has not received a response from the peer within value defined for the path echo interval. Range is 1-5. Default is 2.
- **timeout** *timeout_seconds*: Configures the number of seconds for the fixed retransmission timeout value for GTP-C echo messages. Range from 1 to 20. Default is 5.

### guard-interval *interval_seconds*

Configures the interval (in seconds) for which the SGTP maintains responses sent to gateway. This optimizes the handling of retransmitted messages. This value should be configured to be greater than the gateway's configuration for max-retries multiple by retry-interval.

*interval_seconds*: Enter an integer from 10 to 3600.

Default: 100

### ignore response-port-validation

This keyword is available in releases 8.1 and higher.

This keyword instructs the gateway to ignore the response port validation.

For the gateway to process incoming GTP responses to an *incorrect* port, this keyword must be entered, and the same **bind address** must be configured for GTPC and GTPU in the SGTP service.

Default: Disabled. To reset the default for this parameter, you must enter the following command: **no gtpc ignore response-port-validation**.

### ip qos-dscp *dscp_marking*

Configures the diffserv code point marking to be used per hop behavior (PHB) when sending GTP-C messages originating from the session manager and SGTPC manager.

Note that CS (class selector) mode options below are provided to support backward compatibility with the IP precedence field used by some network devides. CS maps one-to-one to IP precedence, i.e., CS1 is IP precedence value 1. If a packet is received from a non-DSCP aware router, that used IP precedence markings, then the DSCP router can still understand the encoding as a Class Selector code point.

*dscp_marking*: Enter one of the following values:

- **af11**: Marks traffic as Assured Forwarding 11 PHB (high throughput data)
- **af12**: Marks traffic as Assured Forwarding 12 PHB (high throughput data)
- **af13**: Marks traffic as Assured Forwarding 13 PHB (high throughput data)

- **af21**: Marks traffic as Assured Forwarding 21 PHB (low latency data)
- **af22**: Marks traffic as Assured Forwarding 22 PHB (low latency data)
- **af23**: Marks traffic as Assured Forwarding 23 PHB (low latency data)
- **af31**: Marks traffic as Assured Forwarding 31 PHB (multimedia streaming)
- **af32**: Marks traffic as Assured Forwarding 32 PHB (multimedia streaming)
- **af33**: Marks traffic as Assured Forwarding 33 PHB (multimedia streaming)
- **af41**: Marks traffic as Assured Forwarding 41 PHB (multimedia conferencing).
- **af42**: Marks traffic as Assured Forwarding 42 PHB (multimedia conferencing)
- **af43**: Marks traffic as Assured Forwarding 43 PHB (multimedia conferencing)
- **be** : Designates use of Best Effort forwarding PHB. This is the default value.
- **cs0** : Designates use of class selector mode 0 PHB.
- **cs1** : Designates use of class selector mode 1 PHB.
- **cs2** : Designates use of class selector mode 2 PHB.
- **cs3** : Designates use of class selector mode 3 PHB.
- **cs4** : Designates use of class selector mode 4 PHB.
- **cs5** : Designates use of class selector mode 5 PHB.
- **cs6** : Designates use of class selector mode 6 PHB.
- **cs7** : Designates use of class selector mode 7 PHB.
- **ef** : Designates use of Expedited Forwarding PHB

Default: **be** (best effort)

**max-retransmissions *max_retransmissions***

Configures the maximum number of retries for packets.

*max_retransmissions*: Enter an integer from 0 to 15.

Default: 4

**retransmission-timeout *timeout_seconds***

Configures the control packet retransmission timeout in GTP, in seconds.

*timeout_seconds*: Enter an integer value from 1 through 20.

Default: 5

**send { common-flags | rab-context | target-identification-preamble }**

- **common-flags** : This option configures the SGTP service to include or exclude the common flags IE during an Inter-SGSN RAU. When selected, the default is to send the common flags IE.



**Important** Sending of common flags must be enabled to configure dual PDP type (IPv4v6) addressing with the **dual-address-pdp** command in the SGSN global configuration mode.

- **rab-context** : This option configures the SGTP service to include/exclude the radio access bearer (RAB) context IE in SGSN 'context response' message during Inter-SGSN Routing Area Update procedure. Default is to send the RAB context IE.
- **target-identification-preamble** : This option configures the SGTP service to include the Target Identification IE preamble byte in the target-id of Relocation Requests that it sends. By default, the preamble is not included. In accordance with 3GPP TS 29.060, v9.2.0, if the preamble is included then multiple optional parameters, such as Extended RNC ID, are encoded. Extended RNC ID expands the ID range from 4095 to 65535.

  In situations of MME interaction with the SGSN during SRNS procedures via GTPv1, the SGSN can use this Extended RNC ID field to indicate the Target RNC ID associated with the MME and vice versa.

Default: sending RAB context IE.

#### sync-echo-with-peer

This keyword is applicable to the SGSN only.

This keyword enables the SGSN to synchronize path management procedures with the peer after a GTP service restart recovery.

After GTP service recovery, the SGSN restarts the timers for GTP echo transmission, hence a drift in echo request transmission time (from the pre-recovery time) can occur causing the SGSN to be out of sync with the peer. By using this keyword, when the SGSN receives the first Echo Request (GTPC or GTPU) from the peer after the GTP service restart, in addition to replying with an ECHO Response, the SGSN transmits an ECHO Request to the peer and the SGSN restarts the timers associated with the path management procedures. This causes the path management procedure at SGSN to synchronize with the peer node.

Default: Enabled

## Usage Guidelines

Use this command to configure GTP-C settings for the current SGTP service. Repeat the command as needed to configure all required GTP-C parameters.

### Example

Following command excludes the radio access bearer (RAB) context IE in the SGSN Context Response message during the inter-SGSN RAU procedure:

```
no gtpc send rab-context
```

Configure the SGSN to send *common flags* with all GTP-C messages:

```
gtpc send common-flags
```

Set the SGSN to use GTPC echo-retransmission with exponential-backoff and both filters set for default:

```
gtpc echo-retransmission exponential-backoff
```

# gtpu

This command configures the GPRS Tunneling Protocol user data plane parameters (GTP-U) for this SGTP service.

**Product**

eWAG

PDG/TTG

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGTP Service Configuration

**configure > context** *context_name* **> sgtp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgtp-service)#
```

**Syntax Description**

```
gtpu { bind address ipv4_address | echo-interval interval_seconds |
echo-retransmission { exponential-backoff [ [ min-timeout timeout_seconds ]
 [ smooth-factor smooth_factor ] + ] | timeout timeout_seconds } |
max-retransmissions max_retransmissions | retransmission-timeout timeout_seconds
 | sync-echo-with-peer
no gtpu { bind address ipv4_address | echo-interval | sync-echo-with-peer}
default gtpu { echo-interval | echo-retransmission | max-retransmissions
 | retransmission-timeout | sync-echo-with-peer }
```

**no**

Removes the configuration for the specified parameter from the current SGTP service configuration.

**default**

Resets the specified GTP-U parameter to its factory default.

**bind address *ipv4_address***

Defines the GTP-U Gn' interface IP address that binds to this SGTP service.

The **gtpu** and the **gtpc** commands should be configured with the same bind address.

*ipv4_address*: Enter a standard dotted-quad IPv4 address.

**echo-interval *interval_seconds***

Configures the echo interval.

*interval_seconds*: Enter an integer from 60 through 3600.

Default: 60

**echo-retransmission { exponential-backoff [ [ min-timeout *timeout_seconds* ] [ smooth-factor *smooth_factor* ] + ] | timeout *timeout_seconds***

Configures the retransmission parameters for GTP-U echo messages. The operator can choose to use either an "exponential-backoff" timers or a "fixed-retransmission" timer:

- The **exponential-backoff** timer uses an exponential backoff algorithm to better manage the GTP-U path during periods of network congestion and to perform exponential-backoff echo timing. The exponential-backoff timer uses a calculated round-trip time (RTT), as well as a configurable factor or a multiplier to be applied to the RTT statistic. Different paths can each have a different RTT, so the exponential-backoff timer can be configured for multiple paths. One or both of the following parameters can be configured to refine the exponential-backoff timer configuration:
  - **min-timeout** *timeout_seconds*: Specifies the minimum time period (in seconds) for the exponential-backoff echo timer. If the RTT multiplied by the smooth factor is less than this minimum timeout value, then the node uses the value set with this keyword. Range is 1-20. Default is 5.
  - **smooth-factor** *smooth_factor*: Specifies the multiplier that the exponential-backoff echo timer uses when calculating the time to wait to send retries, when the gateway has not received a response from the peer within value defined for the path echo interval. Range is 1-5. Default is 2.
- **timeout** *timeout_seconds*Configures the number of seconds for the fixed retransmission timeout value for GTP-U echo messages. Range from 1 to 20. Default is 5.

**max-retransmissions *max_retransmissions***

Configures the maximum number of retries for retransmitting packets.

*max_retransmissions*: Must be an integer from 0 through 15.

Default: 4

**retransmission-timeout *timeout_seconds***

Configures the retransmission timeout of packets, in seconds.

*timeout_seconds*: Must be an integer from 1 through 20.

Default: 5

**sync-echo-with-peer**

This keyword is applicable to the SGSN only.

This keyword enables the SGSN to synchronize path management procedures with the peer after a GTP service restart recovery.

After GTP service recovery, the SGSN restarts the timers for GTP echo transmission, hence a drift in echo request transmission time (from the pre-recovery time) can occur causing the SGSN to be out of sync with the peer. By using this keyword, when the SGSN receives the first Echo Request (GTPC or GTPU) from the peer after the GTP service restart, in addition to replying with an ECHO Response, the SGSN transmits an ECHO Request to the peer and the SGSN restarts the timers associated with the path management procedures. This causes the path management procedure at SGSN to synchronize with the peer node.

Default: Enabled

## Usage Guidelines

Use this command to configure the GTP-U settings for the SGTP service.

### Example

Set the GTPU echo-interval for 5 seconds:

```
gtpu echo-interval 5
```

Set the gateway to use GTP-U echo-retransmission with exponential-backoff and the smooth-factor set for *4*:

```
gtpc echo-retransmission exponential-backoff smooth-factor 4
```

# ignore-remote-restart-counter-change

With the inclusion of the **disable-remote-restart-counter-verification** command, this command has been deprecated.

# max-remote-restart-counter-change

Use this command to set a restart counter change window to avoid service deactivations and activations that could cause large bursts of network traffic if the restart counter change messages from the GGSN are erroneous.

**Product**

eWAG

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGTP Service Configuration

**configure > context** *context_name* **> sgtp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgtp-service)#
```

**Syntax Description**

**max-remote-restart-counter-change** *variance*
**default max-remote-restart-counter-change**

#### default

If this keyword is used or if a variance window is not configured, then the default value will be 255 and the default behavior will be to detect a restart on any change.

#### *variance*

Set a number (an 8-bit value) that will define the variance range for restart counter change values compared between the gateway's stored value and the value received in messages from the GGSN. Valid entry is an integer from 1 to 255; default is 255.

Value of 32 is recommended as it provides a sufficient window to allow the gateway to handle delayed messages with old restart counters.

### Usage Guidelines

When the gateway detects GTP-C path failure between the gateway and the GGSN, the gateway assumes PDP sessions at the GGSN are lost and the gateway deactivates corresponding PDP sessions towards the UE with an indication that the UE should activate the PDP session again. Detection is based on receipt of restart counter change values in Create PDP Context Response or Update PDP Context Response or Update PDP Context Request (CPCR/UPCR/UPCQ) messages. Potentially, this scenario can cause major traffic increases within the operator's network. It is possible that the messages received from the GGSN are spurious.

The gateway default behavior provides the ability to verify possible GTP-C path failures detected as a result of spurious restart counter change messages received from the GGSN. With the default behavior, the session manager informs the SGTPC manager about a changed restart counter value. The SGTPC manager responds by verifying the PDP context status by performing an Echo Request / Echo Response with the GGSN. If the Echo Response includes a new restart counter change value, then the session manager considers the path failure confirmed and begins the PDP context deactivation sequence.

Use this command to avoid unnecessary path failures and deactivations by setting a restart counter change value 'window' or range of values. With this window, the gateway only accepts linearly increasing values for restart counter change values that are within the specified range of accepted changes before the SGTPC manager verifies. For example, if the allowed window for restart counter change value is set to 32 and the last learnt restart counter change value from the GGSN is 15, then the gateway should detect a restart only if the new restart counter value is between 16 and 47 (range of 32) and then the gateway would verify with the Echo Request/Response. If the received restart counter change value was 200 and the current learnt value was 15 with a window of 32, then the 200 would be ignored as a spurious value.

Also, use this command to set a restart counter change values window to avoid possible 'race conditions' (as defined in 3GPP TS 23.007 v8.7.0) where a new message arrives prior to an older message. This 'race condition' occurs when the gateway's stored restart counter value for the GGSN is larger than the restart counter value received in the messages received from the GGSN.

**Related commands**:

- **disable-remote-restart-counter-verification** - also part of the SGTP service configuration mode, this command allows the operator to disable the default behavior.
- **pdp-deactivation-rate**, in the SGSN Global configuration mode, this allows the operator to modify the rate the gateway deactivates PDP connections when GPT-C path failure is detected.
- **ignore-remote-restart-counter**, also part of the SGTP service configuration mode.

#### Example

Use the following command to configure an allowed restart counter change value window of *32*:

```
max-remote-restart-counter-change 32
```

# mbms

Enables / disables the Multimedia Broadcast Multicast Service.



**Important** The **mbms** command and parameter-configuring keywords are under development for future release and should not be used or included in your configuration at this time.

# path-failure

This command specifies the method for determining if path failure has occurred.

**Product**

eWAG

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGTP Service Configuration

**configure > context** *context_name* **> sgtp-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-sgtp-service)#`

**Syntax Description**

**`path-failure detection-policy gtp { echo | non-echo } + { default | no } path-failure detection-policy`**

**default**

Resets the specified path failure parameter to default.

Default: echo (for both GTPC and GTPU)

**no**

Deletes the path-failure definition from the configuration.

**echo**

Path failure is detected when the retries of echo messages time out.

**non-echo**

Path failure is detected when the retries of non-echo messages time out.

**Usage Guidelines**

Use this command to define the policy to detect gtp path failure.

**Example**

Set *echo* as the polity detection type:

**`path-failure detection-policy gtp echo`**

# pool

This command enables the default SGSN functionality for (flex) pooling and enables inclusion of the configured pool hop-counter count in new SGSN context/identify request messages.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SGTP Service Configuration

**configure > context** *context_name* **> sgtp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgtp-service)#
```

**Syntax Description**

```
pool { default-sgsn | hop-counter count }
no pool { default-sgsn | hop-counter }
default pool hop-counter
```

**no**

Disables the default SGSN pooling functionality or removes the SGSN pool hop-counter IE from the GTP Identity/context requests.

**default**

Removes the SGSN pool hop-counter IE from the GTP Identity/context requests.

**default-sgsn**

Enables default SGSN pooling functionality.

**hop-counter *count***

Enables and configures the SGSN pool hop-counter to set the number of hops and to include the configured count in the **new** SGSN Context Requests or the **new** SGSN Identify Requests.

If **default-sgsn** is enabled, then any messages relayed will have the default value of 4 for the counter if the message does not include this hop-counter ID.

*count:* Enter an integer from 1 to 255.

Default: 4

**Usage Guidelines**

Use this command to enable the default flex functionality without exposing the pool (flex) structure. This functionality provides a means for SGSNs outside of the pool to reach a pooled SGSN on the basis of its NRI.

Once the pooling has been enabled. Repeat the command using the **hop-counter** keyword to enable inclusion of the hop-counter IE in SGSN context/identify request messages and to configure the count for the pooling hop-counter. If the SGSN is behaving as the 'default SGSN', this SGSN will forward (relay) requests with the hop-count included to the target SGSN.

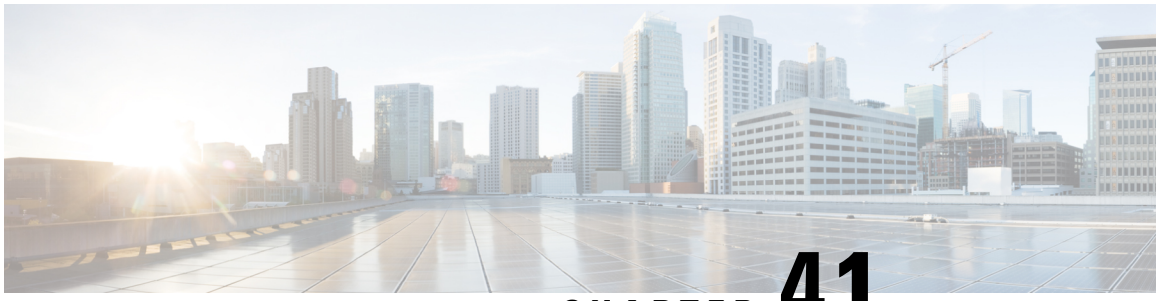
**Example**

Enable the default pooling functionality which allows an outside SGSN to reach a pooled SGSN:

```
pool default-sgsn
```

Set the hop-count to be included in messages to *25*:

```
pool hop-count
```



CHAPTER 41

# S-GW Access Peer Profile Configuration Mode Commands

MME restoration is a 3GPP specification-based feature designed to gracefully handle the sessions at S-GW once S-GW detects that the MME has failed or restarted. If the S-GW detects an MME failure based on a different restart counter in the Recovery IE in any GTP Signaling message or Echo Request / Response, it will terminate sessions and not maintain any PDN connections.

As a part of this feature, if a S-GW detects that a MME or S4-SGSN has restarted, instead of removing all the resources associated with the peer node, the S-GW shall maintain the PDN connection table data and MM bearer contexts for some specific S5/S8 bearer contexts eligible for network initiated service restoration, and initiate the deletion of the resources associated with all the other S5/S8 bearers.

**Command Modes**

This configuration mode enables operators to configure a peer profile for the Network Triggered Service Restoration feature.

Exec > Global Configuration > Peer Profile Configuration

**configure > peer-profile service-type sgw-access name** *profile_name*

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-peer-profile-sgw-access)#
```



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


- description, on page 443
- do show, on page 444
- end, on page 445
- exit, on page 445
- ntsr, on page 445


# description

Creates a textual description for this S-GW access peer profile.

**Product** S-GW

**Privilege** Administrator, Security Administrator

**Command Modes** Exec > Global Configuration > Peer Profile Configuration

**configure > peer-profile service-type sgw-access name** *profile_name*

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-peer-profile-sgw-access)#
```

**Syntax Description** **description** *string*

**description *string***

A text string that describes this S-GW access peer profile. The description can be from 1 to 64 alphanumeric characters in length.

**Usage Guidelines** Use this command to create a textual string that describes this S-GW access peer profile.

**Example**

To create a description titled SGWACCESS:

**description** *SGWACCESS*

# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **do show**

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`end`**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`exit`**

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

# ntsr

Enables network triggered service restoration (NTSR) and identifies the Pool ID to use for the feature.

**Product** S-GW

**Privilege** Administrator, Security Administrator

**Command Modes** Exec > Global Configuration > Peer Profile Configuration

**configure > peer-profile service-type sgw-access name** *profile_name*

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-peer-profile-sgw-access)#
```

**Syntax Description**

**`ntsr pool-id`** *number*
**`no ntsr-pool-id`** *number*
**`default ntsr-pool-id`** *number*

**default**

The specified NTSR pool ID will be used as the default.

**no**

Disables the specified option.

**ntsr *pool-id***

Specifies the NTSR pool ID to use for the NTSR feature. NTSR pool IDs and pool types are configured in Global Configuration Mode using the **ntsr pool-id** command.

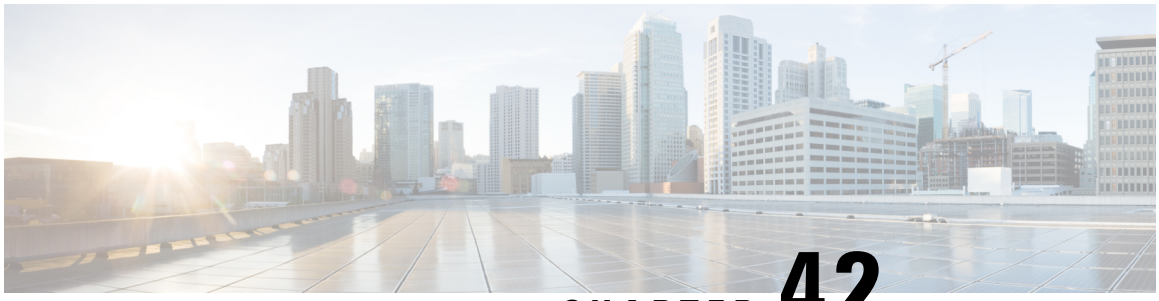
## Usage Guidelines

Use this command to configure an SGW Access Peer Profile for the NTSR feature.

### Example

To enable NTSR for NTSR pool ID 1

```
ntsr pool-id 1
```



CHAPTER 42

# S-GW Paging Profile Configuration Mode Commands

When some operators add an additional IMS service besides VoLTE such as RCS, they can use the same IMS bearer between the two services. In this case, separate paging is supported at the MME using an ID which can be assigned from the S-GW according to the services, where the S-GW distinguishes IMS services using a small DPI function to inspect where the traffic comes from using an ID which is assigned from SGW according to the services. The S-GW distinguishes IMS services using a small DPI function to inspect where the traffic comes from (for example IP, Port and so on). After the MME receives this ID from the S-GW after IMS service inspection, the MME will do classified separate paging for each of the services as usual.

**Command Modes**

This chapter describes SGW paging profile configuration mode commands. These commands support Separate Paging for IMS Service Inspection.

Exec > Global Configuration > S-GW Paging Profile Configuration

**configure > sgw-paging-profile three tupple**

Entering the above command sequence results in the following prompt:

```
[local] host_name(sep-paging-default)#
```

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


- do show, on page 447
- end, on page 448
- exit, on page 448
- ipv4 | ipv6, on page 448


# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description** `do show`

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `end`

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `exit`

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

# ipv4 | ipv6

Enables operators to specify a 3-tuple lookup (source IP address, source port and protocol) on the inner IP packet of the GTPU data packet at the S-GW. This configuration is to support the Separate Paging for IMS Service Inspection feature on the S-GW.

**Product** S-GW

**Privilege**

Administrator, Security Administrator

**Command Modes**

Exec > Global Configuration > S-GW Paging Profile Configuration

**configure > sgw-paging-profile three tupple**

Entering the above command sequence results in the following prompt:

```
[local] host_name(sep-paging-default)#
```

**Syntax Description**

**[ no ] { [ ipv4** *ipv4_address* **| ipv6** *ipv6_address* **] port** *source_port_num* **protocol { [ tcp | udp ] } paging-identifier** *integer*

**no**

Removes the specified paging profile configuration.

**ipv4** ***ipv4_address***

Specifies the IPv4 address to use for Separate Paging for IMS. Must be in IPv4 address format.

**ipv6** ***ipv6_address***

Specifies the IPv6 address to use for Separate Paging for IMS. Must be in IPv6 address format.

**port** ***source_port_num***

Specifies the source port on the S-GW to use for Separate Paging for IMS. Must be an integer from 1 to 65535.

**protocol** ***tcp | udp***

Specifies the protocol type to which this SGW paging profile applies. Must be either **tcp** or **udp**.

**paging-identifier** ***integer***

Specifies a service identifier for this SGW paging profile (for example, Data 0, VoLTE 1, RCS 2, and so on). Must be an integer from 0 to 255.

**Usage Guidelines**

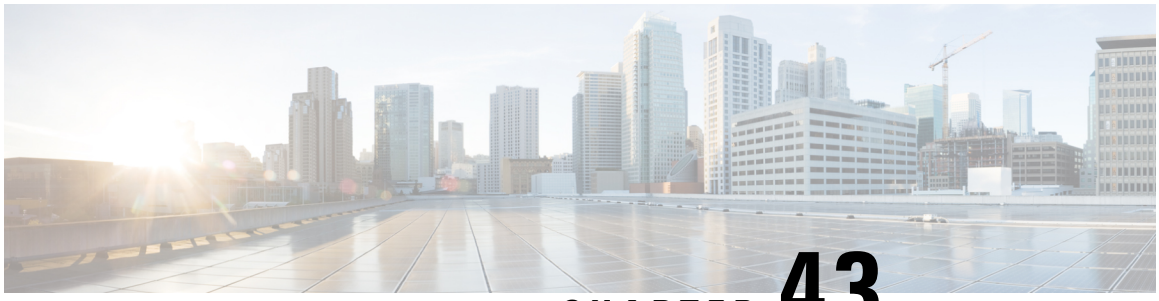
Use this command to identify an IMS specific paging procedure by performing a 3-tuple lookup (source IP address, Source Port and Protoco [TCP/UDP]) on the inner IP packet of the GTPU data packet at Serving Gateway. The Downlink Data Notification (DDN) message from the S-GW would carry a private extension IE with an identifier, which would denote if the paging procedure is for a data, Volte or RCS packet. This identifier helps the MME to apply different paging policies.

This configuration must be associated with an APN Profile by using the **associate** command in APN Profile Configuration Mode.

**Example**

The following example configures a paging procedure consisting of an IPv4 address, source port, protocol, and paging identifier.

```
ipv4  209.165.200.225 port  10 protocol tcp paging-identifier 0
```



CHAPTER 43

# S-GW Service Configuration Mode Commands

The S-GW (Serving Gateway) Service Configuration Mode is used to create and manage the relationship between an eGTP service used for either ingress or egress control plane and user data plane network traffic.

**Command Modes**

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

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


- accounting context, on page 452
- accounting mode, on page 453
- accounting stop-trigger, on page 454
- associate, on page 454
- cc, on page 457
- cc profile, on page 458
- ddn failure-action, on page 459
- ddn isr-sequential-paging, on page 460
- ddn success-action no-user-connect ddn-retry-timer, on page 461
- ddn temp-ho-rejection mbr-guard-timer, on page 462
- ddn throttle, on page 463
- do show, on page 466
- egtp idft-support, on page 466
- egtp, on page 467
- egtp-service, on page 468
- end, on page 469
- exit, on page 469
- gtpc handle-collision upc nrupc, on page 469
- gtpu-error-ind, on page 470
- mag-service, on page 471
- ntsr session-hold timeout, on page 472

- page-ue, on page 473
- paging-policy-differentiation, on page 474
- path-failure, on page 475
- pgw-fteid-in-relocation-cs-rsp, on page 477
- plmn, on page 477
- reporting-action, on page 478
- timeout idle, on page 479


# accounting context

Configures the GTPP accounting context and group selection for S-GW service.

**Product**

S-GW

SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax Description**

```
accounting context name [ gtpp group name ]
no accounting context
```

**no**

Removes the configured accounting context from this service.

**context *name***

Specifies the context where GTPP accounting is performed.

*name* must be an existing context configured on the system expressed as an alphanumeric string of 1 through 79 characters.

If an accounting context name is not configured in the S-GW service, the context where the S-GW service resides is considered the accounting context and the default GTPP group is used.

**gtpp group *name***

Specifies a GTPP group used to perform GTPP accounting.

*name* must be an existing GTPP group configured on the system expressed as an alphanumeric string of 1 through 79 characters.

If a GTPP group is not configured, the system will use the default GTPP group in the specified accounting context. If the accounting context is not specified, the system will use default GTPP group in the context where the S-GW service resides.

**Usage Guidelines** Use this command to specify the accounting context and/or GTPP accounting group the S-GW service will use to perform GTPP accounting.

### Example

The following command specifies a GTPP accounting context named *acct-2* and a GTPP accounting group named *gtpp-grp-3* as the context and group the S-GW service will use:

```
accounting context acct-2 gtpp group gtpp-grp-3
```

# accounting mode

Configures the mode to be used for accounting – GTPP (default), RADIUS/Diameter or None for S-GW service.

**Product** S-GW

SAEGW

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax Description**

```
[ default ] accounting mode { gtpp | none | radius-diameter }
```

### default

Sets the accounting mode to GTPP.

### gtpp

Specifies that GTPP accounting is performed. This is the default mode.

### none

Specifies that no accounting will be performed for the S-GW service.

### radius-diameter

Specifies that RADIUS/Diameter will be performed for the S-GW service.

**Usage Guidelines** Use this command to specify the accounting mode for the S-GW service. However, an accounting mode configured for the call-control profile will override this setting. For additional information on accounting mode and its relationship to operator policy, refer to the *Serving Gateway Administration Guide*.

### Example

The following command specifies that RADIUS/Diameter accounting will be used for the S-GW service:

```
accounting mode radius-diameter
```

# accounting stop-trigger

Configures the trigger point for accounting stop CDR. Default is on session deletion request.

**Product**

S-GW

SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax Description**

```
accounting stop-trigger custom
default accounting stop-trigger
```

#### default

Accounting stop CDR triggered once Delete Session/Delete Bearer Request is received at S-GW.

#### custom

Synchronizes the timestamp in the SGWRECORD CDR and PGWRECORD CDR if the MME cannot reach the UE. When configured, the SGW will also trigger the Accounting stop CDR after receiving the answer (accept for Delete session request) from the MME.

**Usage Guidelines**

Use this command to specify the trigger point for accounting stop CDR for this S-GW service.

### Example

The following command specifies that accounting stop trigger would be at response of session deletion:

```
accounting stop-trigger custom
```

# associate

Associates the S-GW service with QoS and policy control and charging configurations.

**Product**

S-GW

SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax Description**

**associate { access-peer-map | accounting-policy** *name* **| egress-proto { gtp | gtp-pmip | pmip } [ egress-context** *name* **| emps-profile** *emps_profile_name* **| gtpc-load-control-profile** *name* **| gtpc-overload-control-profile** *name* **[ egtp-service** *name* **] [ mag-service** *name* **] ] | ims-auth-service** *name* **| ingress egtp-service** *name***| peer-map** *name* **| qci-qos-mapping** *name* **| subscriber-map** *name*

**no associate { access-peer-map | accounting-policy | egress-proto [ egress-context [ egtp-service ] [ mag-service ] ] | emps-profile | ims-auth-service | ingress egtp-service | peer-map | qci-qos-mapping | subscriber-map }**

**no**

Removes the specified association form the S-GW service.

**access-peer-map*name***

Associates the access/ingress side of the peer-map to the configured S-GW service.

*name* must be an existing peer-map expressed as an alphanumeric string of 1 through 63 characters.

**accounting-policy *name***

Associates the S-GW service with an accounting policy configured in the same context.

*name* must be an existing accounting policy expressed as an alphanumeric string of 1 through 63 characters.

Accounting policies are configured through the **policy accounting** command in the Context Configuration Mode.

**egress-proto { gtp | gtp-pmip | pmip } [ egress-context *name* [ egtp-service *name* ] [ mag-service *name* ] ]**

Associates and configures the egress protocol for this S-GW service.

**gtp**: Specifies that GTP is to be used for the S-GW service egress.

**gtp-pmip**: Specifies that either GTP or PMIP is to be used for the S-GW service egress.

**pmip**: Specifies that PMIP is to be used for the S-GW service egress.

**egress-context** *name*: Specifies that the context in this keyword is to be used for the S-GW service egress.

*name* must be an existing context on this system expressed as an alphanumeric string of 1 through 63 characters.

**egtp-service** *name*: Specifies that the service in this keyword is to be used for the S-GW service egress.

*name* must be an existing eGTP service on this system expressed as an alphanumeric string of 1 through 63 characters.

**mag-service** *name*: Specifies that the service in this keyword is to be used for the S-GW service egress.

*name* must be an existing MAG service on this system expressed as an alphanumeric string of 1 through 63 characters.

**emps-profile*emps_profile_name***

Specifies that an eMPS profile is to be associated with an existing S-GW service in this context.

*emps_profile_name* must be a string of size 1 to 63 and treated as case insensitive.

**gtpc-load-control-profile *name***

Associates a configured GTPC Load Control Profile with this S-GW service.

*name* must be an existing GTPC Load Control Profile on this system expressed as an alphanumeric string of 1 through 64 characters.

**gtpc-overload-control-profile *name***

*name* must be an existing GTPC Overload Control Profile on this system expressed as an alphanumeric string of 1 through 64 characters.

**ims-auth-service *name***

Associates the S-GW service with an IMS authorization service configured in the same context.

*name* must be an existing IMS auth service and be from 1 to 63 alphanumeric characters.

IMS authorization services are configured through the **ims-auth-service** command in the Context Configuration Mode.

**ingress egtp-service *name***

Associates and configures the eGTP service ingress for this S-GW service.

*name* must be an existing eGTP service on this system expressed as an alphanumeric string of 1 through 63 characters.

**peer-map *name***

Associates the access/ingress side of the peer-map to the configured S-GW service

*name* must be an existing peer-map configuration expressed as an alphanumeric string of 1 through 63 characters.

**qci-qos-mapping *name***

Associates the S-GW service with QCI to QoS mapping parameters.

*name* must be an existing QCI-QoS mapping configuration expressed as an alphanumeric string of 1 through 63 characters.

QCI-QoS mapping is configured through the **qci-qos-mapping** command in the Global Configuration Mode.

**subscriber-map *name***

Associates the S-GW service with subscriber map parameters.

*name* must be an existing subscriber map configuration expressed as an alphanumeric string of 1 through 63 characters.

Subscriber maps are configured through the **subscriber-map** command in the LTE Policy Configuration Mode.

## Usage Guidelines

Use this command to select a pre-configured QoS mapping and/or policy control and charging configuration to be used by the S-GW service.

### Example

The following command associates the S-GW service with an IMS authorization service named *ims-23*:

```
associate ims-auth-service ims-23
```

# cc

Configures the charging characteristics (CC) for all three types of potential subscribers using this S-GW service.

## Product

S-GW

SAEGW

## Privilege

Administrator

## Command Modes

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

## Syntax Description

```
cc { home | roaming | visiting } prefer { local-value profile index [
behavior bits ] | peer-supplied }
```

**{ home | roaming | visiting }**

Specifies the type of subscriber that charging characteristics configuration is to be applied.

**home**: Home subscriber.

**roaming**: Roaming subscriber.

**visiting**: Visiting subscriber.

**prefer { local-value profile *index* [ behavior *bits* ] | peer-supplied }**

Specifies whether local charging characteristics values are to be used for subscribers using this S-GW or if values from a peer SGSN/MME are to be used.

**local-value profile** *index* **[ behavior** *bits* **]**: Specifies that local values for charging characteristics are to be applied to the configures subscriber type.

**profile** *index*: Configures profile index for charging characteristics.

*index* must be an integer from 0 through 15. The following values are pre-determined:

- **1**: Hot Billing
- **2**: Flat Billing
- **4**: Prepaid Billing
- **8**: Normal Billing

**behavior** *bits*: Configures behavior bits for charging characteristics.

*bits* must be a hexadecimal value from 0x0 to 0xFFF.

**peer-supplied**: Specifies that the charging characteristics are to be received from the SGSN/MME.

**Usage Guidelines**

Use this command to apply charging characteristics to different subscriber types using the S-GW service.

**Example**

The following command applies a charging characteristic of flat billing to roaming subscribers who use this S-GW service:

```
cc roaming prefer local-value profile 2
```

# cc profile

???

**Product**

S-GW

SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure** > **context** *context_name* > **sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax Description**

```
cc profile type { buckets num | interval sec | tarrif time1 mins hrs [ time2
 mins hrs ] [ time3 mins hrs ]...[ timeX mins hrs ] | volume { downlink octets
 uplink octets | total octets | uplink octets downlink octets } }
```

***type***

Specifies the decimal value of the profile bits defining the charging characteristics.

- A value of 1 specifies that hot billing is to be used.
- A value of 2 specifies that flat billing is to be used.
- A value of 4 specifies that prepaid billing is to be used.
- A value of 8 specifies that normal billing is to be used.

*type* must be an integer value from 1 to 15.

**buckets *num***

integer from 1 to 4

**interval *sec***

integer from 60 to 40000000

**tarrif time1 *mins hrs* [ time2 *mins hrs* ] [ time3 *mins hrs* ]...[ timeX *mins hrs* ]**

*mins*:

*hrs*:

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

**downlink** *octets* **uplink** *octets*:

total *octets*:

uplink *octets* **downlink** *octets*:

**Example**

# ddn failure-action

Configures a timer value to delay paging for this UE when the S-GW has initiated a Downlink Data Notification (DDN) to the MME and has received back a DDN failure.

**Product**

S-GW

SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax Description**

**ddn failure-action pkt-drop-time** *seconds*
**default ddn failure-action pkt-drop-time**

**default**

Resets the command to its default setting of 300 seconds.

**failure-action pkt-drop-time *seconds***

Default: 300

Configures a timer that determines how long the S-GW will discard downlink data packets so the MME has enough time to receive the Modify Bearer Request and prevent further errors being sent to the S-GW in the DDN Ack message.

*seconds* must be an integer value from 1 to 300.

**Usage Guidelines**

Use this command to set a timer value to delay the sending of excessive Downlink Data Notification messages to the MME (and receiving excessive DDN Ack message with errors from the MME) in cases when downlink data is arriving before the Modify Bearer Request is received. During the delay, downlink data packets are discarded until the timer has expired. This timer is triggered upon receiving the first error in a DDN Ack message from the MME.

**Related Functionality**

DDN Delay: By default, the S-GW supports the delay value IE included in a DDN acknowledgement message. The S-GW automatically multiplies this value by 50 ms, then applies the calculated delay for DDN for the UE.

**Example**

The following command configures the S-GW to discard downlink data packets for *200* seconds after the S-GW receives an error in a DDN Ack message from the MME :

**ddn failure-action pkt-drop-time 200**

# ddn isr-sequential-paging

Configures the delay time in 100 millisecond increments between paging of different RAT types in support of the Intelligent Paging for ISR feature.

**Product**

S-GW

SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax Description**

**ddn isr-sequential-paging delay-time** *delay*
**default ddn isr-sequential-paging**

**default**

Returns the delay time to its default value of 10 ( 10 * 100 ms = 1 second).

**delay-time *delay***

Configures delay between paging of different RAT types.

*delay* must be an integer from 1 to 255, representing increments of 100 milliseconds (*delay* = 1-255 * 100 ms).

Default: 10 (10 * 100 ms = 1 second)

**Usage Guidelines**

Use this command to configure the delay time in (100 millisecond increments) between paging of different RAT types in support of the Intelligent Paging for ISR feature.

**Example**

The following command configures the delay timer to 5 seconds.

**ddn isr-sequential-paging delay-timer 50**

# ddn success-action no-user-connect ddn-retry-timer

Use this command to resend DDN if no MBR or DDN Failure is received within the specified timer value.

**Product**

S-GW

SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax Description**

**ddn success-action no-user-connect ddn-retry-timer** *value_sec*
**default ddn success-action no-user-connect ddn-retry-timer**

**default**

Resets the command to its default setting of 60 seconds.

**ddn success-action no-user-connect ddn-retry-timer *value_sec***

Resends DDN if no MBR or DDN Failure is received within the specified timer value.

*value_sec*: Valid entries are from 60 to 300 seconds.

**Usage Guidelines**

After receiving DDN Ack, this timer is started and when it expires, S-GW sends one DDN and restarts the timer for same value. If no MBR is received within this time, S-GW clears the data buffers and waits for new data to trigger a new DDN.

This configuration is applicable only for non-ISR calls. If ISR is active, this configuration will be ignored. This extra DDN is sent under extreme circumstances. So, neither DDN delay nor throttling will be applied on it.

**Example**

The following command configures the DDN retry timer to 180 seconds.

```
ddn success-action no-user-connect ddn-retry-timer 180
```

# ddn temp-ho-rejection mbr-guard-timer

Sets the guard timer to wait for a MBR when DDN Ack with Cause #110 temp-ho-rejection) is received.

If the guard timer expires and if no MBR of any type or DDN Failure Indication is received, all the buffered downlink data is flushed out and paging flags are reset. If the guard timer is running and any MBR is received, the timer is stopped and no further action is taken. If the guard timer is running and DDN Failure Indication is received, the timer is stopped and standard DDN failure action is taken. By default, this CLI command is always enabled.

**Product**

S-GW

SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax Description**

**ddn temp-ho-rejection mbr-guard-timer** *time_in_seconds*

**no**

Disables the guard timer.

**default**

Enables the guard timer and sets it to the default value, 60 seconds.

**temp-ho-rejection**

Action to be taken when peer node indicates temporary rejection of paging due to handover-in-progress.

**mbr-guard-timer**

Sets the guard timer for a MBR when DDN Ack with Cause #110 (temp-ho-rejection) is received. When the timer expires, S-GW flushes all the buffered downlink data packets. The range of this timer is from 60 seconds to 300 seconds. Default timer value is 60 seconds.

**Usage Guidelines**

Use this CLI command to enable guard timer to wait for MBR once the DDN Ack with cause#110 (Temporary Handover In Progress) is received. If the guard timer expires and if no MBR of any type or DDN Failure Indication is received, all the buffered downlink data is flushed out and paging flags are reset. If the guard timer is running and DDN Failure Indication is received, the timer is stopped and standard DDN failure action is taken.

By default, this CLI command is always enabled.

**Example**

The following CLI command sets the guard timer for 200 seconds to wait for a MBR when DDN Ack with Cause #110 temp-ho-rejection) is received.

```
ddn temp-ho-rejection mbr-guard-timer 200
```

# ddn throttle

Configures Downlink Data Notification throttle parameters.

**Product**

S-GW

SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax Description**

```
ddn throttle arp-watermark arp_value [ rate-limit limit time-factor seconds
throttle-factor percent increment-factor percent [ poll-interval seconds ]
throttle-time-sec seconds [ throttle-time-min minutes ] [ throttle-time-hour
 hour ] stab-time-sec seconds [ stab-time-min minutes ] [ stab-time-hour hour
 ]
no ddn-throttle
```

**no**

Disables the DDN throttling feature.

**throttle arp-watermark *arp_value***

If ARP watermark is configured and if an MME/SGSN sends the throttling factor and delay in a DDN ACK message, all the DDNs which have an ARP value greater than the configured value will be throttled by the throttle factor for the specified delay.

*arp_value* is an integer from 1 through 15.

**rate-limit *limit***

Configures the rate limit (Use this and subsequent tokens to rate-limit only if the MME is a Non-Release 10 MME).

*limit* is an integer from 1 through 999999999.

**time-factor *seconds***

Configures the time duration during which the S-GW makes throttling decisions.

*seconds* is an integer from 1 to 300.

**throttle-factor *percent***

Configures the DDN throttling factor. Enter the percentage of the DDN to be dropped upon detecting a DDN surge.

*percent* is an integer from 1 through 100.

**increment-factor *percent***

Configures the DDN throttling increment factor. Enter the percentage by which the DDN throttling should be increased.

*percent* is an integer from 1 through 100.

**poll-interval *seconds***

Configures the polling interval in DDN throttling.

*seconds* is an integer from 2 through 999999999.

**throttle-time-sec *seconds***

Configures the DDN throttling time in seconds. Enter time period in seconds over which DDN are throttled at the S-GW.

*seconds* is an integer from 0 through 59.

**throttle-time-min *minutes***

Configures the DDN throttling time in minutes. Enter time period in minutes over which DDN are throttled at the S-GW.

*minutes* is an integer from 0 through 59.

**throttle-time-hour *hour***

Configures the DDN throttling time in hours. Enter time period in hours over which DDN are throttled at the S-GW.

*hour* is an integer from 0 through 310.

**stab-time-sec *seconds***

Configures the DDN throttling stabilization time in seconds. Enter a time period in seconds over which if the system is stabilized, throttling will be disabled.

*seconds* is an integer from 0 through 59.

**stab-time-min *minutes***

Configures the DDN throttling stabilization time in minutes. Enter a time period in minutes over which if the system is stabilized, throttling will be disabled.

*minutes* is an integer from 0 through 59.

**stab-time-hour *hour***

Configures the DDN throttling stabilization time in hours. Enter a time period in hours over which if the system is stabilized, throttling will be disabled.

*hour* is an integer from 0 through 310.

## Usage Guidelines

Use this command to throttle DDNs to allow for the creation of the tunnel and avoid unnecessary DDNs.

For a UE in idle mode, S1U bearers are not established. In such a case, if a downlink packet arrives for the UE, the S-GW initiates a paging procedure towards the MME. The MME in turn pages the UE in its tracking area to search for the UE. Upon receiving the paging request, the UE establishes S1U bearers. Too many DDN requests towards the MME from the S-GW could overload the MME. To reduce this load, the MME can dynamically request S-GW to reduce a certain percentage of DDN messages sent towards it for a given period time.

The S-GW supports the following IEs for this feature:

- ARP IE in Downlink Data Notification
- DL Low Priority Traffic Throttling IE in DDN Acknowledge Message

More information is available in Release 10 of 3GPP 29.274, section 5.3.4.3.

The S-GW supports DDN throttling for up to 24 MMEs. DDNs for additional MMEs (25+) will be sent as normal and will not be throttled.

Throttling statistics can be viewed by issuing the Exec mode command:

**show sgw-service statistics all**

### Example

The following command sets the ARP watermark lowest priority to *10* seconds:

```
ddn throttle arp-watermark 10
```

If the ARP value provided is 10, all bearers with ARP value between 10-15 are treated as low priority bearers and are given throttling treatment. Throttling would not be enabled if the ARP value is not

provided through S-GW service configuration. Also, the ARP IE in DDN message towards MME would not be included unless DDN throttling is configured in S-GW service.

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution**

There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# egtp idft-support

Enables or disables the Indirect Forwarding Tunnel (IDFT) feature in CUPS.

**Product**

CUPS

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax Description**

```
[ default | no ] egtp idft-support
```

**default**

Resets the command to its default setting. By default, the CLI is disabled.

**no**

Removes the configured IDFT support.

**Usage Guidelines** By default, the IDFT feature is disabled and this CLI command is applicable on run-time change.

# egtp

Configures the temporary failure response for Delete Bearer or for Update Bearer Request - Modify Bearer Command (UBR-MBC) collision for S-GW.

**Product** S-GW

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-sgw-service)#`

**Syntax Description**

```
[ default | no ] egtp cause-code temp-failure { dbr-proc| ubr-mbc-collision
  | egtp change-notification-req rat-type eutran
ignore-uli-with-rai-sai-cgi  }
```

**no**

Disables the specified parameter.

**cause-code**

Configures the collision-handling failure response.

**temp-failure**

Configures the service to handle temporary failure from peer.

**dbr-proc**

Configures the service to send cause code 110 (temporary failure) for Delete Bearer failure response. The default behavior is disabled.

**ubr-mbc-collision**

Configures the service to send cause code 110 (temporary failure) for UBR-MBC collision. The default behavior is disabled.

Use this command to configure and to enable the temporary failure response for Delete Bearer or for UBR-MBC collision.

**egtp change-notification-req rat-type eutran ignore-uli-with-rai-sai-cgi**

Configure this parameter to ignore SAI/RAI/CGI in the Change Notification Request message under 4G CALL FLOW (EUTRAN RAT type) for S-GW services.

# egtp-service

Configures an eGTP service to use as either an ingress (S1-U) or egress (S5/S8) service for the S-GW.

**Product**

S-GW

SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax Description**

**egtp-service { egress { context** *name* **| service** *name* **} | ingress service** *name* **}**
**no egtp-service { egress { context | service } | ingress service }**

**no**

Removes the selected EGTP service from this service.

**egress { context *name* | service *name* }**

Specifies the egtp-service to be used as the egress eGTP service on a GTP-based S5/S8 interface.

**context** *name*: Specifies the name of the context where the eGTP service resides.

*name* must be an existing context name where an eGTP service resides expressed as an alphanumeric string of 1 through 63 characters.

**service** *name*: Specifies the name of the egress eGTP service.

*name* must be an existing eGTP service name expressed as an alphanumeric string of 1 through 63 characters.

**ingress service *name***

Specifies the egtp-service to be used as the ingress eGTP service on the S11 interface.

*name* must be an existing eGTP service name expressed as an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to configure the eGTP service to use with this S-GW service. The eGTP service must be existing and be configured with the appropriate parameters supporting the intended service type.

### Example

The following command configures the S-GW service to use an eGTP service named *s1u-egtp* as its ingress service:

**egtp-service ingress service slu-egtp**

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# gtpc handle-collision upc nrupc

This command helps in enabling or disabling collision handling between SGSN initiated UPC and NRUPC request.

**Product** S-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure** > **context** *context_name* > **sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-sgw-service)#`

**Syntax Description** `[ no | default ] gtpc handle-collision upc nrupc`

**no**

Disables collision handling between SGSN initiated UPC and NRUPC request.

**default**

Sets default collision handling behavior between SGSN initiated UPC and NRUPC request. By default, collision handling is enabled.

**handle-collision upc nrupc**

Enables/Disables collision handling between SGSN initiated UPC and network requested UPC. By default, collision handling is enabled.

**Usage Guidelines** This command is used to enable or disable collision handling between SGSN initiated UPC and NRUPC request.

**Example**

The following example disables collision handling between SGSN initiated UPC and NRUPC request.

```
no gtpc handle-collision upc nrupc
```

# gtpu-error-ind

Configures the actions to be taken upon receiving a GTP-U error indication from an RNC, eNodeB, SGSN, or P-GW.

**Product** S-GW

SAEGW

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure** > **context** *context_name* > **sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax Description**

```
gtpu-error-ind { { s12 | s1u | s11u } { local-purge | page-ue [
custom1-behavior ] } | { s4u | s5u } { local-purge | signal-peer } }
default gtpu-error-ind { s12 | s1u | s11u | s4u | s5u }
```

**default**

Resets the command to the default action for the specified interface. For S12 and S1-U, **page-ue** is the default action. For S4-U and S5-U, **local-purge** is the default action.

**{ s12 | s1u  | s11u }{ local-purge | page-ue [ custom1-behavior ] }**

Specifies the action to take when a GTP-U error indication is received from a Radio Network Controller (RNC) over an S12 interface or from an eNodeB over the S1-U interface.

**local-purge**: The S-GW clears the affected bearer (or PDN if error-indication is received on default bearer) locally without informing peer.

**page-ue [ custom1-behavior ]**: The S-GW moves the complete UE state to S1-Idle and starts paging for this UE. If the custom1-behavior option is specified, the S-GW will guard the paging attempt with a timer of 60 seconds. Within this time the bearer must have the eNodeB TEID refreshed by an MME. Otherwise, the S-GW will clear the affected bearer with signaling. This is the default action for GTP-U error indication messages received on the S12 and S1-U interfaces.

**{ s4u | s5u }{ local-purge | signal-peer }**

Specifies the action to take when a GTP-U error indication is received from an SGSN over an S4-U interface or from a P-GW over the S5-U interface.

**local-purge**: The S-GW clears the affected bearer (or PDN if error-indication is received on a default bearer) locally without informing the peer. This is the default action for GTP-U error indication messages received on the S4-U and S5-U interfaces.

**signal-peer**: The S-GW initiates control signalling towards the peer MME and P-GW. When signalling:

- For a bearer deletion, the S-GW sends a Delete-Bearer-Command message to the P-GW and a Delete-Bearer-Request (with EBI) message to the MME.
- For PDN deletion, the S-GW sends a Delete-Session-Request message to the P-GW and a Delete-Bearer-Request (with LBI) message to the MME.
- The S-GW will not wait for Delete replies from the peer. The request will be sent only once and local resources will be reset.

**Usage Guidelines**

Use this command to specify the action to taken upon receiving a GTP-U error indication from an RNC over an S12 interface, an eNodeB across an S1-U interface, an SGSN over an S4-U interface, or from a P-GW across an S5-U interface.

**Example**

The following command sets the action to take upon receipt of a GTP-U error indication from the eNodeB to clear affected bearer:

```
gtpu-error-ind s1u local-purge
```

# mag-service

Identifies the Mobile Access Gateway (MAG) egress service through which calls are to be routed for this S-GW service.

**Product**

S-GW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax Description**

**mag-service egress service** *name*
**no mag-service egress service**

**no**

Removes the configured MAG egress service from this service.

**egress service *name***

Specifies the MAG service name to be used as the egress MAG service on a Proxy Mobile IPv6 (PMIP) based S5/S8 interface.

*name* must be an existing MAG service expressed as an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to specify the name of the MAG service where calls are to be routed.

**Example**

The following command specifies that an existing MAG service named *mag3* is to be used to route call through for this S-GW service:

```
mag-service egress service mag3
```

# ntsr session-hold timeout

Configures a timer to hold the session after path failure is detected at the MME (for Network Triggered Service Restoration).

**Product**

S-GW

**Privilege**

Administrator, Security Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax Description**

**[ no ] ntsr session-hold timeout** *seconds*

**no**

Disables the NTSR session-hold timeout.

**ntsr session-hold timeout *seconds***

Configures the timer duration, in seconds, that determines how long the session will be held after path failure is detected during MME restoration. Valid entries are from 1 to 3600 seconds.

**Note** For VPC-DI platform, the maximum range can be set as 172800 seconds (2 days).

**Usage Guidelines** Use this command to configure the timer duration, in seconds, that determines how long the session will be held after path failure is detected during MME restoration.

**Example**

To configure the ntsr session-hold timeout for 10 seconds.

```
ntsr session-hold timeout 10
```

# page-ue

Allows the S-GW to page the UE for P-GW-initiated procedures (Create Bearer Request (CBR)/Modify Bearer Request (MBR)/Update Bearer Request (UBR)) when the UE is idle, and sends a failure response to the P-GW with the cause code 110 (Temporary Failure) when the UE is idle or a collision is detected at the S-GW.

**Product** S-GW

SAEGW

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax Description**

```
[ default | no ] page-ue pgw-initiated-proc
```

**default**

Returns the command to its default setting of disabled.

**no**

Disables the feature.

**pgw-initiated-proc**

Sets the command to page the UE for P-GW initiated MBR, UBR, and CBR procedures.

**Usage Guidelines** Use this command to allow the S-GW to page a UE for P-GW-initiated procedures (CBR/MBR/UBR) when the UE is idle, and sends a failure response to the P-GW with the cause code 110 (Temporary Failure) when the UE is idle or a collision is detected at the S-GW.

### Example

The following command enable the S-GW to page the UE

```
page-ue pgw-initiated-proc
```

# paging-policy-differentiation

Controls Paging Policy Differentiation (PPD) functionality on the S-GW.

**Product** S-GW

**Privilege** Administrator, Security Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax Description** **`[ default | no ] paging-policy-differentiation`**

### default

Restores the PPD functionality to its default setting of disabled.

### no

Disables this option. This is the default setting.

### paging-policy-differentiation

When S-GW supports the PPD feature, it shall include Paging and Service Information IE in the Downlink Data Notification message triggered by the arrival of downlink data packets at the S-GW. The Paging Policy Indication value within this IE will contain the value of the DSCP in TOS (IPv4) or TC (IPv6) information received in the IP payload of the GTP-U packet from the P-GW.

It is up to MME/S4-SGSN to use the Paging and Service Information IE of DDN message.

To support PPD feature in SAEGW, both S-GW and P-GW configuration is required.

**Usage Guidelines** Use this command to enable/disable PPD functionality on S-GW.

**Important** P-GW and S-GW should apply the PPD feature for both Default and Dedicated bearers. As per the specifications, P-GW transparently passes the user-datagram packet towards S-GW. This means, if PPD feature is enabled, operator can't apply different behavior for Default and Dedicated bearers.

Once the PPD feature is enabled, it is applicable for both existing and new calls.

If PPD feature is enabled at S-GW service, it is applicable for all calls irrespective of the APN profiles.

The PPD feature is license controlled under the license for S-GW Paging Profile. Once the license is enabled, both features co-exist together and work independently. That means, DDN message might carry both DSCP marking specified by PPD feature and Priority DDN value specified by S-GW Paging Profile feature.

At S-GW, the user-datagram packet DSCP value is used to send in DDN. S-GW can't change the DSCP, as per the local configuration (APN profile or service level). At eNodeB, the scheduling of the packet is based on the QCI instead of DSCP, however, any EPC node should not change/modify the inner DSCP value.

**Important** For the PPD feature to work, it must be enabled for P-GW and S-GW.

Both P-GW and S-GW services apply PPD configuration independently. Therefore, for any downlink data packet from an APN, there could be a case where P-GW does not have PPD configuration but S-GW has PPD configuration. To avoid such a conflict, you must configure the PPD functionality on both P-GW (APN level granularity) and S-GW (service level granularity).

See the *Paging Policy Differentiation* chapter in the *S-GW Administration Guide* for detailed information on PPD functionality.

### Example

To enable PPD functionality on S-GW, enter the following command:

```
paging-policy-differentiation
```

# path-failure

Configures the action to take upon the occurrence of a path failure between the S-GW and the MME, P-GW, RNC, SGSN, or eNodeB.

**Product**

S-GW

SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

## Syntax Description

```
path-failure { s11 | s11u | s12 | s1u | s4 | s4u | s5 | s5u } ( local-purge
 | signal-peer }
default path-failure { s11 | s11u | s12 | s1u | s4 | s4u | s5 | s5u } (
local-purge | signal-peer }
```

### default

Returns the command to the default setting of "local purge" for the selected interface.

### { s11 | s12 | s1u | s4 | s4u | s5 | s5u }

Specifies the interface to which the action will be applied.

**s11**: Applies the path failure action to the S11 interface between the S-GW and the MME.

**s11u**: Applies the path failure action to the S11-U interface between the S-GW and the MME.

**s12**: Applies the path failure action to the S12 interface between the S-GW and the RNC.

**s1u**: Applies the path failure action to the S1-U interface between the S-GW and the eNodeB.

**s4**: Applies the path failure action to the S4 control plane interface between the S-GW and the SGSN.

**s4u**: Applies the path failure action to the S4-U user plane interface between the S-GW and the SGSN.

**s5**: Applies the path failure action to the S5 interface between the S-GW and the P-GW.

**s5u**: Applies the path failure action to the S5-U user plane interface between the S-GW and the P-GW.

### { local-purge | signal-peer }

Specifies the action to apply to the selected interface.

**local-purge**: The S-GW clears the affected bearer (or PDN if path failure is received on a default bearer) locally without informing the peer. This is the default action for all interface.

**signal-peer**: The S-GW initiates control signalling towards the peer MME and P-GW. When signalling:

- For a bearer deletion, the S-GW sends a Delete-Bearer-Command message to the P-GW and a Delete-Bearer-Request (with EBI) message to the MME.
- For PDN deletion, the S-GW sends a Delete-Session-Request message to the P-GW and a Delete-Bearer-Request (with LBI) message to the MME.
- The S-GW will not wait for Delete replies from the peer. The request will be sent only once and local resources will be reset.

## Usage Guidelines

Use this command to specify the type of action to take when a path failure occurs on one of the supported interfaces.

### Example

The following command sets the path failure action for the S5 interface to "signal peer":

```
path-failure s5 signal-peer
```

# pgw-fteid-in-relocation-cs-rsp

Controls the sending of the PGW Fully Qualified Tunnel Endpoint Identifier (FTEID) for relocation Create Session Response procedures with an S-GW change.

**Product**

S-GW

**Privilege**

Administrator, Security Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-sgw-service)#`

**Syntax Description**

**`[ no ] pgw-fteid-in-relocation-cs-rsp`**

**no**

Disables the sending of the P-GW FTEID in Create Session Response procedures where there is an S-GW relocation change. This is the default setting.

**pgw-fteid-in-relocation-cs-rsp**

Enables the sending of the P-GW FTEID in Create Session Response procedures where there is an S-GW relocation change.

**Usage Guidelines**

Use this command to control the sending of the PGW Fully Qualified Tunnel Endpoint Identifier (FTEID) for relocation Create Session Response procedures with an S-GW change. For backward compatibility with earlier 3GPP release peer nodes requiring the P-GW FTEID in the Create Session Response procedures, this configurable can be enabled.

**Example**

To enable the sending of the FTEID for relocation Create Session REsponse procedures with an S-GW change:

**`pgw-fteid-in-relocation-cs-rsp`**

# plmn

Configures the public land mobile network (PLMN) identifiers for this S-GW. service

**Product**

S-GW

SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax Description**

**plmn id mcc** *number* **mnc** *number* **[ primary ]**
**no plmn id mcc** *number* **mnc** *number*

**no**

Removes the configured PLMN ID for this S-GW service.

**mcc *number***

Configures the Mobile Country Code for this PLMN ID.

*number* must be an integer from 100 through 999.

**mnc *number***

Configures the Mobile Network Code for this PLMN ID.

*number* must be a 2- or 3-digit integer from 00 through 999,

**primary**

Specifies that this is the primary PLMN ID for this S-GW service.

**Usage Guidelines**

The PLMN identifier is used by the S-GW service to determine whether or not a mobile station is visiting, roaming, or home. Multiple S-GW services can be configured with the same PLMN identifier. Up to five PLMN IDs can be configured for each S-GW Service. In Release 15.0 and later, up to 15 PLMN IDs can be configured.

**Example**

The following command configures a "primary" PLMN ID for this S-GW service with an MCC of *123* and an MNC of *12*:

```
plmn id mcc 123 mnc 12 primary
```

# reporting-action

Configures the system to start reporting session events.

**Product**

S-GW

SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-sgw-service)#`

**Syntax Description**

**`[ no ] reporting-action event-record [ trigger active-idle ]`**
**`default reporting-action event-record`**

**default**

Returns the command to its default setting of disabled.

**no**

Disables session event reporting.

**trigger active-idle**

Specifies that the event is only to be reported upon the going from active to idle.

**Usage Guidelines**

Use this command to enable the session event reporting feature on the S-GW.

**Example**

The following command enables event reporting but does not limit it to events triggered by going active to idle:

**`reporting-action event-record`**

# timeout idle

This command removes S-GW sessions that remain idle for longer than the configured time limit.

**Product**

S-GW

SAE-GW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

**configure > context** *context_name* **> sgw-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-sgw-service)#`

**Syntax Description**

**`timeout idle`** *`dur_seconds`* **`[ micro-checkpoint-periodicity`***`time_in_seconds`* **`| micro-checkpoint-deemed-idle`***`time_in_seconds`* **`]`**
**`{ default | no } timeout idle`**

**default**

Indicates the timeout specified is to be returned to its default behavior.

**no**

Disables the timeout idle functionality.

**timeout idle**

Enables the S-GW session idle timer.

***dur_seconds***

Specifies the time limit, in seconds, after which the S-GW session will be torn down. Valid entries are from 0 to 4294967295.

**micro-checkpoint-periodicity*time_in_seconds***

Specifies the micro-checkpoint periodicity for idlesecs, in seconds.

*time_in_seconds* must be an integer from 10 to 10000 seconds.

Default: 10



**Important** The **micro-checkpoint-periodicity** value should be less than **idle timeout** value.

**micro-checkpoint-deemed-idle*time_in_seconds***

Specifies the time duration, in seconds, after which a session state is deemed to have changed from active to idle or idle to active, and a micro-checkpoint is then sent from the active to the standby chassis.

*time_in_seconds* must be an integer from 10 to 1000.

Default: 180



**Important** The **micro-checkpoint-deemed-idle** value should be less than the **timeout idle** value.

## Usage Guidelines

The S-GW session idle timer removes stale sessions in those cases where the session is removed on the other nodes but due to some issue remains on the S-GW. Once configured, the session idle timer will tear down such sessions that remain idle for longer than the configured time limit. The implementation of the session idle timer allows the S-GW to more effectively utilize system capacity.

Optionally, ICSR micro-checkpoint periodicity for idlesecs is configurable instead of using the default periodicity of 10 seconds. Operators can configure this setting to a large value to suit their need to reduce the number of micro-checkpoints on the SRP link. When this CLI command is configured, idleseconds micro-checkpoints are sent at configured regular intervals to the standby chassis. If not configured, micro-checkpoints are sent at intervals of 10 seconds, which is the default.

Finally, the operator can choose to configure micro-checkpoint-deemed-idle. This process enables the active and standby chassis to be synchronized with respect to when a particular session became active or idle. Since this feature is event-based, it enables the chassis to send micro-checkpoints only when an event is deemed to

have occurred, as opposed to sending micro-checkpoints based on a configured time duration, which sends the micro-checkpoints regardless of whether a session state change occurred or not. Using **micro-checkpoint-deemed-idle** results in a more efficient event-based sending of micro-checkpoints to the standby chassis and also increases SRP bandwidth.

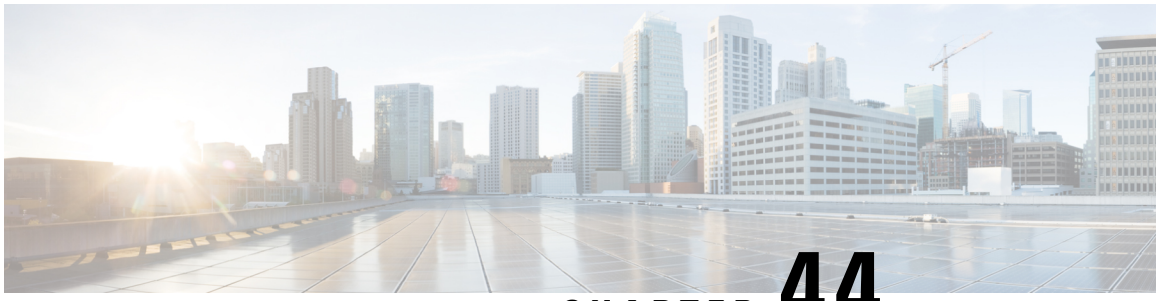


**Important** Either the **micro-checkpoint-deemed-idle** or **micro-checkpoint-periodicity** value can be configured for idle time duration. Any change from **micro-checkpoint-deemed-idle** to **micro-checkpoint-periodicity**, or vice versa, requires removing the first configuration before adding the new configuration.

### Example

The following example configures the S-GW session idle timer 3600 seconds (one minute).

```
timeout idle 3600
```



CHAPTER 44

# SLs Service Configuration Mode Commands

The SLs interface is used to convey Location Services Application Protocol (LCS-AP) messages and parameters between the MME to the E-SMLC. It is also used for tunnelling LTE Positioning Protocols (LPP between the E-SMLC and the target UE, LPPa between the E-SMLC and the eNodeB), which are transparent to the MME.

**Command Modes**

Exec > Global Configuration > Context Configuration > SLs Service Configuration

**configure > context** *context_name* **> sls-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sls-service)#
```

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


- bind, on page 483
- do show, on page 485
- end, on page 485
- esmlc, on page 485
- exit, on page 487
- ip, on page 487
- max-retransmissions, on page 488
- t-3x01, on page 488
- t-3x02, on page 489


# bind

Binds the SLs service to a local SCTP IP address, configures the SCTP port number, and associates an SCTP parameter template. This interface is used by the SLs service to communicate with the E-SMLC.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SLs Service Configuration

**configure** > **context** *context_name* > **sls-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sls-service)#
```

## Syntax Description

**bind { ipv4-address** *ipv4_address_value1* **[ ipv4-address** *ipv4_address_value2* **] | ipv6-address** *ipv6_address_value1* **[ ipv6-address** *ipv6_address_value2* **] [ port** *port_num* **] } sctp-template** *sctp_param_template_name*
**no bind**

### no

Removes the interface binding from this SLs service.

### ipv4-address *ipv4_address_value1* [ ipv4-address *ipv4_address_value2* ]

Specifies the IPv4 address of an interface in the current context through which communication with the E-SMLC occurs.

A second IPv4 address can be specified for multi-homing purposes with the optional **ipv4-address** keyword.

### ipv6-address *ipv6_address_value1* [ ipv6-address *ipv6_address_value2* ]

Specifies the IPv6 address of an interface in the current context through which communication with the E-SMLC occurs.

A second IPv6 address can be specified for multi-homing purposes with the optional **ipv6-address** keyword.

### port *port_num*

Specifies the SCTP port through which communication with the E-SMLC occurs.

*port_num* must be an integer from 1 through 65535. Default: 9082.

### sctp-template *sctp_param_template_name*

Associates an existing SCTP Parameter Template with this SCTP connection.

The SCTP template is mandatory for the SLs Service to start.

## Usage Guidelines

Use this command to bind the SLs service to an IP address.

This command is service critical; removing the configuration will stop the SLs service.

Up to 2 IPv4 or 2 IPv6 addresses can be specified for multi homing purposes.

### Example

The following command configures 2 IPv4 addresses for the SCTP connection (for multi-homing), assumes the default SCTP port of 9082, and associates this connection with an SCTP parameter template named *sctp_sls*:

```
bind ipv4-address 209.165.200.234 ipv4-address 209.165.200.244
sctp-template sctp_sls
```

# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `do show`

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `end`

**Usage Guidelines** Use this command to return to the Exec mode.

# esmlc

Configures an Evolved Serving Mobile Location Center (E-SMLC) within this SLs service. The E-SMLC provides location information to the MME.

**Product** MME

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > SLs Service Configuration

**configure > context** *context_name* **> sls-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sls-service)#
```

## Syntax Description

**esmlc esmlc-id** *esmlc_id_value* **{ ipv4-address** *ipv4_address_value1* **[ ipv4-address** *ipv4_address_value2* **] | ipv6-address** *ipv6_address_value1* **[ ipv6-address** *ipv6_address_value2* **] } port** *port_num* **weight** *weight-val*
**no esmlc-id** *esmlc_id_value*

### esmlc-id *esmlc_id_value*

Specifies an ID to uniquely identifiy this E-SMLC within this SLs service.

*esmlc_id_value* must be an integer from 0 through 255.

### ipv4-address *ipv4_address_value1* [ ipv4-address *ipv4_address_value2* ]

Specifies the IPv4 address of the E-SMLC to be used by this SLs service.

A second IPv4 address can be specified for multi-homing purposes with the optional **ipv4-address** keyword.

### ipv6-address *ipv6_address_value1* [ ipv6-address *ipv6_address_value2* ]

Specifies the IPv6 address of the E-SMLC to be used by this SLs service.

A second IPv6 address can be specified for multi-homing purposes with the optional **ipv6-address** keyword.

### port *port_num*

Specifies the SCTP port number of the E-SMLC server.

*port_num* must be an integer from 1 through 65535. Default: 9082.

### weight *weight-val*

The MME performs a weighted round robin selection of E-SMLC based on this weight factor.

*weight-val* must be an integer from 1 through 5, where 1 represents the least available capacity and 5 represents the greatest.

## Usage Guidelines

Use this command to configure an E-SMLC within this SLs service. The E-SMLC provides location information to the MME.

Up to 8 E-SMLC entries can be configured per SLs service.

The SLs service is started when the first E-SMLC is configured. The SLs service is stopped when the last E-SMLC is removed.

A single E-SMLC can be configured to serve multiple MMEs or multiple SLs services within the same MME.

### Example

The following command creates an E-SMLC entry for this SLs service for an E-SMLC with an IPv6 address, a port value of 9082 (default), and a round robin selection weight value of 5 (highest capacity).

```
esmlc esmlc-id 1 ipv6-address fe80::2e0:b6ff:fe01:3b7a port 9082 weight
5.
```

# exit

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**exit**

**Usage Guidelines**

Use this command to return to the parent configuration mode.

# ip

This command configures the IP parameters on the SLs interface.

**Product**

MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SLs Service Configuration

**configure > context** *context_name* **> sls-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-sls-service)#`

**Syntax Description**

**[ no ] ip qos-dscp** *dscp_value*

**no**

Removes IP parameter configuration from the SLs service/interface.

**qos-dscp *dscp_value***

The **qos-dscp** keyword designates the Quality of Service - Differentiated Services Code Point value to the packet leaving through the SLs interface.

*dscp_value* is a value assigned to the packet for DSCP marking. The value can be a pre-defined DSCP value or an arbitrary value ranging from 0x01 to 0x3F.

**Usage Guidelines**

SLs interface allows Differentiated Services Code Point (DSCP) marking functionality. DSCP marking helps in packet traffic management. DSCP marking can be performed on both IPv4 and IPv6 packets leaving the SLs interface.

Either the pre-defined DSCP values can be used for marking, or any arbitrary value ranging from 0x01 to 0x3F can be assigned. The default DSCP value is 0x00 or be (Best Effort). The default DSCP value is automatically set when the configuration is disabled.

### Example

The following command shows the IP configuration for DSCP marking on the SLs service.

```
ip qos-dscp ef
```

# max-retransmissions

Configures the maximum number of times the MME will resend messages to the E-SMLC.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SLs Service Configuration

**configure > context** *context_name* **> sls-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sls-service)#
```

**Syntax Description**

**max-retransmissions reset** *retries*
**default max-retransmissions reset**

#### default

Resets the command to the default of 0 (zero).

#### reset

Configures the maximum number of times the MME will resend the RESET REQUEST to the E-SMLC

*retries* must be an integer from 1 to 5. The default setting is 0.

**Usage Guidelines**

Use this command to configure the maximum number of times the MME will resend the RESET REQUEST to the E-SMLC.

Refer to the **t-3x02** command to configure the timer settings for resending the Reset Request message to the E-SMLC.

# t-3x01

Configures timer settings for "low delay" and "delay tolerant" response times from the E-SMLC.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SLs Service Configuration

**configure** > **context** *context_name* > **sls-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sls-service)#
```

**Syntax Description**

**t-3x01 low-delay** *seconds* **delay-tolerant** *seconds*
**default t-3x01**

#### default

Resets the timer to the default setting of 20 seconds for both low delay and delay tolerant requests.

#### low-delay

Indicates the number of seconds within which the MME expects to receive a "low delay" response from the E-SMLC, where fulfillment of the response time requirement takes precedence over fulfillment of the accuracy requirement.

*seconds* must be an integer from 10 to 30. The default setting is 20 seconds.

#### delay-tolerant

Indicates the number of seconds within which MME expects to receive a "delay tolerant' response from the E-SMLC, where fulfillment of the accuracy requirement takes precedence over fulfillment of the response time.

*seconds* must be an integer from 10 to 40. The default setting is 20 seconds.

**Usage Guidelines**

These timer options can be configured to prioritize location request response times from the E-SMLC. The T-3x01 timer is started by the MME on sending a location-request to the E-SMLC, and is stopped when either the requested is responded, aborted, or reset by either the MME or the E-SMLC.

A location procedure ends after the Delay Tolerant timer expires and no response is received from an E-SMLC.

More details about these settings are available in 3GPP TS 22.071.

#### Example

The following command configures the low-delay timer for 15 seconds and the delay-tolerant timer for 25 seconds.

```
t-3x01 low-delay 15 delay-tolerant 25
```

# t-3x02

Configures timer settings for resending the Reset Request message to the E-SMLC.

**Product**

MME

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SLs Service Configuration

**configure** > **context** *context_name* > **sls-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sls-service)#
```

## Syntax Description

```
t-3x02  seconds
default t-3x02
```

### default

Resets the timer to the default setting of 3 seconds.

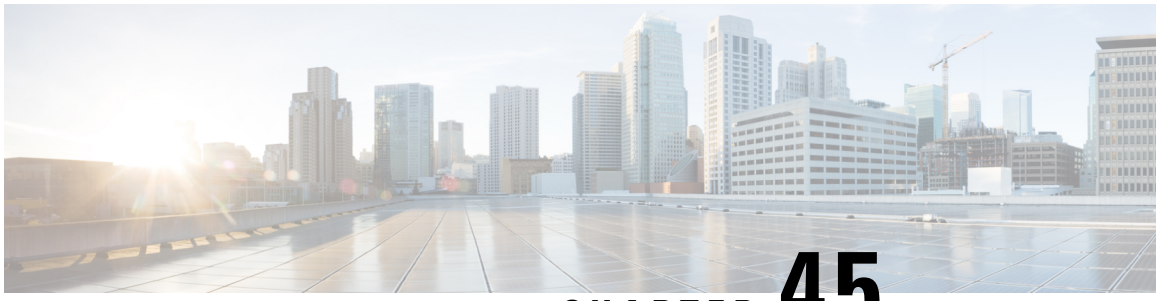
### *seconds*

*seconds* must be an integer from 1 to 5. The default setting is 3 seconds.

## Usage Guidelines

The T-3x02 timer is started on the MME when the MME sends a RESET REQUEST to the E-SMLC. Once the T3x02 timer expires, the MME can resend the RESET REQUEST to the E-SMLC.

Refer to the **max-retransmissions** command to configure the maximum number of times the MME will resend a RESET REQUEST to the E-SMLC.



CHAPTER 45

# SMS Service Configuration Mode Commands

The SGSN uses the SMS Service component to communicate via the Gd interface with a gateway message service controller (GMSC) to send short text messages (up to 140 octets in length) to a mobile (SMS-MT) and/or receive messages from a mobile (SMS-MO) .

**Command Modes**

The SMS (short message service) Service configuration mode is used to create and manage properties of the SMS Service configuration.

Exec > Global Configuration > Context Configuration > MAP Service Configuration > SMS Service Configuration

**configure > context** *context_name* **> map-service** *service_name* **> short-message-service**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-map-service-service_name-sms-service)#
```

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


- cp-data, on page 491
- do show, on page 492
- end, on page 493
- exit, on page 493
- mo-message-forwarding-destination, on page 493
- smsc-address-restiction-list, on page 494
- smsc-address-restiction-type, on page 495
- smsc-address-selection-prioritization, on page 496
- smsc-routing, on page 497
- timeout, on page 498


# cp-data

Enables the SGSN to send and/or receive cp-data (text messages).

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > MAP Service Configuration > SMS Service Configuration

**configure > context** *context_name* **> map-service** *service_name* **> short-message-service**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-map-service-service_name-sms-service)#`

**Syntax Description**

**`cp-data max-retransmission`** *`retries_num`*
**`default cp-data max-retransmissions`**

**default**

This keyword resets the SGSN's max-retransmission to the default number of retries.

**max-retransmission *retries_num***

*retries_num:* enter an integer from 1 to 3.

**Usage Guidelines**

Use this command to configure the number of times the SGSN will attempt to retransmit a message.

**Example**

**`cp-data max-retransmission`** *`2`*

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**`do show`**

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`end`**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`exit`**

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

# mo-message-forwarding-destination

This command defines the SGSN's handling policy for MO (mobile originating) message.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > MAP Service Configuration > SMS Service Configuration

**configure > context** *context_name* **> map-service** *service_name* **> short-message-service**

Entering the above command sequence results in the following prompt:

`[`*`context_name`*`]`*`host_name`*`(config-map-service-`*`service_name`*`-sms-service)#`

**Syntax Description** **`[ default ] mo-message-forwarding-destination { gmsc-selected-from-imsi | smsc-supplied-by-subscriber }`**

**default**

Resets the SMS service configuration to the default message forwarding technique.

#### gmsc-selected-from-imsi

Entering this keyword enables SMS-MO messages to be forwarded on the basis of their IMSI prefix.

#### smsc-supplied-by-subscriber

Entering this keyword enables SMS-MO messages to be forwarded on the basis of the SMSC (SMS controller) address provided by the subscriber.

### Usage Guidelines

Use this command to define how the mobile originated SMS are to be routed.

#### Example

```
mo-message-forwarding-destination gmsc-selected-from-imsi
```

# smsc-address-restiction-list

Define the list of SMS-C addresses to be screened.

### Product

SGSN

### Privilege

Security Administrator, Administrator

### Command Modes

Exec > Global Configuration > Context Configuration > MAP Service Configuration > SMS Service Configuration

**configure** > **context** *context_name* > **map-service** *service_name* > **short-message-service**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-map-service-service_name-sms-service)#
```

### Syntax Description

**smsc-address-restriction-list** *isdn-no +*
**no smsc-address-restriction-list** *isdn-no*

#### no

Delete an SMS-C address (ISDN number) from the list.

#### *isdn-no +*

Enter up to 10 ISDN numbers, each up to 15 digits. Put a single space, without a comma, between each ISDN number being added to the list with one command.

### Usage Guidelines

Use this command to identify a list of SMS-C that are to be screened and restricted from receiving forwarded SMS. This list is part of the SMS-C address denial mechanism. For the mechanism to actually function, a second command must be configured, the **smsc-address-restriction-list** command.

#### Example

Add 3 ISDN numbers to the list of restricted SMS-C addresses.

**smsc-address-restriction-list** *443719933751427 422311198977765 901231445513131*

Remove an ISDN number from the list of restricted SMS-C addresses.

**no smsc-address-restriction-list** *443719933751427*

# smsc-address-restiction-type

Define the list of SMS-C addresses to be screened.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > MAP Service Configuration > SMS Service Configuration

**configure > context** *context_name* **> map-service** *service_name* **> short-message-service**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-map-service-service_name-sms-service)#`

**Syntax Description**

**smsc-address-restriction-type { mo-mt-sms | mo-sms | mt-sms }**
**default smsc-address-restriction-type**

**default**

Resets the restriction type to the default of both MT and MO types.

**mo-mt-sms**

Sets the restriction for both types of messages - mobile-originated (MO-SMS) and mobile-terminated (MT-SMS).

**mo-sms**

Sets the restriction for the mobile-originated (MO-SMS) messages.

**mo-mt-sms**

Sets the restriction for the mobile-terminated (MT-SMS) messages.

**Usage Guidelines**

Use this command to identify the types of messages that are to be denied to the SMS-C identified in the **smsc-address-restriction-type**. Both commands must be configured for the SMS-C address denial mechanism to function.

**Example**

Restrict MO-SMS messages from being forwarded to the SMS-C listed in the restriction list:

**smsc-address-restriction-type mo-sms**

Reset the restriction to both types of messages:

**default smsc-address-restriction-type**

# smsc-address-selection-prioritization

Define the routing selection priority for the SMSC (short message service center) address to be used for all MO-SMS.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > MAP Service Configuration > SMS Service Configuration

**configure > context** *context_name* **> map-service** *service_name* **> short-message-service**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-map-service-service_name-sms-service)#`

**Syntax Description**

**smsc-address-selection-prioritization from-ms** *priority* **imsi-prefix** *priority* **msisdn-prefix** *priority*
**default smsc-address-selection-prioritization**

#### from-ms *priority*

Configures a priority for the SMSC address send from the MS.

*priority* : Value must be a single digit, range 1-3.

#### imsi-prefix *priority*

Configures a priority for the SMSC address that is based on the IMSI-prefix.

*priority* : Value must be a single digit, range 1-3.

#### msisdn-prefix *priority*

Configures a priority for the SMSC address that is based on the MSISDN-prefix.

*priority* : Value must be a single digit, range 1-3.

#### default

By including the **default** keyword with the command, the SGSN knows to use the encoded default priorities for SMSC address selection for SMSC routing:

- *from-ms* priority 1,
- *imsi-prefix* priority 2,
- *msisdn-prefix* priority 3.

**Usage Guidelines**

Use this command to define SMSC address routing priorities. Priorities must be defined for all parameters, all keywords, but they can be entered in any order. The addresses for the SMSCs are defined with the **smsc-routing** command.

An operator can use this configuration to prevent subscribers from using unauthorized SMSC addresses, for example, an unauthorized international SMSC.

### Example

The keywords can be entered in any order but all keywords must be included in the command:

**smsc-address-selection-prioritization msisdn-prefix** *3* **from-ms** *1* **imsi-prefix** *2*

# smsc-routing

This command configures the routing to the short message service center (SMSC).

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > MAP Service Configuration > SMS Service Configuration

**configure > context** *context_name* **> map-service** *service_name* **> short-message-service**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-map-service-service_name-sms-service)#`

**Syntax Description**

**[ no ] smsc-routing { { any | imsi-starts-with | msisdn-starts-with } { isdn** *isdn_number* **| mobile-global-title** *mgt_number* **[ max-gt-address-len** *max_gt_length* **] | point-code** *pt_code* **} }**

### any

Configures routing according to any IMSI prefix.

### imsi-starts-with *IMSI_prefix*

Defines the IMSI prefix. Enter a string of up to 15 digits.

### msisdn-starts-with *msisdn_prefix*

Defines the MSISDN prefix. Enter a string of up to 15 digits.

### isdn *isdn_number*

Defines the ISDN E.164 number (up to 15 digits) of the SMSC.

**mobile-global-title *mgt_number* [ max-gt-address-len *max_gt_length* ]**

Defines the mobile global title (MGT) E.214 address to be used for IMSI conversion.

Optionally, the maximum length of the GT address can be defined. If the length of the MGT string is greater than the defined max, then the least significant digits will be omitted.

*mgt_number* is a string of digits, up to 18 digits.

*max_gt_address* is an integer from 1 to 32.

**point-code *pt_code***

Defines the point code for the SMSC. Enter a string of up to 11 digits in SS7 dotted decimal or decimal format

**Usage Guidelines**

This command defines the address format (IMSI, point code, mobile global title) and the address for SMSC routing.

**Example**

Use this command to define routing to the SMSC based on any point code.

```
smsc-routing any point-code 1.222.1
```

# timeout

This command defines the SMS service timers.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > MAP Service Configuration > SMS Service Configuration

**configure** > **context** *context_name* > **map-service** *service_name* > **short-message-service**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-map-service-service_name-sms-service)#
```

**Syntax Description**

```
timeout { tc1n-timertime | tr1n-timer time | tr2n timer time }
default timeout { tc1n-timer | tr1n-timer | tr2n timer }
```

**default**

Resets the configuration to the default value for the specified timer.

**tc1n-timer *time***

Configures the TC1N timer in seconds.

*time:* Must an integer from 1 to 255. The default is 5 seconds.

**tr1n-timer *time***

Configures the TR1N timer in seconds.

*time:* Must an integer from 1 to 255. The default is 30 seconds.

**tr2n-timer *time***

Configures the TR2N timer in seconds.

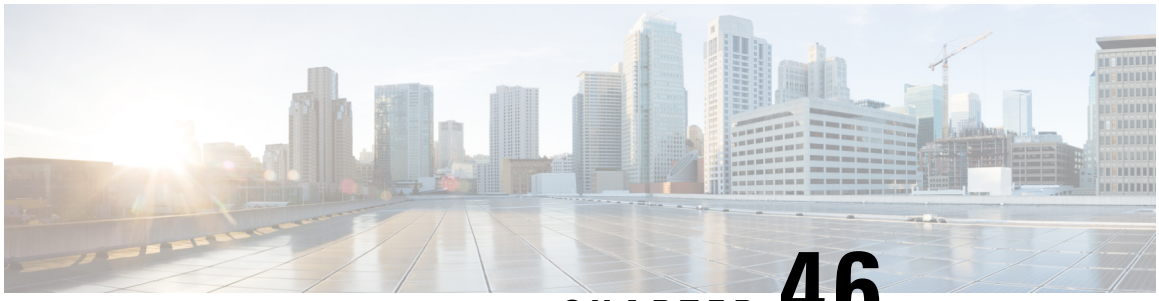
*time:* Must an integer from 1 to 255. The default is 30 seconds.

## Usage Guidelines

Use this command to set SMS service timers. The command can be repeated to set all of the timers, one-at-a-time.

### Example

```
tr1n-timer 25
```



CHAPTER 46

# SS7 Routing Domain Configuration Mode Commands

**Command Modes**

The SS7 Routing Domain configuration mode is used to configure Signaling System 7 (SS7) parameters. For convenience in configuration management, all SS7 parameters have been collected into a proprietary grouping called an *SS7 routing domains*.

Exec > Global Configuration > SS7 Routing Domain Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-ss7-routing-domain-ss7rd_id)#`

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


- asp, on page 501
- description, on page 502
- do show, on page 503
- end, on page 504
- exit, on page 504
- inbound-asp-identifier validate, on page 504
- linkset, on page 505
- MTU-size, on page 506
- peer-server, on page 506
- route, on page 507
- routing-context, on page 508
- ssf, on page 509


# asp

This command creates or removes an M3UA Application Server Process (ASP) instance and enters the ASP configuration mode. See the *SGSN ASP Configuration Mode* chapter in the *Command Line Interface Reference* for command details.

**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

**Product**

SGSN

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-routing-domain-ss7rd_id)#
```

**Syntax Description**

**asp instance** *asp_inst*
**no asp instance** *asp_inst*
**default asp instance** *asp_inst* **end-point port**

**no**

Deletes the ASP instance for the SS7 routing domain configuration.

**default**

Sets the ASP instance parameters to the end-point port value of 2905.

**instance *asp_inst***

Identifies a specific ASP configuration. Up to four ASP instances can be configured for a single SS7 routing domain.

*asp_inst* : instance must be an integer from 1 through 4. For SGSN with release 15.0, the instance must be an integer from 1 to 12.

**Usage Guidelines**

Use this command to create an ASP instance or enter the ASP configuration mode.

**Example**

The following command enters the ASP configuration mode for a specific ASP.

```
asp instance 1
```

# description

This command defines an alphanumeric string that describes the current SS7 routing domain. This is used for operator reference only.

**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

**Product**

SGSN

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-ss7-routing-domain-ss7rd_id)#`

**Syntax Description**

**description** *string*
**no description**

**no**

Removes the description string from the current SS7 routing domain configuration.

***string***

Specifies the alphanumeric string that is stored. Strings with spaces must be enclosed in double-quotes (see the example below).

*string:* Must be from 1 to 255 alphanumeric characters.

**Usage Guidelines**

Use this command to set a description for reference by operators.

**Example**

The following command sets the description to identify a routing domain for messages transmitted within a national boundary.

**description** *"National Service Routing Domain"*

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**do show**

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character | is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# inbound-asp-identifier validate

This command enables validation of ASP identifiers inbound to the SGSN via routes defined with this SS7 routing domain.



**Important** This command is only available in Release 8.1 and higher releases.

**Product** SGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > SS7 Routing Domain Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-ss7-routing-domain-ss7rd_id)#`

**Syntax Description**

```
inbound-asp-identifier validate
default inbound-asp-identifier validate
no inbound-asp-identifier validate
```

**default**

Validates the inbound ASP Id.

**no**

Disables validation of the inbound ASP Id.

**Usage Guidelines** The standard is to validate the ASP Id. However, in some circumstances it is necessary to skip such validation. For example, if the same ASP Id is assigned to more than one RNC (peer-server).

**Example**

Use the following command to skip validation of inbound ASP Ids:

```
no inbound-asp-identifier validate
```

Use either of the following commands to enable validation if it has been disabled:

```
default inbound-asp-identifier validate
inbound-asp-identifier validate
```

# linkset

This command creates an instance of an MTP3 linkset and enters the Linkset configuration mode. See the Linkset configuration mode chapter for the commands to configure the linkset.

**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

**Product** SGSN

HNB-GW

**Privilege** Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-ss7-routing-domain-ss7rd_id)#`

**Syntax Description**

**linkset id** *id*
**no linkset id** *id*

**no**

Removes the identified linkset definition from the system configuration.

***id***

This value uniquely identifies a linkset for the specific SS7 routing domain.

*id* : Must be an integer of 1 to 49.

**Usage Guidelines**

This command creates instances of linkset configurations and provides access to the linkset configuration mode.

**Example**

Use the following command to create the 12th linkset:

**linkset id** *12*

# MTU-size

This command has been deprecated.

# peer-server

This command creates a peer-server instance to setup a SIGTRAN peer for sending and receiving M3UA traffic. Completing the command automatically enters the peer- server configuration mode. To define 1 or more (up to 145) peer servers, use the commands documented in the *Peer-Server Configuration Mode* chapter in this reference.



**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

**Product**

SGSN

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-routing-domain-ss7rd_id)#
```

**Syntax Description**

**peer-server id** *srvr_id*
**no peer-server id** *srvr_id*

**no**

Removes the identified peer-server definition from the system configuration.

***srvr_id***

*srvr_id* uniquely identifies a peer-server. The id must be an integer from 1 to 144. For SGSN Release 15.0, the id must be an integer from 1 to 256.

**Usage Guidelines**

Use the following command to create a definition for peer-server 2 and enter the configuration mode to configure the communication parameters for peer-server 12.

**Example**

**peer-server id** *12*

# route

This command configures SS7 routes for the current SS7 routing domain.

**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

**Product**

SGSN

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-routing-domain-ss7rd_id)#
```

**Syntax Description**

**route destination-point-code** *dp_code* **{ linkset id** *id* **[ priority** *pri_value* **] | peer-server-id** *srvr_id* **}**

**no route destination-point-code** *dp_code* **{ linkset id** *id* **| peer-server-id** *srvr_id* **}**

**no**

Removes the SS7 route from the current SS7 routing domain configuration.

**destination-point-code *dp_code***

Specifies the SS7 destination point code for this route.

Reminder: the point-code structure must match the variant defined for the SS7 routing domain when the SS7RD was configured in the global configuration mode.

**linkset id *id***

This keyword identifies a linkset instance, created and configured with the **linkset** command.

This keyword identifies a linkset instance, created and configured with the **linkset** command.

*id* : Must be an integer from 1 to 49.

**peer-server-id *srvr_id***

This keyword identifies a peer-server configuration instance, created and configured with the **peer-server** command.

*srvr_id* must be an integer from 1 to 49.

**Usage Guidelines**

This command associates the previoiusly configured linksets and peer servers and the destination point codes with a specified SS7 route.

**Example**

Define a route setting an ITU-type destination point-code address for the linkset Id 12:

**route destination-point-code** *6.211.6* **linkset id** *12*

# routing-context

Identifies the routing context for this SS7 routing domain.

**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

**Product**

SGSN

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-ss7-routing-domain-ss7rd_id)#`

**Syntax Description**

**`routing-context`** *`value`*
**`default routing-context`**

**default**

Resets the local routing context value to the index (instance ID) for this SS7 routing domain.

***value***

An integer that uniquely identifies the routing context for this SS7 routing domain.

*value* : Must be integers from 1 to 65535 (for releases 8.0) or 1 to 4294967295 (for releases 8.1 to 17.0) or 0 to 4294967295 (for releases 17.1 and higher) .

**Usage Guidelines**

Use this command to set the routing context IDs for a specific SS7 routing domain configuration.

**Example**

**`routing-context`** *`2355`*

# ssf

This command sets the network indicator in the subservice field for SS7 message signal units (MSUs).

**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

**Product**

SGSN

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SS7 Routing Domain Configuration

**configure > ss7-routing-domain** *routing_domain_id* **variant** *variant_type*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-ss7-routing-domain-ss7rd_id)#`

**Syntax Description**

**`ssf ( international | national | reserved | spare }`**

**international**

The network indicator identifies the message as international with a point code structure that does not match the national point code structure,

**national**

The network indicator identifies the messages as having a national point code structure.

**reserved**

Provides an alternate network indicator for national messages.

**spare**

Provides an alternate network indicator for international messages.

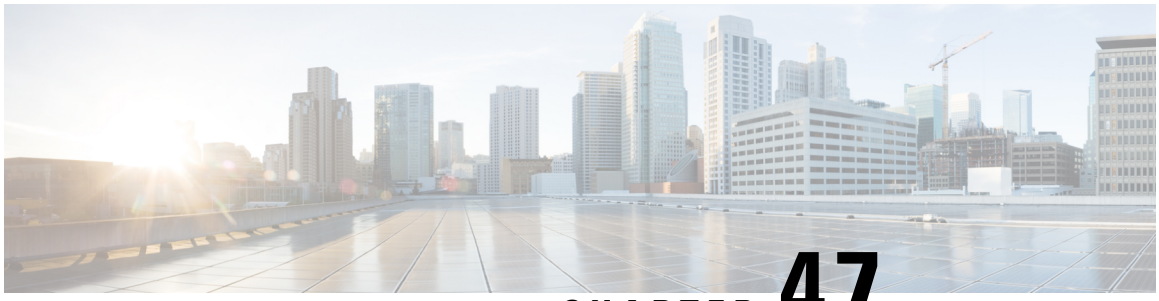
## Usage Guidelines

In SS7 signaling, the Message Transfer Part (MTP) Level 2 message signal units (MSUs) contain a service information octet (SIO). The SIO field in an MSU contains a 4-bit subservice field (SSF) followed by a 4-bit service indicator. The indicator carried in the message's routing information typically identifies the structure of the point code as a message from within a nation or as a message coming from outside the nation - international. As well, the 4-bit SSF determines the point code structure of the messages transmitted from the SGSN.

### Example

For messages being transmitted within a country, set the indicator to national with the following command.

```
ssf national
```



CHAPTER 47

# SSHD Configuration Mode Commands

The Secure Shell Configuration Mode is used to manage the SSH server options for the current context.

**Important**

- Use the **ssh generate key** command in Context Configuration Mode to generate the sshd keys before you can configure the sshd server.
- The global limit for utility service connections, including SSH, Telnet, and SFTP, is 201. This includes any inter-card communication that uses SSH.

## Command Modes

Exec > Global Configuration > Context Configuration > SSH Configuration

**configure > context** *context_name* **> server sshd**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sshd)#
```

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


- allowusers add, on page 512
- authorized-key, on page 513
- challenge-response-authentication, on page 514
- ciphers, on page 515
- client-alive-countmax, on page 517
- client-alive-interval, on page 518
- do show, on page 519
- end, on page 519
- exit, on page 520
- listen, on page 520
- macs, on page 521
- max servers, on page 522
- subsystem, on page 523

# allowusers add

Specifies and controls which users can access SSH services.

**Product**

All

**Privilege**

Security Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SSH Configuration

**configure > context** *context_name* **> server sshd**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sshd)#
```

**Syntax Description**

**[ default | no ] allowusers add** *user_list*

**default**

Unrestricted access for all users.

**no**

Removes the list of user name patterns resulting in unresticted access by all users.

***user_list***

Specifies a list of user name patterns, separated by spaces, as an alphanumeric string of 1 through 999 characters. If the pattern takes the form 'USER' then login is restricted for that user. If the pattern is in the format 'USER@IP_ADDRESS' then USER and IP address are separately checked, restricting logins to those users from that particular iIP address.

The following limits apply to the *user_string*:

- The maximum length of this string is 3000 bytes including spaces.
- The maximum number of allowusers, which is counted by spaces, is 256, which is consistent with the limit from OpenSSH.

**Important** If you exceed either of the above limits, an error message is displayed. The message prompts you to use a regular expression pattern to shorten the string, or remove all the allowusers with **no allowusers add** or **default allowusers add** and re-configure.

**Important** For more details about how to create complex rules, see the OpenSSH sshd_config man page. add - Add more users to the list of user name patterns.

**Usage Guidelines**

Use this command to specify and control which users can access SSH services.

Access to a service may be restricted to users having a legitimate need. This restriction applies on a white-list basis: only explicitly allowed users shall connect to a host via SSH and possibly from a specified source IP addresses. Under OpenSSH, the AllowUsers directive of sshd_config specifies a list of SSH authorized users and groups.

### Example

The following command specifies an AllowUsers list of four users:

```
allowusers add user1 user2@10.1.1.1 user3@10.1.1.2 user4
```

# authorized-key

Sets or removes a user name having authorized keys for access to the sshd server in the current context.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SSH Configuration

**configure > context** *context_name* **> server sshd**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sshd)#
```

**Syntax Description**

**authorized-key username** *user_name* **host** *host_ip* **[ type { v2-dsa | v2-rsa } ]**

#### default

Resets the parameter to the default value.

#### username *user_name*

Sets a username as having authorized keys for access to the sshd server. Specifies the username as an alphanumeric string of 1 through 255 characters.

#### host *host_ip*

Associates an SSH host having the authorization keys for the username as an host IP address in IPv4 dotted decimal or IPv6 colon-separated-hexadecimal notation.

#### [ type { v2-dsa | v2-rsa } ]

Specifies which type of SSH authorization key will be accepted instead of all key types. The options are: **v2-dsa** (SSHv2 Digital Signature Algorithm), or **v2-rsa** (SSHv2 Rivest, Shamir and Adleman).

**Usage Guidelines**

Use this command to set a username with authorized keys for access to the sshd server within the current context.

Usernames should be created using the **nopassword** option to prevent bypassing of the sshd keys (**administrator** command in Context Configuration mode).

**Important** Only 10 sshd authorization-keys can be configured per context.

### Example

The following command specifies that username *dbailey* with authorization keys at host IP address *209.165.200.225* can access the system with all types of authorization keys:

```
authorized-key username dbailey host 209.165.200.225
```

# challenge-response-authentication

The challenge-response-authentication option under SSHD configuration is used to enable the Keyboard Interactive Authentication method.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > SSH Configuration

**configure > context** *context_name* **> server sshd**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sshd)#
```

**Syntax Description** **`[ no ] challenge-response-authentication`**

#### no

Disables the challenge-response-authentication parameter.

#### challenge-response-authentication

Enables the challenge-response-authentication in SSHD server configuration.

**Note**

1. The challenge-response-authentication option is only supported from release 21.28.
2. Enabling challenge-response-authentication is only advised in certain special cases. For example, when the TACACS server chooses to display a specific prompt to the user. Unless there is a very specific reason, challenge-response-authentication must not be enabled. Contact your Cisco representative before enabling this option.
3. Even though it is not explicity restricted, customers are strongly advised not to enable challenge-response-authentication for any products other than legacy PGW, SGW, and SAEGW.
4. To use Keyboard Interactive Authentication method, challenge-response-authentication must be enabled under the context which owns the IP address that is used for SSH login.
5. The challenge-response-authentication has no effect on SSH logins through the console.
6. The challenge-response-authentication is an SSHD option, and it doesn't affect logins for telnet or FTP.
7. The user responses must be of size less than 128 bytes.

**Important** We envisage challenge-response-authentication being used in conjunction with TAC special cases. The TACACS server can send up to 511 characters in AUTHEN-RE and those characters shall be passed to the end user who is trying to login. If the len field is 512 bytes or above, following error message is shown to the user and TAC as expected: ERROR: Enter any key to proceed.

8. When challenge-response-authentication is enabled, the user has 60 seconds to respond to the prompt.

# ciphers

Configures the cipher priority list in sshd for SSH symmetric encryption. It changes the cipher option for that context.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SSH Configuration

**configure > context** *context_name* **> server sshd**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sshd)#
```

**Syntax Description**

**[ default ] ciphers** *algorithm*

**default**

**Release 20.x to 21.15 (Normal build only)**

Resets the value of *algorithm* in a Normal build to:

```
blowfish-cbc,3des-cbc,aes128-cbc,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com
```

Resets the value of *algorithm* in a Trusted build as follows:

```
aes256-ctr,aes192-ctr,aes128-ctr
```

**Release 21.16 onwards: Post OpenSSH to CiscoSSH Upgrade and Migration**

**Default Algorithms in a Normal Build:**

```
aes256-ctr,aes192-ctr,aes128-ctr,aes256-gcm@openssh.com,aes128-gcm@openssh.com,chacha20-poly1305@openssh.com
```

**Available Algorithms in a Normal Build:**

```
aes256-ctr,aes192-ctr,aes128-ctr,aes256-gcm@openssh.com,aes128-gcm@openssh.com,chacha20-poly1305@openssh.com,aes128-cbc
```

**Default and Available Algorithms in Trusted Builds:**

```
aes256-ctr,aes192-ctr,aes128-ctr
```

**Note** There is no change in the default and configurable Ciphers for Trusted builds.

***algorithm***

Specifies the algorithm to be used as a single string of comma-separated variables (no spaces) in priority order from those shown below:

- **blowfish-cbc** – symmetric-key block cipher, Cipher Block Chaining, CBC

**Note** This algorithm is removed post the OpenSSH to CiscoSSH upgrade and migration.

- **3des-cbc** – Triple Data Encryption Standard, CBC
- **aes128-cbc** – Advanced Encryption Standard, 128-bit key size, CBC
- **aes128-ctr** –Advanced Encryption Standard, 128-bit key size, Counter-mode encryption, CTR
- **aes192-ctr** – Advanced Encryption Standard, 192-bit key size, CTR
- **aes256-ctr** – Advanced Encryption Standard, 256-bit key size, CTR
- **aes128-gcm@openssh.com** – Advanced Encryption Standard, 128-bit key size, Galois Counter Mode [GCM], OpenSSH
- **aes256-gcm@openssh.com** – Advanced Encryption Standard, 256-bit key size, GCM, OpenSSH
- **chacha20-poly1305@openssh.com** – ChaCha20 symmetric cipher, Poly1305 cryptographic Message Authentication Code [MAC], OpenSSH

*algorithm* is a string of 1 through 511 alphanumeric characters.



**Important** For release 20.0 and higher Trusted builds, only the AES128-CTR, AES-192-CTR and AES-256CTR ciphers are available.

**Usage Guidelines** Use this command to configure the cipher priority list in sshd for SSH symmetric encryption.

**Example**

The following command sets the supported SSH algorithms and their priority.

```
ciphers blowfish-cbc,aes128-cbc,aes128-ctr,aes192-ctr,aes256-ctr
```

# client-alive-countmax

Sets the number of client-alive messages which may be sent without sshd receiving any messages back from the SSH client. If this threshold is reached while the client-alive messages are being sent, sshd disconnects the SSH client thus terminating the session.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > SSH Configuration

**configure** > **context** *context_name* > **server sshd**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sshd)#
```

**Syntax Description** **[ default | no ] client-alive-countmax** *count_number*

**default**

Sets the default value for this parameter to 3.



**Important** For higher security, Cisco recommends at least a client-alive-countmax of 2 and client-alive-interval of 5. Smaller session logout values may lead to occasional ssh session logouts. Adjust values to balance security and user friendliness.

**no**

Disables the client-alive-countmax parameter.

***count_number***

Specifies the number of times a client-alive message will be sent as an integer from 1 through 3. The messages are sent following the expiry of each client-alive interval. Default = 3

Unresponsive SSH clients will be disconnected when the maximum number of client-alive-intervals have expired.

**Usage Guidelines**

Use this command to set the number of client-alive messages which may be sent without sshd receiving any messages back from the SSH client. If this threshold is reached while client-alive messages are being sent, sshd will disconnect the SSH client, terminating the session. The client-alive messages are sent through the encrypted channel and, therefore, are not spoofable. The client-alive mechanism is valuable when the client or server depend on knowing when a connection has become inactive.



**Important** This parameter applies to SSH protocol version 2 only.

### Example

The following command sets the SSH client-alive-countmax to 2.

```
client-alive-countmax 2
```

# client-alive-interval

Sets a timeout interval in seconds after which if no data has been received from the SSH client, sshd sends a message through the encrypted channel to request a response from the client.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SSH Configuration

**configure > context** *context_name* **> server sshd**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sshd)#
```

**Syntax Description**

**[ default | no ] client-alive-interval** *seconds*

### default

Sets the client-alive-interval to 15 seconds.



**Important** For higher security, Cisco recommends at least a client-alive-interval of 5 and client-alive-countmax of 2. Smaller session logout values may lead to occasional ssh session logouts. Adjust values to balance security and user friendliness.

### no

Disables the client-alive-interval parameter.

***seconds***

Specifies the amount of time in seconds that sshd waits to receive a response from the SSH client as an integer from 1 through 15. Default = 15

**Usage Guidelines**

Use this command to set a timeout interval in seconds after which if no data has been received from the client, sshd sends a message through the encrypted channel to request a response from the client. The number of times that the message is sent is determined by the client-alive-countmax parameter. The approximate amount of time before sshd disconnects an SSH client disconnect = client-alive-countmax X client-alive-interval.



**Important** This parameter applies to SSH protocol version 2 only.

**Example**

The following command sets the SSH client-alive-interval to 5 seconds.

```
client-alive-interval 5
```

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privprivilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character | is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product**

All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# listen

Configures the SSH server in the current context to only listen for connections from the interface with the specified IP address. The default behavior is to listen on all interfaces.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > SSH Configuration

**configure > context** *context_name* **> server sshd**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sshd)#
```

**Syntax Description**

**listen** *ip_address*
**no listen**

**no**

Disable listening for a specific interface address and enable listening on all interfaces.

***ip_address***

Enables listening only on the interface with the specified IP address. *ip_address* must be entered using IPv4 dotted-decimal notation.

**Usage Guidelines** Use this command to configure the SSH server for the current context to only listen for connections from the interface with the specified IP address. Only one IP address may be set for listening.

### Example

The following command specifies that the Server should only listen for connections in the interface with the IP address of *192.168.0.10*:

```
listen 192.168.0.10
```

# macs

Configures the MAC algorithm priority list in sshd for SSH symmetric encryption. It changes the MAC algorithm for that context.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SSH Configuration

**configure > context** *context_name* **> server sshd**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sshd)#
```

**Syntax Description**

**macs***algorithm*

**default macs**

#### default

**Release 20.x to 21.15**

Resets the value of *algorithm* in a Normal build and Trusted build to:

```
hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha2-512,
hmac-sha2-256,hmac-sha1
```

Available algorithms in a Normal build are:

```
hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha2-512,
hmac-sha2-256,hmac-sha1,umac-128-etm@openssh.com,umac-128@openssh.com,umac-64-etm@openssh.com,umac-64@openssh.com
```

Available algorithms in a Trusted build are:

```
hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha2-512,
hmac-sha2-256,hmac-sha1
```

**Release 21.16 onwards: Post OpenSSH to CiscoSSH Upgrade and Migration**

**Default and Available Algorithms in Normal Builds:**

```
hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha2-512,
hmac-sha2-256,hmac-sha1
```

**Default Algorithms in Trusted Builds:**

```
hmac-sha2-512,hmac-sha2-256,hmac-sha1
```

**Available Algorithms in Trusted Builds:**

```
hmac-sha2-512,hmac-sha2-256,hmac-sha1
```

**Note** hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com are removed from the Trusted builds.

***algorithm***

- Specifies the algorithms to be used as a single string of comma-separated variables (no spaces) in priority order (left to right) from those listed as follows:
  - HMAC = hash-based message authentication code
  - SHA2 = Secure Hash Algorithm 2
  - SHA1 = Secure Hash Algorithm 1
  - ETM = Encrypt-Then-MAC
  - UMAC = message authentication code based on universal hashing

*algorithm* is a string of 1 through 511 alphanumeric characters.

**Usage Guidelines** Use this command to configure the priority of MAC algorithms in sshd for SSH symmetric encryption.

**Example**

The following command sets the supported MAC algorithms and their priority.

```
MACs
hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha2-512,hmac-sha2-256,hmac-sha1
```

# max servers

Configures the maximum number of SSH servers that can be started within any 60-second interval. If this limit is reached, the system waits two minutes before trying to start any more servers.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > SSH Configuration

**configure > context** *context_name* **> server sshd**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sshd)#
```

**Syntax Description** **max servers** *number*

***number***

Default: 40

Specifies the maximum number of servers that can be spawned in any 60-second interval. *number* must be an integer from 1 through 100.

In 16.0 and later releases, this range is increased to 1-4000 to support the Stranded CDR feature. For more information on this feature, see the "**gtpp push-to-active url**" CLI command in the Global Configuration mode.

**Usage Guidelines**

Set the number of servers to tune the system response as a heavily loaded system may need more servers to support the incoming requests.

The converse would be true as well in that a system can benefit by reducing the number of servers such that telnet services do not cause excessive system impact to other services.

**Example**

```
max servers 50
```

# subsystem

Configures the system to perform file transfers using Secure FTP (SFTP) over ssh v2. Administrators must be configured with the FTP attribute privilege to issue this command. This command also supports creation of SFTP subsystem root directories with access privileges. Administrators can assign an SFTP subsystem to local users.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > SSH Configuration

**configure > context** *context_name* **> server sshd**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sshd)#
```

**Syntax Description**

```
subsystem { cli | sftp [ name sftp_name root-dir pathname mode { read-only |
 readwrite } ] }
no
subsystem { cli | sftp }
no subsystem sftp name stfp_name
```

**no**

Disables the SFTP ssh file transfer method or access to the CLI via ssh or a specified SFTP subsystem.

**Important** An SFTP subsystem can only be removed if the subsystem is not currently assigned to any local user.

**cli**

Default: Enabled

Configures the SSH system for the current context to allow access to the CLI.

**sftp**

Default: Disabled

Enables the SSH system for the current context to perform file transfers using Secure FTP (SFTP) over ssh v2.

**name *sftp_name***

Assigns a name for this SFTP subsystem. *sftp_name* is an alphanumeric string that uniquely identifies this subsystem.

**root-dir *pathname***

Specifies the root directory to which SFTP files can be transferred. Options include:

- /hd-raid/records/cdr
- /flash

**mode { read-only | readwrite }**

Specifies the SFTP transfer mode. Options include:

- read-only
- read-write

## Usage Guidelines

Use this command to enable or disable file transfers using SFTP over an ssh v2 tunnel.

You can also create multiple SFTP subsystems with an associated pathname and access privilege (read-only or read-write). When creating a local user, an administrator can assign the user an SFTP subsystem. If the user is not an administrator, he or she will only be able to access the subsystem with read-only privilege. The SFTP subsystem directory becomes the SFTP user's root directory with associated access privileges.

Also use this command to enable or disable access to the CLI over an SSH connection.

### Example

The following command enables SFTP for the current context:

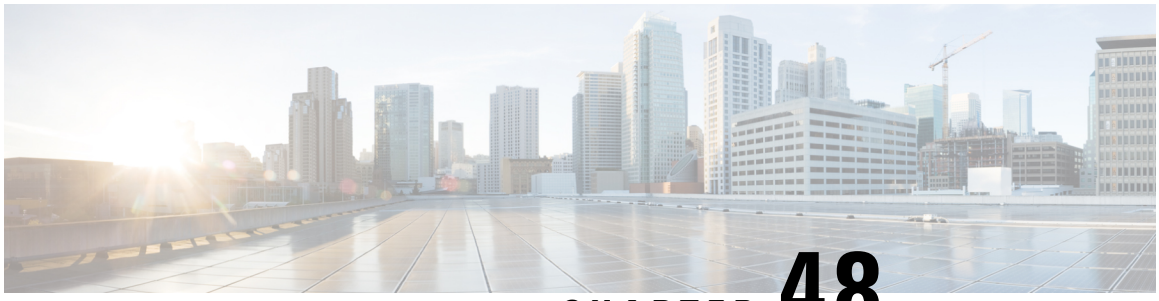
```
subsystem sftp
```

The following command disables access to the CLI through an SSH session for the current context:

```
no subsystem cli
```

The following command creates an SFTP subsystem for CDR records with read-write privileges:

```
subsystem sftp name cdr-rw-server root-dir /hd-raid/records/cdr mode
readwrite
```



CHAPTER 48

# SSH Client Configuration Mode Commands

The Secure Shell Client Configuration Mode manages SSH client key pairs that support secure access with external servers.

**Command Modes**

Exec > Global Configuration > Context Configuration > SSH Configuration

**configure > client ssh**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ssh)#
```

**Important**

- The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
- The global limit for utility service connections, including SSH, Telnet, and SFTP, is 201. This includes any inter-card communication that uses SSH.


- ciphers, on page 525
- do show, on page 527
- end, on page 527
- exit, on page 527
- preferredauthentications, on page 528
- ssh, on page 528


# ciphers

Configures the cipher priority list in SSH client symmetric encryption that is used to generate an SSH client key pair.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SSH Client Configuration

**configure > client ssh**

Entering the above command results in the following prompt:

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

## Syntax Description

**[ default ] ciphers** *algorithm*

### default

Resets the value of *algorithm* in a Normal build to:

```
aes256-ctr,aes192-ctr,aes128-ctr,aes256-gcm@openssh.com,aes128-gcm@openssh.com,chacha20-poly1305@openssh.com,
blowfish-cbc,3des-cbc,aes128-cbc
```

Resets the value of *algorithm* in a Trusted build to:

```
aes256-ctr,aes192-ctr,aes128-ctr
```

### *algorithm*

Specifies the algorithm(s) to be used as a single string of comma-separated variables (no spaces) in priority order from those shown below:

- **blowfish-cbc** – symmetric-key block cipher, Cipher Block Chaining, CBC
- **3des-cbc** – Triple Data Encryption Standard, CBC
- **aes128-cbc** – Advanced Encryption Standard, 128-bit key size, CBC
- **aes128-ctr** –Advanced Encryption Standard, 128-bit key size, Counter-mode encryption, CTR
- **aes192-ctr** – Advanced Encryption Standard, 192-bit key size, CTR
- **aes256-ctr** – Advanced Encryption Standard, 256-bit key size, CTR
- **aes128-gcm@openssh.com** – Advanced Encryption Standard, 128-bit key size, Galois Counter Mode [GCM], OpenSSH
- **aes256-gcm@openssh.com** – Advanced Encryption Standard, 256-bit key size, GCM, OpenSSH
- **chacha20-poly1305@openssh.com** – ChaCha20 symmetric cipher, Poly1305 cryptographic Message Authentication Code [MAC], OpenSSH

*algorithm* is a string of 1 through 511 alphanumeric characters.

**Important** For release 20.0 and higher Trusted builds, only the AES128-CTR, AES-192-CTR and AES-256CTR ciphers are available.

## Usage Guidelines

Use this command to configure the cipher priority list for SSH client symmetric encryption that is used to generate an SSH client key pair.

### Example

The following command sets the supported SSH algorithms and their priority.

```
ciphers blowfish-cbc,aes128-cbc,aes128-ctr,aes192-ctr,aes256-ctr
```

# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
end
```

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
exit
```

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

# preferredauthentications

Specifies the order in which the client should try SSH client protocol authentication methods. This allows the client to prioritize one method over another method – public key, keyboard-interactive and password.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SSH Client Configuration

**configure > client ssh**

Entering the above command results in the following prompt:

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

**Syntax Description**

**`[ default ] preferredauthentications`** *`methods`*

**default**

Resets the value of *methods* to:

`publickey,password`

***methods***

Specifies the preferred methods of authentication to be used as a single string of comma-separated variables (no spaces) in priority order (left to right) from those shown below:

- **publickey** – authentication via SSH v2-RSA protocol.
- **keyboard-interactive** – request for an arbitrary number of pieces of information. For each piece of information the server sends the label of the prompt.
- **password** – simple request for a single password

**Usage Guidelines**

Use this command to specify the order in which the client should try SSH client protocol authentication methods. This allows the client to prioritize one method over another method – public key, keyboard-interactive and password.

**Example**

The following command sets the supported SSH authentication protocols and their priority.

**`preferredauthentications publickey,keyboard-interactive,password`**

# ssh

Allows you to specify SSH client key parameters and generate an SSH client key pair.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > SSH Client Configuration

**configure > client ssh**

Entering the above command results in the following prompt:

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

**Syntax Description**

**ssh { generate key | key** *private_key_string* **length** *length_value* **} [ type v2-rsa ] [ key-size { 2048 | 3072 | 4096 | 5120 | 6144 | 7168 | 9216 } ]**
**no ssh key type v2-rsa**

**no ssh key**

Removes the specified SSH client key configuration. The only supported SSH client key type is V2-RSA.

**generate key [ type v2-rsa ]**

Generates SSH client key pairs based on parameters specified via the **ssh key** command. The only supported SSH client key type is V2-RSA.

**key *private_key_string* length *length_value* [ type v2-rsa ]**

Sets parameters for the SSH client keys.

- **key** *private_key_string* specifies a private key value as an alphanumeric string of 1 through 4499 characters.
- **length** *key_length* specifies the length of the key in bytes as an integer from 0 through 65535.
- **type v2-rsa** specifies the SSH client key type. The only supported SSH client key type is V2-RSA.

**key-size { 2048 | 3072 | 4096 | 5120 | 6144 | 7168 | 9216 }**

Specifies the key size for SSH client.

**Usage Guidelines**

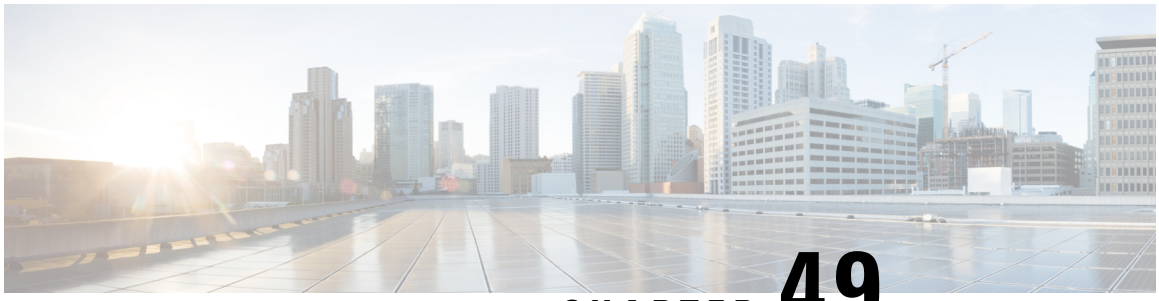
Use this command to specify SSH client private key values or generate an SSH client key pair. You can then push the public key to external servers via the Exec mode **push ssh-key** command. Pushing the key supports SSH access without a password between the StarOS gateway and external servers.

**Example**

The following command sequence specifies a private key and generates an SSH client key pair.

```
ssh key
AAAAB3NzaC1yc2EAAAADAQABAAABAQDn0X5xmZ1BrK2sEvzS+CRvD8mwOKHxb8Nwq64sunvjzcdc
length 512 type v2-rsa
```

```
ssh generate key type v2-rsa
```



CHAPTER 49

# Stats Profile Configuration Mode Commands

The Stats Profile Configuration Mode Commands allow operators to support the collection and viewing of QoS statistics on a Quality of Service Class Index (QCI) and Allocation and Retention Priority (ARP) basis.

Specifically, this mode enables operators to monitor QoS statistics that identify multiple services running with the same QCI value. In addition, packet drop counters provide the specific reason the Enhanced Charging Service (ECS) dropped a packet. The packet drop counters provide output on a per ARP basis. This provides additional information that operators can use to troubleshoot and identify network issues that may be affecting service.

**Command Modes**

Exec > Global Configuration > Stats-Profile

**configure > stats-profile >***stats_profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-stats-profile)#
```

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


- do show, on page 531
- end, on page 532
- exit, on page 532
- packet-drop, on page 532
- qci, on page 533
- rat-type, on page 534


# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character | is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# packet-drop

Enables the collection of detailed packet drop counters.



**Important** ARP Granularity for QCI Level Counters is a license-controlled feature. Per QCI Packet Drop Counters functionality does not require a license. Contact your Cisco account or support representative for licensing details.

**Product**

GGSN

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Stats-Profile

**configure > stats-profile >***stats_profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-stats-profile)#`

**Syntax Description**

**`[ no ] packet-drop`**

**no**

Disables the collection of packet drop statistics.

**packet-drop**

Enables the collection of packet drop statistics.

**Usage Guidelines**

Use this command to enable the collection of packet drop statistics.

**Example**

The following command enables the collection of packet drop statistics:

**`packet-drop`**

# qci

Enables the collection of QCI level statistics for a configured Stats Profile.

**Important** ARP Granularity for QCI Level Counters is a license-controlled feature. Per QCI Packet Drop Counters functionality does not require a license. Contact your Cisco account or support representative for licensing details.

**Product**

GGSN

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Stats-Profile

**configure** > **stats-profile** >*stats_profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-stats-profile)#
```

**Syntax Description**

```
[ no ] qci { all | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | [ non-std { non-gbr
 | gbr } ] } { arp { all | [ 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11
 |12 | 13 | 14 | 15 ] + } }
```

**no**

Disables the collection of the specified QCI level statistics.

**qci**

Enables the collection of QCI level statistics:

- **qci**: enables the collection of ARP priority level statistics for the specified QCIs. Valid entries are standard QCI values 1 through 9 or **all**.
- **non-std**: enables the collection of ARP priority level statistics for non-standard QCIs.
- **non-gbr**: enables the collection of ARP priority level statistics for non-standard non-guaranteed bit rate (GBR) QCIs.
- **gbr**: enables the collection of ARP priority level statistics for non-standard GBR QCIs.
- **arp**: enables the collection of ARP priority level statistics for the specified ARP values. Valid entries are from 1 to 15 or **all**.

**Usage Guidelines**

Use this command to enable the collection of QCI and ARP level statistics.

**Example**

The following command enables the collection of ARP priority level statistics for all QCI and ARP values:

```
qci all arp all
```

# rat-type

Configures collection of RAT level statistics.

**Product**

GGSN

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Stats-Profile

**configure** > **stats-profile** >*stats_profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-stats-profile)#`

## Syntax Description

**`[ no ] rat-type { [geran | utran | eutran]* }`**

### no

Disables statistics collection based on RAT type.

### rat-type

Configures collection of RAT level statistics.

### geran

Configures collection of statistics for RAT Type GERAN.

### utran

Configures collection of statistics for RAT Type UTRAN.

### eutran

Configures collection of statistics for RAT Type EUTRAN.

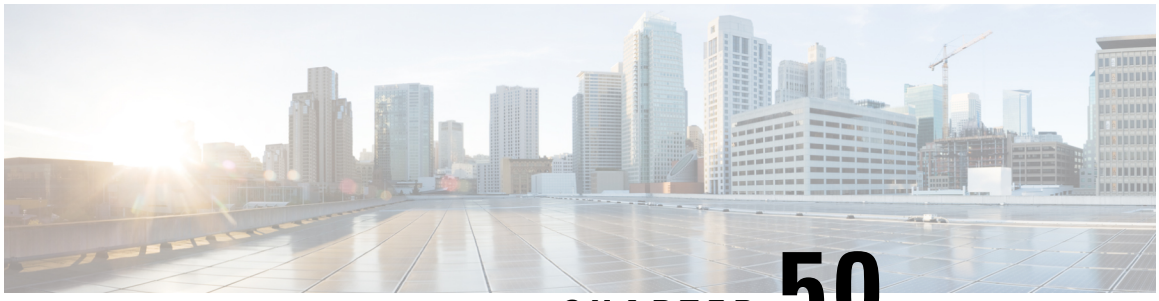
## Usage Guidelines

Use this command to configure collection of RAT level statistics.

### Example

The following command configures collection of statistics for RAT type GERAN:

**`rat-type geran`**



CHAPTER 50

# Subscriber Configuration Mode Commands

The Subscriber Configuration Mode is used to create local subscribers as well as to set default subscriber options for the current context.

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

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


- aaa, on page 540
- access-link ip-fragmentation, on page 542
- accounting-mode, on page 543
- active-charging bandwidth-policy, on page 544
- active-charging link-monitor tcp, on page 545
- active-charging radio-congestion, on page 546
- active-charging rulebase, on page 547
- always-on, on page 548
- asn-header-compression-rohc, on page 549
- asn nspid, on page 550
- asn-pdfid, on page 551
- asn-policy, on page 552
- associate accounting-policy, on page 554
- authorized-flow-profile-id, on page 555
- content-filtering category, on page 556
- credit-control-client, on page 557
- credit-control-group, on page 558
- credit-control-service, on page 559
- data-tunneling ignore df-bit, on page 560
- dcca peer-select, on page 560
- default, on page 561

- description, on page 564
- dhcp dhcpv6, on page 565
- dhcp options, on page 566
- dhcp parameter-request-list-option, on page 566
- dhcp service, on page 567
- dns, on page 568
- do show, on page 569
- eap, on page 569
- encrypted password, on page 571
- end, on page 571
- exit, on page 571
- external-inline-server, on page 572
- firewall policy, on page 572
- fw-and-nat policy, on page 573
- gtpp, on page 574
- idle-timeout-activity, on page 575
- ikev2 tsr, on page 576
- ims application-manager, on page 577
- ims-auth-service, on page 578
- inter-pdsn-handoff, on page 579
- ip access-group, on page 579
- ip address, on page 580
- ip address alloc-method, on page 581
- ip address pool, on page 583
- ip address secondary-pool, on page 584
- ip allowed-dscp, on page 585
- ip context-name, on page 588
- ip header-compression, on page 589
- ip hide-service-address, on page 591
- ip local-address, on page 592
- ip multicast discard, on page 593
- ip qos-dscp, on page 593
- ip route, on page 595
- ip source-validation, on page 596
- ip user-datagram-tos copy, on page 596
- ip vlan, on page 598
- ipv6 access-group, on page 599
- ipv6 address, on page 599
- ipv6 dns, on page 600
- ipv6 dns-proxy, on page 601
- ipv6 egress-address-filtering, on page 602
- ipv6 initial-router-advt, on page 603
- ipv6 interface-id, on page 604
- ipv6 minimum-link-mtu, on page 605
- ipv6 secondary-address, on page 606
- l2tp send accounting-correlation-info, on page 607

- l3-to-l2-tunnel address-policy, on page 608
- loadbalance-tunnel-peers, on page 609
- long-duration-action, on page 610
- max-pdn-connections, on page 611
- mediation-device, on page 612
- mobile-ip, on page 613
- mobile-ip ha, on page 616
- mobile-ip reg-lifetime-override, on page 617
- mobile-ip send access-technology, on page 618
- mobile-ip send accounting-correlation-info, on page 619
- mobile-ip send bsid, on page 620
- mobile-ip send pcf-address, on page 621
- mobile-ip send service-option, on page 622
- mobile-ip send subnet-id, on page 623
- mobile-ipv6, on page 623
- nai-construction-domain, on page 625
- nbns, on page 625
- nexthop-forwarding-address, on page 626
- npu qos, on page 627
- nw-reachability-server, on page 628
- outbound, on page 629
- overload-disconnect, on page 630
- password, on page 631
- pdif mobile-ip, on page 633
- permission, on page 634
- policy ipv6 tunnel, on page 634
- policy-group, on page 635
- ppp, on page 636
- prepaid 3gpp2, on page 639
- prepaid custom, on page 641
- prepaid unclassify, on page 642
- prepaid voice-push, on page 643
- prepaid wimax, on page 643
- proxy-dns intercept list-name, on page 643
- proxy-mip, on page 644
- qos apn-ambr, on page 645
- qos rate-limit, on page 646
- qos traffic-police, on page 653
- qos traffic-shape, on page 655
- radius accounting, on page 658
- radius group, on page 660
- radius returned-framed-ip-address, on page 661
- radius rulebase-format, on page 662
- rohc-profile-name, on page 664
- secondary ip pool, on page 664
- send-destination-pgw, on page 665

- service-option, on page 666
- simultaneous, on page 667
- timeout absolute, on page 668
- timeout idle, on page 668
- timeout long-duration, on page 670
- tpo policy, on page 671
- tunnel address-policy, on page 671
- tunnel gre, on page 672
- tunnel ipip, on page 673
- tunnel ipsec, on page 674
- tunnel l2tp, on page 675
- w-apn, on page 677


# aaa

Configures authentication, authorization and accounting (AAA) functionality at the subscriber level.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no ] aaa { accounting interim { interval-timeout interval_timeout | normal
 | suppress } | group aaa_group_name | secondary-group aaa_secondary_group_name
}
default aaa { accounting interim [ interval-timeout ] | group |
secondary-group }
no aaa { accounting interim [ interval-timeout ] | group [ aaa_group_name ]
 | secondary-group }
```

**default**

Configures the default setting for the specified parameter.

- **accounting**: Enables AAA accounting for subscribers.
- **group**: Uses the default AAA group—the one specified at the context level or in the default subscriber profile.
- **secondary-group**: Removes the secondary AAA group from the subscriber configuration.

**no**

- **accounting**: Disables AAA accounting for subscribers.

- **group**: Uses the default AAA group—the one specified at the context level or in the default subscriber profile.
- **secondary-group**: Removes the secondary AAA group from the subscriber configuration.

**accounting interim { interval-timeout *interval_timeout* | normal | suppress }**

Specifies when system should send an interim accounting record to the server.

- **interval-timeout**: Specifies the time interval (in seconds) at which to send an interim accounting record.

  *interval_timeout* must be an integer from 50 through 40000000.
- **normal**: If RADIUS accounting is enabled, send this Acct-Status-Type message when normally required by operation.
- **suppress**: If RADIUS accounting is enabled, suppress the sending of Acct-Status-Type message.

**group *aaa_group_name***

Specifies the AAA server group for the subscriber for authentication and/or accounting.

*aaa_group_name* must be an alphanumeric string of 1 through 63 characters.

**secondary-group *aaa_secondary_group_name***

Specifies the secondary AAA server group for the subscriber.

*aaa_secondary_group_name* must be an alphanumeric string of 1 through 63 characters.

## Usage Guidelines

Use this command to configure AAA functionality at the subscriber level.

Instead of having a single list of servers per context, this feature configures multiple server groups within a context and applies individual server group for subscribers in that context. Each server group consists of a list of AAA servers for each AAA function (accounting, authentication, charging, etc.).

The AAA secondary server group supports the No-ACK RADIUS Targets feature in conjunction with PDSN/HA for secondary accounting (with different RADIUS accounting group configuration) to the RADIUS servers without expecting the acknowledgement from the server, in addition to standard RADIUS accounting. This secondary accounting will be an exact copy of all the standard RADIUS accounting message (RADIUS Start/Interim/Stop) sent to the standard AAA RADIUS server.

If the same AAA group is configured with both the **aaa group** *aaa_group_name* and the **aaa secondary-group** *aaa_group_name* commands, then this configuration will have no effect and secondary accounting will not happen.

The AAA secondary server group configuration takes effect only when used with subscriber accounting-mode set to radius-diameter. The RADIUS accounting triggers for both standard RADIUS accounting and secondary accounting will be taken from the AAA group configured with the **aaa group** *aaa_group_name* command. On the fly change of this configuration is not supported. Any change to the configuration will have effect only for new calls.

### Example

The following command applies the AAA server group *star1* to subscribers:

```
aaa group star1
```

# access-link ip-fragmentation

Configures IP fragmentation processing over the Access-link.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**access-link ip-fragmentation { normal | df-ignore | df-fragment-and-icmp-notify }**

**df-ignore**

Default: Enabled

Ignores the DF (Don't Fragment) bit setting. Fragments and forwards the packet over the access link.

**df-fragment-and-icmp-notify**

Default: Disabled

Partially ignores the DF bit. Fragments and forwards the packet, but also returns an ICMP error message to the source of the packet. The number of ICMP errors sent like this is rate-limited to one ICMP error packet per second per session.

**normal**

Default: Disabled

Normal processing. Drops the packet and sends an ICMP unreachable message to the source of packet. This is the default behavior.

**Usage Guidelines**

If the IP packet to be forwarded is larger than the access-link MTU and if the DF (Don't Fragment) bit is set for the packet, then the fragmentation behavior configured by this command is applied. Use this command to fragment packets even if they are larger than the access-link MTU.

**Example**

Set fragmentation so that the DF bit is ignored and the packet is forwarded anyway by entering the following command:

```
access-link ip-fragmentation df-ignore
```

# accounting-mode

Sets the accounting mode for the current local subscriber configuration.

**Product**

PDSN

HA

ASN-GW

SAEGW

S-GW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
accounting-mode { flow-based | gtpp [ radius-diameter ] | none |
radius-diameter [ gtpp ] | rf-style }
default accounting-mode
```

**default**

Sets the type of accounting to be performed for the current local subscriber to the default setting.

Default: **radius-diameter**

**flow-based**

Diameter flow-based accounting is enabled for the current local subscriber.

**gtpp [ radius-diameter ]**

GTPP CDR RADIUS accounting is enabled for the current local subscriber. The **radius-diameter** keyword is available if both GTPP RADIUS and RADIUS-Diameter accounting are to be used.

**none**

Accounting is disabled for the current local subscriber and no charging records will be generated.

**radius-diameter [ gtpp ]**

RADIUS-Diameter accounting is enabled for the current local subscriber. The **gtpp** keyword is available if both GTPP RADIUS and RADIUS-Diameter accounting are to be used.

**rf-style**

Diameter Rf interface accounting is enabled for the current local subscriber.

**Usage Guidelines**

This command specifies which protocol, if any, will be used to provide accounting for PDP contexts accessing the APN profile.

Use this command to enable or disable RADIUS/Diameter accounting for any subscribers that use the current local subscriber configuration.

If the **gtpp** option is used, then GTPP RADIUS is used as configured in the Context Configuration mode or the AAA Server Group Configuration mode and GTPP charging records will be enabled.

If the **radius-diameter** option is used, either the RADIUS or the Diameter protocol is used as configured in the Context Configuration mode or the AAA Server Group Configuration mode.

RADIUS accounting can also be enabled and disabled at the context level with the **aaa accounting** command in the Context Configuration Mode. If RADIUS accounting is enabled at the context level, the accounting-mode command can be used to disable RADIUS accounting for individual local subscriber configurations.

If the accounting mode is set to **rf-style**, then BM will generate accounting records corresponding to AIMS RF.

#### Example

To disable accounting for the current subscriber, enter the following command:

```
accounting-mode none
```

# active-charging bandwidth-policy

Configures the bandwidth policy to be used for the subscriber.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**active-charging bandwidth-policy** *bandwidth_policy_name*
**{ default | no } active-charging bandwidth-policy**

#### default

Specifies that the default bandwidth policy configured in the rulebase be used for this subscriber.

#### no

Disables bandwidth control for this subscriber.

**active-charging bandwidth-policy *bandwidth_policy_name***

Specifies name of the bandwidth policy.

*bandwidth_policy_name* must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to configure bandwidth policy to be used for subscribers.

**Example**

The following command configures a bandwidth policy named *standard* for the subscriber:

```
active-charging bandwidth-policy standard
```

# active-charging link-monitor tcp

Enables the TCP link monitoring feature on the Mobile Video Gateway. This command can be configured in either APN Configuration Mode or Subscriber Configuration Mode.



**Important** In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

**Product**

MVG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ default | no ] active-charging link-monitor tcp [ log [ rtt [ histogram
 | time-series ] [ bitrate [ histogram | time-series ] ] | bitrate [
histogram | time-series ] [ rtt [ histogram | time-series ] ] ] ][
-noconfirm ]
```

**default**

Sets TCP link monitoring to its default value, which is the same as **[ no ]**.

**no**

Deletes the TCP link monitoring settings and disables TCP link monitoring if previously configured.

**active-charging link-monitor tcp**

Enables the TCP link monitoring feature on the Mobile Video Gateway. Note that TCP link monitoring is not enabled by default. Also note that when this command is configured without the **log** option, TCP link monitoring

is enabled without logging, and the output from TCP link monitoring is only used by the dynamic translating feature.

**log [ rtt [ histogram | time-series ] [ bitrate [ histogram | time-series ] ] | bitrate [ histogram | time-series ] [ rtt [ histogram | time-series ] ] ]**

This option enables statistical logging for TCP link monitoring.

The **rtt** option can be used to enable either **histogram** or **time-series** logging for round-trip time (RTT).

Similarly, the **bitrate** option can be used to enable either **histogram** or **time-series** logging for bit rate.

When **rtt** and **bitrate** options are used without additional options, histogram and time-series logging are enabled for round-trip time (RTT) and/or bit rate respectively.

**-noconfirm**

Specifies that the command must execute without prompting for confirmation.

**Usage Guidelines**

Use this command to enable TCP link monitoring on the Mobile Video Gateway.

**Examples**

The following command enables TCP link monitoring with statistical logging, with histogram and time-series logging enabled for both RTT and bit rate:

```
active-charging link-monitor tcp log
```

The following command enables TCP link monitoring with statistical logging, with histogram and time-series logging enabled for RTT:

```
active-charging link-monitor tcp log rtt
```

The following command enables TCP link monitoring with statistical logging, with histogram logging enabled for RTT:

```
active-charging link-monitor tcp log rtt histogram
```

The following command enables TCP link monitoring with statistical logging, with histogram logging enabled for RTT and time-series logging enabled for bit rate:

```
active-charging link-monitor tcp log rtt histogram bitrate time-series
```

# active-charging radio-congestion

Enables the Congestion Management feature on the Mobile Video Gateway. This command can be configured in either APN Configuration Mode or Subscriber Configuration Mode.

**Important** In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

**Product**

MVG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**active-charging radio-congestion policy** *policy_name*

**[ default | no ] active-charging radio-congestion policy**

**default**

Sets congestion management to its default value, which is the same as **[ no ]**.

Default: Disabled

**no**

Deletes the settings and disables congestion management if previously configured.

**active-charging radio-congestion policy *policy_name***

Enables the Congestion Management feature on the Mobile Video Gateway.

*policy_name* must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to enable or disable congestion management on the Mobile Video Gateway at either APN or subscriber. As congestion management makes use of the Link Monitoring feature, this must also be enabled along with the congestion monitoring feature.

**Example**

The following command enables radio congestion for a policy named *test123* for the subscriber:

**active-charging radio-congestion policy test123**

# active-charging rulebase

Specifies the rulebase to be used for this subscriber.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**active-charging rulebase** *rulebase_name*

**no active-charging rulebase**

**no**

Removes the previously configured rulebase for the subscriber.

**active-charging rulebase *rulebase_name***

Specifies name of the ACS rulebase.

*rulebase_name* must be the name of an ACS rulebase expressed as an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

This command specifies the name of the rulebase for specific subscriber (reals).

If the specified rulebase does not exist in the Active Charging service, the call will be rejected.

**Example**

The following command configures the ACS rulebase named *rule1* for the subscriber:

**active-charging rulebase rule1**

# always-on

Once the idle timeout limit is reached, keeps the current subscriber session connected as long as the subscriber is reachable.



**Caution** When always-on is enabled, the subscriber must have an idle time-out period configured (default is 0, no time-out). Failure to configure an idle time-out results in a subscriber session that is indefinite.

Two timers and a counter are associated with this feature. Refer to the **timeout** command in this chapter and the **ppp echo-retransmit-timeout msec** and **ppp echo-max-retransmissions num_retries** commands.

Default: Disabled.

**Product**

PDSN

ASN-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

*[context_name]host_name*(config-subscriber)#

**Syntax Description** `[ no ] always-on`

**always-on**

Specifies that the user will remain connected after the idle time expires.

**no**

Disables **always-on**. The user is disconnected after the idle time expires.

**Usage Guidelines** If this parameter is enabled for a subscriber, when the idle time-out limit is reached the subscribers IP/PPP session remains connected as long as the subscriber is reachable. This is true even if the airlink between the mobile device and the RN (Radio Node) is moved from active to dormant (inactive) status. When the idle timeout limit is reached, the PDSN determines availability using link control protocol (LCP) keepalive messages. A response to these messages indicates that the "always-on" status should be maintained. Failure to respond to a predetermined number of LCP keepalive messages causes the PDSN to tear-down (disconnect) the subscriber session.

**Example**

Enable always on for the current subscriber by entering the following command:

```
always-on
```

# asn-header-compression-rohc

Negotiates Robust Header Compression (ROHC) support for subscriber calls with AAA and WiMAX. This configuration indicates the type of header compression supported and enabled on the ASN.

**Product** ASN-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-subscriber)#`

**Syntax Description** `[ no | default ] asn-header-compression rohc`

**no**

Removes or disables the configured identifiers for ROHC in ASN-GW service.

**default**

The default is *disabled*.

**Usage Guidelines** Network Attached Storage (NAS) uses this configuration to indicate ROHC support of the subscriber TLV in the WiMAX-capability attribute within the Access Request. ROHC is applied only when ROHC is supported on the ASNGW and ROHC support is indicated by the AAA.

### Example

The following command enables ROHC:

```
asn-header-compression rohc
```

# asn nspid

Specifies the network service provider (NSP) associated with a WiMAX subscriber in an ASN-GW service. When configured, the NSP ID is sent in the Access-Request and Accounting messages.

**Product** ASN-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description** **[ no ] asn nspid** *nsp_id*

#### no

Removes or disables the configured identifiers for this network service provider in ASN-GW service.

#### asn nspid *nsp_id*

Specifies the network service provider for this subscriber. This enables the MS to discover all accessible NSPs, and to indicate the NSP selection during connectivity to the ASN.

**Usage Guidelines** Use this command to specify the NSP associated with a subscriber in an ASN-GW service.

*nsp_id* is three bytes in hexadecimal format. For example: FF-EE-01

### Example

The following command specifies the NSP for a subscriber in an ASN service:

```
asn nspid 0F-01-FE
```

# asn-pdfid

Configures the identifiers for packet data flow, service data flow, and service profile in an ASN-GW service.

**Product**

ASN-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] asn-pdfid** *pdf_id* **asn-service-profile-id** *svc_profile_id* **asn-sdfid** *sdf_id*

**no**

Removes/disables the configured identifiers for this subscriber in ASN-GW service.

**asn-pdfid *pdf_id***

Specifies the an unique ASN Packet Data Flow identifier for this subscriber.

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

**asn-service-profile-id *svc_profile_id***

Specifies a unique ASN Service Profile Identifier for this subscriber.

*svc_profile_id* is a Service Profile Identifier configured in the Context Configuration Mode.

**asn-sdfid *sdf_id***

Specifies the an unique ASN Service Data Flow identifier for this subscriber.

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

**Usage Guidelines**

Use this command to configure subscriber profile for QoS parameters in an ASN-GW service.

A maximum of four QoS profiles can be configured for a subscriber.

**Example**

The following command configures the QoS profile for a subscriber as PDF id 1, Service Profile id 3, and Service Data Flow id 2:

```
asn-pdfid 1 asn-service-profile-id 3 asn-sdfid 2
```

# asn-policy

Configures the identifiers for packet data flow, service data flow, and service profile in an ASN-GW service.

**Product**

ASN-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
asn-policy [classifiers downlink { strict | loose} | idle-mode { allow |
 disallow } | notification-idle-mode {allow | disallow} |
notification-handoff { allow | disallow }auth-only {allow | disallow } |
 ms-requested-classifiers {allow | dissalow}]
```

```
[ default ] asn-policy classifiers downlinkidle-mode
```

**no**

Removes or disables the configured policy for this subscriber in ASN-GW service.

**default**

Sets the ASN policy to default for this subscriber.

For downlink traffic classifier default policy is "loos" and for idle mode policy the default action is to allow idle mode operation in an ASN-GW service.

**idle-mode**

Sets the idle mode policy for this subscriber in an ASN-GW service. If enabled, Interim-Update is sent with the BSID and WiMAX-Idle_Mode Transition as Idle. If disabled, the Interim can be sent when the call is in the idle mode based on the interim timer. At this point, the last known BSID is reported to the RADIUS server.

**notification-idle-mode**

Default: allow

Use to enable or disable Idle-Mode-Notification capabilities. When you enable this command, when the call moves from active to idle, or idle to active, Accounting Interim is sent.

**notification-handoff**

Default: allow

If enabled, the Interim-Update is sent with the BSID and SN-Handoff-Indicator as Active Handoff.

**allow**

Default: enabled

Enables the policy for this subscriber to allow idle mode operation in an ASN-GW service.

**disallow**

Default: disabled

Enable the policy for this subscriber to disallow idle mode operation in an ASN-GW service.

**classifiers downlink**

Sets the classifier policy for all service flows coming from HA to FA for this subscriber's matching classifier.

**strict**

Default: disabled

This option discards all the service flows coming from HA to FA and any other packets not matching to any of the classifiers set for this subscriber.

**loose**

Default: enabled

This option allows all the service flows coming from HA to FA and any other packet does not matching to any of the classifiers set for this subscriber and sent to the BS/MS over downlink flow

**auth-only**

Specifies whether the call is Auth only or not.

**allow**

Enables the policy for this subscriber to allow auth-only in an ASN-GW service.

**disallow**

Default

Disables the policy for this subscriber to allow auth-only in an ASN-GW service.

**ms-requested classifiers**

Default: allow

By default ASNGW allows dynamic addition of classifiers by the MS during MS-initiated service flow creation or modification.

## Usage Guidelines

Use this command to configure subscriber policy to allow/disallow the idle mode operation or the downlink traffic flow for a subscriber in an ASN-GW service.

For authentication configuration, the ASN-GW supports the Initial Network Entry (INE) for Ethernet CS calls. The base station supports Ethernet CS traffic to the network. The INE procedure includes the

Authentication of the service flows and IP-Address allocation through DHCP. Authentication is based on the Extensible Authentication Protocol (EAP).

This command allows MS to transition to idle mode with an ASN-GW.

### Example

The following command configures the policy to allow the idle mode for an MS with an ASN-GW:

```
default asn-policy idle-mode
```

# associate accounting-policy

Associates the subscriber with specific pre-configured policies configured in the same context.

**Product**

P-GW

SAEGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] associate accounting-policy** *name*

#### no

Removes the selected association from this subscriber.

#### *name*

Associates the subscriber with an accounting policy configured in the same context.

*name* must be an existing accounting policy expressed as a string of 1 through 63 characters.

Accounting policies are configured through the **policy accounting** command in the Context Configuration mode.

**Usage Guidelines**

Use this command to associate the subscriber with an accounting policy configured in this context.

### Example

The following command associates this subscriber with an accounting policy called *acct1*:

```
associate accounting-policy acct1
```

# authorized-flow-profile-id

When a profile ID is requested by the Mobile Node (MN), this command sets the value that is authorized by the Access Gateway (AGW).

**Product**

PDSN

ASN-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**authorized-flow-profile-id** *profile_id* **direction { bidirectional | forward | reverse }**

**no authorized-flow-profile-id** *profile_id*

#### no

Removes the existing profile ID setting specified by *profile_id*. *profile_id* must be an integer from 0 through 65535.

#### authorized-flow-profile-id *profile_id*

The profile ID number that is authorized for the current subscriber. *profile_id* must be an integer from 0 through 65535.

#### direction { bidirectional | forward | reverse }

This specifies in which data direction the profile ID should be applied.

- **bidirectional**: This profile ID pertains to both the forward and reverse directions.
- **forward**: This profile ID pertains to data going to the MN.
- **reverse**: This profile ID pertains to data coming from the MN.

**Usage Guidelines**

Use this command to set the profile ID that the AGW will authorize for a subscriber.

#### Example

Set the profile ID for both directions to 3 for the current subscriber by entering the following command:

```
authorized-flow-profile-id 3 direction bidirectional
```

# content-filtering category

Enables or disables the specified preconfigured Category Policy Identifier for policy-based Content Filtering support to the subscriber.

**Product**

CF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**content-filtering category policy-id** *cf_policy_id*

**no content-filtering category policy-id**

**no**

Disables the configured category policy ID for content filtering support to the subscriber. This is the default setting.

**content-filtering category policy-id *cf_policy_id***

Applies the content filtering category policy ID, configured in ACS Configuration Mode, to this subscriber.

*cf_policy_id* must be a category policy ID expressed as an integer from 1 through 4294967295.

If the specified category policy ID is not configured in the ACS Configuration Mode, all packets will be passed regardless of the categories determined for such packets.

**Important** Category Policy ID configured through this mode overrides the Category Policy ID configured using the **content-filtering category policy-id** command in the ACS Rulebase Configuration Mode.

**Usage Guidelines**

Use this command to enter the Content Filtering Policy Configuration Mode and enable or disable the Content Filtering Category Policy ID for a subscriber.

**Important** If Content Filtering Category Policy ID is not specified here, the similar command in the ACS Rulebase Configuration Mode determines the policy.

Up to 64 different policy identifier can be defined in a Content Filtering support service.

### Example

The following command enters the Content filtering Policy Configuration Mode and enables the Category Policy ID *101* for Content Filtering support:

```
content-filtering category policy-id 101
```

# credit-control-client

Configures the credit-control client parameters for the subscriber.

**Product**

GGSN

HA

IPSG

PDSN

P-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**credit-control-client { event-based-charging | override session-mode { per-sub-session | per-subscriber } }**

**no credit-control-client { event-based-charging | override session-mode }**

**default credit-control-client event-based-charging**

#### no

Disables the configured setting.

#### default

Resets the command to its default setting of disabled.

#### event-based-charging

Enables event-based charging.

#### override session-mode { per-sub-session | per-subscriber }

Overrides the session-mode configured through the CLI command "**require ecs credit-control session-mode per-subscriber**" in Global Configuration mode so that different subscriber groups can operate in different

modes. For example, one subscriber group can be configured to work in per-subscriber mode, while another in per-sub-session mode.

This keyword is used to switch between subscriber level Gy and sub-session level Gy.



**Important** This CLI can be changed on the fly. The modified values will be reflected only in the new subscriber session.

The **no** command removes the override CLI and makes the subscriber group fall back to the configuration specified through the CLI command "**require ecs credit-control session-mode per-subscriber**".

**Usage Guidelines** Use this command to configure the credit-control client parameters for the subscriber.

This configuration should be enabled to report UE's PLMN, timezone and ULI changes through Event-based-Gy session. In the event that both Gy Online charging and Gy event reporting are enabled, the P-GW shall send only CCR-Update requests to the OCS and shall not send CCR-Event requests.

With the inclusion of this keyword **override session-mode ...** in 14.1 release, it is possible to seamlessly change the configuration from bearer level to subscriber level and vice-versa without requiring a system reboot.

### Example

The following command enables event-based Gy support for the subscriber:

```
credit-control-client event-based-charging
```

# credit-control-group

Configures the credit-control group for this subscriber.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
credit-control-group cc_group_name
no credit-control-group
```

### no

Removes the credit-control group from the subscriber configuration, if configured.

**credit-control-group *cc_group_name***

Specifies name of the credit-control group.

*cc_group_name* must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to configure the credit-control group for the subscriber.

**Example**

The following command configures the credit-control group named *test12* for the subscriber:

```
credit-control-group test12
```

# credit-control-service

Configures the credit-control service for this subscriber.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] credit-control-service** *cc_service_name*

**no**

Disables the credit-control service, if configured.

**credit-control-service *cc_service_name***

Specifies the name of the credit-control service.

*cc_service_name* must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to configure the credit-control service for subscribers.

**Example**

The following command configures the credit-control service named *test12* for the subscriber:

```
credit-control-service test12
```

# data-tunneling ignore df-bit

Controls the handling of the DF (Don't Fragment) bit present in the user IPv4/IPv6 packet for GRE, IP-in-IP tunneling used for the MIP data path. If this feature is enabled, and fragmentation is required for the tunneled user IPv4/IPv6 packet, then the DF bit is ignored and the packet is fragmented. Also the DF bit is not copied to the outer header. Default is enabled.

**Product**

PDSN

HA

FA

ASN-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] data-tunneling ignore df-bit**

**no**

Disables this option. The DF bit in the tunneled IP packet header is not ignored during tunneling.

**data-tunneling ignore df-bit**

Ignores the DF bit in the tunneled IP packet header.

**Usage Guidelines**

Use this command to configure a user so that during Mobile IP tunneling the DF bit is not ignored and packets are not fragmented.

**Example**

To disable fragmentation of a subscribers packets over a MIP tunnel even when the DF bit is present, enter the following command:

```
no data-tunneling ignore df-bit
```

# dcca peer-select

Specifies the Diameter credit control primary and secondary peer for credit control.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**dcca peer-select peer** *host_name* **[ realm** *realm_name* **] [ secondary-peer** *host_name* **[ realm** *realm_name* **] ]**

**no dcca peer-select**

**no**

Removes the previously configured Diameter credit control peer selection.

**peer *host_name***

Specifies a unique name for the peer. *peer_name* must be an alphanumeric string of 1 through 63 characters that allows punctuation marks.

**secondary-peer *host_name***

Specifies a back-up host that is used for fail-over processing. When the route-table does not find an available route, the secondary host performs a fail-over processing. *host_name* must be an alphanumeric string of 1 through 63 characters that allows punctuation marks.

**realm *realm_name***

The *realm_name* must be an alphanumeric string of 1 through 63 characters that allows punctuation marks. The realm may typically be a company or service name.

**Usage Guidelines**

Use this command to select a Diameter credit control peer and realm.



**Caution** This configuration completely overrides all instances of **diameter peer-select** that have been configured with in the Credit Control Configuration Mode for an Active Charging service.

**Example**

The following command selects a Diameter credit control peer named *test* and a realm of *companyx*:

**dcca peer-select peer test realm companyx**

# default

Restores the default value for the option specified for the current subscriber.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
default { access-link ip-fragmentation | accounting-mode | data-tunneling
 ignore df-bit | idle-timeout-activity dormant-downlink-data |
inter-pdsn-handoff | ip { alloc-method | allowed-dscp | header-compression
 | hide-service-address | multicast discard | qos-dscp | source-validation
 } | loadbalanace-tunnel-peers | long-duration-action | mobile-ip {
home-agent | mn-aaa-removal-indication | mn-ha-hash-algorithm |
reverse-tunnel | security-level | send { dns-address |
terminal-verification } } | permission | ppp { always-on-vse-packet |
data-compression { mode | protocols } | keepalive | min-compression-size
 | mtu } | radius accounting interim interval-timeout | timeout { absolute
 | idle } }
```

#### access-link ip-fragmentation

Sets the method for fragmenting packets over the MN access link to its default of normal. Drop the packet and send ICMP unreachable to the source of packet.

#### accounting-mode

Enables Radius accounting for the current local subscriber configuration.

#### data-tunneling ignore df-bit

Sets this option to the default behavior, which is to send an *ICMP unreachable - need to frag* message back to the sender and drop the packet, in the case that fragmentation is required but the DF bit is set.

#### idle-timeout-activity dormant-downlink-data

Sets this option to the default behavior. When downlink data packets are transmitted to the Mobile node and the session is in dormant mode the session idle timer is reset.

#### inter-pdsn-handoff

During a handoff from one PDSN to another, if the Mobile requests an IP address of 0.0.0.0 or a mismatched IP address the PDSN will not disconnect the session immediately. The PDSN tries to assign the proposed address of the session in the IPCP configuration NAK.

#### ip { alloc-method | allowed-dscp | dhcp-relay | header-compression | hide-service-address | multicast discard | qos-dscp | source-validation | user-datagram-tos copy }

**allowed-dscp**: resets the allowed DSCP parameters to the system defaults: class none, max-class be.

**hide-service-address**: specifies the default setting for hide the ip-address of the service from the subscriber. Default is Disabled

**dhcp-relay**: Configured with the DHCP server address during MS authentication. The AAA server sends the address of the DHCP server in the Access-Accept message. The DHCP relay uses this address to relay the DHCP messages from the MS to the DHCP server.

**multicast discard**: Configures the default multicast settings which is to discard PDUs

**qos-dscp**: Sets the quality of service setting to the system default.

**source-validation**: Specifies the default IP source validation. Default is Enabled.

**user-datagram-tos copy**: Disables copying of the IP TOS octet value to all tunnel encapsulation IP headers.

### loadbalance-tunnel-peers

Sets the tunnel load balancing algorithm to the system default.

### long-duration-action

Sets the action that is taken when the long duration timer expires to the default: detection.

### mobile-ip { home-agent | mn-aaa-removal-indication | mn-ha-hash-algorithm | reverse-tunnel | security-level | send { dns-address | terminal-verification } }

**allow-aaa-address-assignment**: Disables the FA from accepting a home address assigned by an AAA server.

**home-agent**: Sets home agent IP address to its default of 0.0.0.0.

**match-aaa-assigned-address**: Disables the FA validating the home address in the RRQ against the one assigned by AAA server.

**mn-aaa-removal-indication**: Sets this parameter to its default of disabled.

**mn-ha-hash-algorithm**: Sets the encryption algorithm to the default of hmac-md5.

**reverse-tunnel**: Sets this parameter to its default of enabled.

**security-level**: Sets this parameter to its default of none.

**send dns-address**: Disables the HA from sending the DNS address NVSE in the RRP.

**send terminal-verification**: Disables the FA from sending the terminal verification NVSE in the RRQ.

### permission

Restores the subscriber's service usage defaults.

### ppp { always-on-vse-packet | data-compression { mode | protocols } | ip-header-compression negotiation | keepalive | min-compression-size | mtu }

Sets the point-to-point protocol option defaults.

**always-on-vse-packet**: Re-enables the PDSN to send special 3GPP2 VSE PPP packets to the Mobile Node with a max inactivity timer value for always on sessions. This configuration is applicable only for PDSN or PDSNCLOSED-RP sessions.

**data-compression** { **mode** | **protocols** }: restores the default value for either the data compression **mode** or compression **protocols** as follows:

- mode stateless
- all protocols enabled

**ip-header-compression negotiation**: Sets the IP header compressions negotiation to the system default: force.

**keepalive**: sets the subscriber's PPP keep alive option to the system default: 30 seconds.

**min-compression-size**: Restores the PPP minimum packet size for compression: 128 octets.

**mtu**: Sets the maximum message transfer unit packet size to the system default: 1500 octets.

#### radius accounting interim interval-timeout

Disables the RADIUS accounting interim interval for the current subscriber.

#### timeout [ absolute | idle | long-duration ]

When a keyword is entered, this command resets the specified timeout to the system default: 0. When no keyword is specified, all timeouts are reset to the system defaults: 0.

**Usage Guidelines**

Use this keyword to reset subscriber data to the system defaults. This is useful in setting the subscriber back to the basic values to possibly aid in trouble shooting or tuning a subscriber's access and options.

#### Example

The following CLI commands restore default values for various options:

```
default ip qos-dscp
default permission
default data-compression mode
```

# description

Allows you to enter descriptive text for this configuration.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
description text
no description
```

#### no

Clears the description for this configuration.

#### *text*

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

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

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

#### Example

The following command enters the text description: *EO134 Anaheim*.

```
description "EO134 Anaheim"
```

# dhcp dhcpv6

Specifies the DHCPv6 service to be used for this subscriber.

**Product**

GGSN

P-GW

SAEGW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**dhcp dhcpv6 service-name** *service_name*

**no dhcp dhcpv6 service-name**

#### no

Removes the DHCPv6 service for the subscriber.

#### dhcpv6 service-name *service_name*

Specifies the name of an existing DHCPv6 service to be used for this subscriber.

*service_name* must be the name of a DHCPv6 service expressed as an alphanumeric string of 1 through 63 characters.

**Usage Guidelines** Use this command to apply or remove an existing DHCPv6 service to a subscriber template.

#### Example

The following command applies a previously configured DHCPv6 service named *dhcpv6_1* to a subscriber template:

```
dhcp dhcpv6 service-name dhcpv6_1
```

# dhcp options

Specifies the DHCP options which can be sent from the DHCP server for this subscriber.

**Product**

GGSN

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**dhcp options code 43 hex-values** *hex_values*

**no dhcp options**

**no**

Removes the DHCP options for the subscriber.

**options code 43 hex-values *hex_values***

Specifies hex values for DHCP option 43.

*hex_values* must be a dash-delimited list of hex data of size smaller than 506 datum.

**Usage Guidelines**

Use this command to specify the DHCP options which can be sent from the DHCP server for this subscriber.

**Example**

The following command applies hex values *ff-fe* for DHCP option 43:

**dhcp options code 43 hex-values ff-fe**

# dhcp parameter-request-list-option

Enables the sending of DHCP parameter request list option(s) in all outgoing messages for this subscriber.

**Product**

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**`[ no ] dhcp parameter-request-list-option [ options ]`**

**no**

Disables the sending of DHCP parameter request list option(s) in all outgoing messages.

***options***

Specifies the value of particular DHCP parameter request list option(s).

*options* must be an integer from 1 through 254.



**Important** Multiple options may be selected in the same command.

**Usage Guidelines**

Use this command to enable or disable the sending of DHCP parameter request list option(s) in all outgoing messages for this subscriber.

**Example**

The following command enables DHCP parameter request list option inclusion in outgoing messages:

**`dhcp parameter-request-list-option`**

# dhcp service



**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Enables DHCP service configuration accessible to the Se-GW context for subscriber. The specified DHCP service will be used for performing DHCP procedures between HNB-GW and HMS.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**dhcp service** *dhcp_svc_name* **context** *ctxt_name*
**no dhcp service**

**no**

Removes the specified DHCP service from the subscriber template configuration.

***dhcp_svc_name***

Specifies name of the DHCP service configured in Context configuration mode for DHCP proxy support on HNB-GW.

*dhcp_svc_name* must be an alphanumeric string of 1 through 63 characters preconfigured within the same context of this subscriber.

**context *ctxt_name***

Specifies the name of the context where DHCP service is configured for HNB-GW subscribers. *ctxt_name* must be an alphanumeric string of 1 trough 79 characters.

**Usage Guidelines**

This command associates the subscriber template with pre-configured DHCP service configuration to provide accessibility to Se-GW with HNB-GW.

**Example**

Following command applies a previously configured DHCP service named *dhcp_hnb1* to a subscriber template within the context named *femto_hnb*.

```
dhcp service dhcp_hnb1 context femto_hnb
```

# dns

Configures the domain name servers for the current subscriber.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] dns { primary | secondary }** *ip_address*

**no**

Indicates the IP address is to be removed as either a primary or secondary domain name server.

**dns primary | secondary**

**dns primary**: Updates the primary domain name server for the subscriber.

**dns secondary**: Updates the secondary domain name server for the subscriber.

***ip_address***

Specifies the IP address of the domain name server using IPv4 dotted-decimal notation.

**Usage Guidelines** Set the subscriber DNS server lists as not all users will have the same set of servers.

**Example**

The following commands enable primary and secondary DNS servers for the subscriber:

```
dns primary 10.2.3.4
dns secondary 10.2.5.6
```

# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# eap

Specifies the lifetime for a primary session key (PSK) for extensible authentication protocol (EAP) authentication.

**Product** ASN-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

In releases prior to StarOS 21.26:

**[ default ] eap msk-lifetime** *dur*

From StarOS 21.26 and later releases:

**[ default ] eap psk-lifetime** *dur*

**psk-lifetime *dur***

Specifies the lifetime duration (in seconds) on Primary Session Key (PSK) in seconds for a WiMAX subscriber EAP authentication.

*dur* is an integer from 60 through 65535.

**psk-lifetime *dur***

Specifies the lifetime duration (in seconds) on Primary Session Key (PSK) in seconds for a WiMAX subscriber EAP authentication.

*dur* is an integer from 60 through 65535.

**Usage Guidelines**

In releases prior to StarOS 21.26:

This command is used to set the lifetime for MSK in EAP authentication for WiMAX subscriber.

**Example**

The following command sets the lifetime for MSK key to *4800* seconds for a WiMAX subscriber through EAP authentication:

**eap msk-lifetime 4800**

From StarOS 21.26 and later releases:

**Usage Guidelines**

This command is used to set the lifetime for PSK in EAP authentication for WiMAX subscriber.

**Example**

The following command sets the lifetime for PSK key to *4800* seconds for a WiMAX subscriber through EAP authentication:

**eap psk-lifetime 4800**

# encrypted password

Designates use of password encryption.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description** **`encrypted password`** *`password`*

**encrypted password *password***

*password* is the encrypted password and must be an alphanumeric string of 1 through 132 characters.

**Usage Guidelines** This command is normally used only inside configuration files.

**Example**

The following command sets an encrypted password of *qsdf12d4*:

**`encrypted password qsdf12d4`**

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`end`**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `exit`

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

# external-inline-server

This is a restricted command.

# firewall policy



**Important** This command is only available in StarOS 8.0. In StarOS 8.1 and later releases, this configuration is available in the ACS Rulebase Configuration Mode.

Enables or disables Stateful Firewall support for the subscriber.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**`firewall policy firewall-required`**

**`{ default | no } firewall policy`**

**no**

Disables Stateful Firewall support for this subscriber.

**default**

Configures the default setting for Stateful Firewall support.

Default: Disabled

**firewall-required**

Enables Stateful Firewall support for this subscriber.

**Usage Guidelines** Use this command to enable or disable Stateful Firewall support for this subscriber.

**Important** Unless Stateful Firewall support for this subscriber is enabled using this command, firewall processing for this subscriber is disabled.

**Important** If firewall is enabled, and the rulebase has no firewall configuration, Stateful Firewall will cause all packets to be discarded.

### Example

The following command enables Stateful Firewall support for this subscriber:

```
firewall policy firewall-required
```

The following command disables Stateful Firewall support for this subscriber:

```
no firewall policy
```

# fw-and-nat policy

**Important** This command is only available in StarOS 8.1. This customer-specific command must be used to configure the Policy-based Firewall-and-NAT feature.

**Product**

PSF

NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**fw-and-nat policy** *fw_nat_policy*

**{ default | no } fw-and-nat policy**

#### default

Specifies that the default Firewall-and-NAT policy configured in the rulebase be used for the subscriber.

#### no

Disables Firewall and NAT processing for the subscriber.

***fw_nat_policy***

Specifies the Firewall-and-NAT policy for the subscriber.

*fw_nat_policy* must be an alphanumeric string of 1 through 63 characters. Note that this policy will override the **default Firewall-and-NAT policy** configured in the ACS rulebase.

**Usage Guidelines**

Use this command to configure the Firewall-and-NAT policy for subscribers. Note that the policy configured in the subscriber mode will override the default policy configured in the ACS rulebase. If a policy is not configured in the subscriber mode, the default policy configured in the ACS rulebase will be applied.

**Example**

The following command configures a Firewall-and-NAT policy named *standard* for the subscriber:

```
fw-and-nat policy standard
```

# gtpp

Configures GTP-P related parameters for a subscriber.

**Product**

IPSG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ default | no ] gtpp { group | secondary-group }** *group_name* **[ accounting-context** *context_name* **]**

**default**

Resets the GTTP group name to the default group.

**no**

Deletes the specified group name.

**group**

Specifies primary group parameters.

**secondary-group**

Specifies secondary group parameters.

***group_name***

Specifies the name of the GTP-P group as an alphanumeric string of 1 through 63 characters.

**accounting-context *context_name***

Specifies the GTPP accounting context as an alphanumeric string of 1 through 79 characters. Default is the GGSN service context.

**Usage Guidelines**

Use this command to enable or disable the generation of eG-CDRs for CDMA traffic observed in the customer network during IPSG deployment.

**Example**

The following command establishes the primary GTPP group *gtpp22*:

```
gtpp group gtpp22
```

# idle-timeout-activity

Defines whether downlink (towards Mobile Node) data packets transmitted when the session is dormant are treated as activity for the idle-timer (inactivity timer).

By default, downlink data transmitted over a dormant session restarts the idle-timer for that session; it is treated as activity for the session.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no ] idle-timeout-activity dormant-downlink-data
```

**no**

Dormant mode downlink data is not treated as activity for the session idle-timer. The session idle timer is not reset.

**idle-timeout-activity dormant-downlink-data**

Treats dormant mode downlink data as activity for the session idle-timer. The session idle timer is reset.

**Usage Guidelines**

Use this command to disable or re-enable restarting the session idle timer when downlink data packets are transmitted to the Mobile Node when the session is in dormant mode.

### Example

Use the following command to disable restarting the session idle timer when downlink data packets are transmitted to the Mobile Node when the session is in dormant mode:

```
no idle-timeout-activity dormant-downlink-data
```

Use the following command to re-enable restarting the session idle timer when downlink data packets are transmitted to the Mobile Node when the session is in dormant mode:

```
idle-timeout-activity dormant-downlink-data
```

# ikev2 tsr

Configures the Traffic Selector responder (TSr) negotiation behavior during IKEv2 Security Association (SA) establishment.

**Product**

PDG/TTG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ default ] ikev2 tsr { wildcard | user-specified }**

#### default

Specifies the default behavior, which is wildcard TSr negotiation.

#### ikev2 tsr

Enables TSr negotiation.

#### wildcard

Specifies that during TSr negotiation, the PDG/TTG always returns an any-to-any IP address range, an any-to-any port range, and allows any protocol, irrespective of the traffic selector ranges received from the UE. This is the default behavior.

#### user-specified

Specifies that during TSr negotiation, the PDG/TTG responds to each UE request with the UE-specified IP address ranges. This enables split tunneling on the PDG/TTG, and enables the UE to tunnel only a specified traffic range to the PDG/TTG and send other traffic directly out the WLAN.

**Usage Guidelines**

Use this command to specify the TSr negotiation behavior on the PDG/TTG.

### Example

The following command enables user-specified TSr negotiation on the PDG/TTG:

```
ikev2 tsr user-specified
```

# ims application-manager

Specifies the IP Multimedia Subsystem (IMS) application manager for the subscriber.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] ims application-manager { domain-name** *domain-name* **| ipv4-address** *ipv4_address* **}**

#### no

Disables the IMS application manager for this subscriber.

#### ims application-manager

Enables the IMS application manager for this subscriber.

#### domain-name *domain-name*

Specifies the domain name of the application manager.

*domain-name* must be an alphanumeric string of 1 through 63 characters.

#### ipv4-address *ipv4_address*

Specifies the IP address of the application manager using IPv4 dotted-decimal notation.

**Usage Guidelines**

The IMS application manager address is returned by HA to MN in DHCP Ack when it receives the DHCP inform from an AIMS subscriber.

### Example

The following commands specify IMS application managers by domain name and IPv4 address:

```
ims application-manager domain-name domain23
ims application-manager ipv4-address 209.165.200.225
```

# ims-auth-service

Enables IP Multimedia Subsystem (IMS) authorization support for subscriber. The specified IMSA service will be used for performing IMS authorization and flow-based charging procedures.

**Product**

PDSN

GGSN

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ default | no ] ims-auth-service** *auth_svc_name*

**default**

Configures default setting.

Default: Disabled or as specified at the context or network access service level or in subscriber template.

**no**

Removes the specified IMS authorization service from the subscriber configuration.

**ims-auth-service *auth_svc_name***

Specifies name of the IMS authorization service.

*auth_svc_name* must be an alphanumeric string of 1 through 63 characters preconfigured within the same context of this subscriber.

**Usage Guidelines**

This feature provides the IMS authorization service configuration for Gx interface in IMS service node.

**Example**

The following command applies a previously configured IMS authorization service named *ims_interface1* to a subscriber within the specific context.

```
ims-auth-service ims_interface1
```

# inter-pdsn-handoff

Configure the system to force the MN to use its assigned IP address during Internet Protocol Control Protocol (IPCP) negotiations resulting from inter-PDSN handoffs.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**`[ no ] inter-pdsn-handoff require ip-address`**

**no**

Disables the rejecting of sessions when the MN uses a non-allocated IP address during IPCP re-negotiations.

**inter-pdsn-handoff require ip-address**

Rejects sessions when the MN uses a non-allocated IP address during IPCP re-negotiations.

**Usage Guidelines**

This command is used to configure the system to reject sessions that are re-negotiating IPCP after an inter-PDSN handoff if the IP address they propose does not match the one initially provided by the PDSN. The session would be rejected even if the proposed address was 0.0.0.0.

If this parameter is disabled, the PDSN will attempt to re-assign the IP address initially provided.

**Example**

To set the PDSN to not allow a mismatched IP address during a PDSN to PDSN handoff of a MIP call, use the following command:

**`inter-pdsn-handoff require ip-address`**

To set the PDSN so that it will not disconnect the session immediately, if the Mobile requests an IP address of 0.0.0.0 or a mismatched IP address after inter-pdsn handoff, use the following command:

**`no inter-pdsn-handoff require ip-address`**

# ip access-group

Configures IP access group for the current subscriber.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] ip access-group** *group_name* **[ in | out ]**

**no**

Indicates the access group specified is to be cleared from the subscribers configuration.

**ip access-group *group_name***

Specifies the name of the IPv4/IPv6 access group. *acl_group_name* is a configured ACL group expressed as an alphanumeric string of 1 through 79 characters.

**in | out**

Default: both (in and out)

Specifies the access-group as either inbound or outbound by the keywords **in** and **out**, respectively. If neither of these key words is specified, the command associates the *group_name* access group with the current subscriber for both inbound and outbound access.

**Usage Guidelines**

Set the subscriber access group to manage the access control for subscribers as a logical group.

**Example**

The following command associates the *sampleGroup* access group with the current subscriber for both inbound and outbound access:

```
ip access-group sampleGroup
```

The following removes the outbound access group flag for *sampleGroup*:

```
no ip access-group sampleGroup out
```

# ip address

Configures a static IPv4 address for use by the subscriber.

**Product**

PDSN

GGSN

HA

ASN-GW

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**`[ no ] ip address`** *`ip_address netmask`*

**no**

Removes a previously configured IP address assignment.

**ip address *ip_address***

Specifies the IP address assigned to the subscriber using IPv4 dotted-decimal notation.

***netmask***

The subnet mask that corresponds to the assigned IPv4 address.

**Usage Guidelines**

Use this command to assign a static IPv4 address to the subscriber. This address will be used each time the subscriber establishes data sessions.

**Example**

The following command configures a static IP address of *192.168.1.15* with a subnet mask of *255.255.255.224* to the subscriber:

```
ip address 192.168.1.15 255.255.255.224
```

# ip address alloc-method

Configures the IP address allocation method for the current subscriber.

**Product**

PDSN

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

## Syntax Description

```
ip address allocation-method { dhcp-client | dhcp-relay | local |
no-dynamic } [ allow-user-specified ]
```

### dhcp-client

Default: Disabled

Configures the APN to assign an IP address received from a DHCP server.

**Important** If this option is used, the system's DHCP parameters must be configured.

### dhcp-relay

Default: Disabled

Configures the APN to forward DHCP packets received from the MS to a DHCP server.

**Important** If this option is used, the system's DHCP parameters must be configured.

### local

Default: Enabled

Configures the subscriber to dynamically receive IP addresses from a pool configured in the destination context on the system.

**Important** If this option is used, the name of the IP address pool from which to allocate addresses must be configured using the **ip address pool** command. If no pool name is specified, the system will attempt to allocate an address from any public pool configured in the destination context.

### no-dynamic

Default: Disabled

Disables the dynamic assignment of IP addresses to sessions for this subscriber.

If a a session is received for this subscriber with this option enabled, it will be rejected with a cause code of 129, Registration Denied - administratively prohibited (for PDSN), 220, Unknown PDP address or PDP type (for GGSN).

### allow-user-specified

Default: Enabled

Enables support for sessions requesting the use of specific (static) addresses.

**Important** If this option is not enabled, sessions requesting the use of a static address will be rejected with a cause code of 129, Registration Denied - administratively prohibited (for PDSN), 220 (Unknown PDP address or PDP type).

**Usage Guidelines** Use this parameter to dictate how dynamic IP addressing is to be handled for the subscriber when a static address is not provided.

**Important** When used in conjunction with the GGSN product, the settings for this command override those for the APN being accessed by the subscriber.

### Example

The following command dictates that the subscriber is to receive a dynamically assigned address with the system configured as a DHCP client:

```
ip address alloc-method dhcp-client
```

# ip address pool

Configures IP address pool properties for the subscriber.

**Product**

PDSN

GGSN

HA

ASN-GW

P-GW

SAEGW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] ip address pool name** *pool_name*

**no**

Removes a previously configured static address.

**ip address pool name *pool_name***

Specifies the IP address pool or IP address pool group from which the subscribers IP address is assigned.

*pool_name* must be the name of an existing IP pool or IP pool group expressed as an alphanumeric string of 1 through 31 characters.

**Usage Guidelines**

Use this command to specify the name of an IP address pool configured on the system from which IP addresses are to be dynamically assigned to sessions from this subscriber.

This command can be issued multiple times to specify multiple address pools for the subscriber. If multiple pools are specified, addresses are assigned for subscriber sessions from the pools based on the order in which the pools were configured.

If an address cannot be provided from the first-specified pool for whatever reason, the system attempts to assign an address from the second-specified pool, and so on. This operation is independent of the priorities configured for the pools. For example, if pool1 was specified for the subscriber first, and pool2 second, the system always attempts to assign addresses from pool1. If an address can not be assigned from pool1 (i.e. all addresses are in use), the system then attempts to assign an address from pool2.

**Example**

The following command configures the subscriber to receive IP addresses from an IP address pool named *public1*:

```
ip address pool name public1
```

# ip address secondary-pool

Configures secondary IP address pool properties for the subscriber to provide multiple IP host configuration behind one WiMAX Customer Premise Equipment (CPE).

**Product**

ASN-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] ip address secondary-pool name** *aux_pool_name*

**no**

Removes a previously configured auxiliary pool named *aux_pool_name* for multiple host support in ASN-GW service.

#### ip address secondary-pool name *aux_pool_name*

Specifies the secondary/auxiliary IP address pool or IP address pool group from which the IP address is assigned to host behind a WiMAX CPE having primary IP address.

*pool_name* must be the name of an existing IP pool or IP pool group expressed as an alphanumeric string of 1 through 31 characters.

**Usage Guidelines**

Use this command to specify the name of an IP address pool configured on the system from which IP addresses are to be dynamically assigned to host behind a WiMAX CPE for multiple host session support.

This command designates the IP address to secondary hosts from locally configured secondary IP address pool. To enable multiple host support behind a WiMAX CPE and configure maximum number of supported hosts use **secondary-ip-host** command in ASN Gateway Service Configuration mode.

#### Example

The following command configures the subscriber to receive IP addresses from a secondary IP address pool named *auxiliary1* for secondary hosts behind the WiMAX CPE:

```
ip address secondary-pool name auxiliary1
```

# ip allowed-dscp

Sets the Quality of Service (QoS) Differentiated Services (DiffServ) marking that a subscriber session is allowed. The DSCP is disabled by default.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
ip allowed-dscp class class max-class maxclass [ rt-marking marking ]
no ip allowed-dscp class
```

#### no

Resets the parameters to the defaults: class none, max-class **be**. This indicates that all packets are let through without any dscp checking

#### ip allowed-dscp class *class*

Specifies the Differentiated Services Codepoint (DSCP) class with which the subscriber session may mark its packets. If the subscriber sessions packets request a code point class higher than the code point class specified, the PDSN service re-marks the packets with the QOS-DSCP value specified by the **ip qos-dscp** command.

Default: none

*class* must be one of the following;

**a**: allow packets with AF DSCPs

**e**: allow packets with EF DSCP

**o**: allow packets for experimental or local use

**ae**: allow packets with AF and EF DSCPs

**ao**: allow packets with AF DSCPs or packets for experimental or local use

**eo**: allow packets with EF DSCPs or packets for experimental or local use

**aeo**: allow packets with AF or EF DSCPs or packets for experimental or local use

**none**: allow only the **be** and **sc1** through **sc7** code points

### max-class *maxclass*

This parameter specifies the maximum code point with which a subscriber session may mark its packets. The subscriber sessions packets must be marked with a code point equal to or less than the code point specified. If the subscriber sessions packets request a code point higher than the code point specified, the PDSN service re-marks the packets with the QOS-DSCP value specified by the lower of the max-class and the **ip qos-dscp** command.

The list below identifies the code points from lowest to highest precedence. For example, if the **maxclass** is set to af22, that becomes the maximum code point that the subscriber session may mark it's packets with and only **be, af13, af12, af11,af23**, and **af22** are allowed. If a subscriber session marks its packets with anything after af22 in this list, the PDSN service re-marks the packets with the QOS-DSCP value specified by the lower of the maxclass and the **ip qos-dscp** command.

If class is set to none only the be and sc1 through sc7 codepoints are allowed. For example; if **class** is set to none and you set **max-class** to **sc1**, only the **sc1** and **be** codepoints are allowed.

Default: **be**

*maxclass* must be one of the following;

**be**: best effort forwarding

**af13**: assured Forwarding 13

**af12**: assured Forwarding 12

**af11**: assured Forwarding 11

**af23**: assured Forwarding 23

**af22**: assured Forwarding 22

**af21**: assured Forwarding 21

**af31**: assured Forwarding 31

**af32**: assured Forwarding 32

**af33**: assured Forwarding 33

**af41**: assured Forwarding 41

**af42**: assured Forwarding 42

**af43**: assured Forwarding 43

**ef**: expedited forwarding

**sc1**: selector class 1

**sc2**: selector class 2

**sc3**: selector class 3

**sc4**: selector class 4

**sc5**: selector class 5

**sc6**: selector class 6

**sc7**: selector class 7

### rt-marking *marking*

This parameter is used for Mobile IP (MIP) reverse tunnels. When MIP session packets do not have a DSCP marking, the Foreign Agent (FA) marks the packets with the value specified by **rt-marking** *marking*.

If MIP sessions packets have a DSCP marking, the marking is subjected to the conformance rules for the values of class and max-class; the final DSCP marking is then copied from the inner IP header to the outer IP header.

Default: **be**

*marking* must be one of the following;

**be**: best effort forwarding

**af11**: assured Forwarding 11

**af12**: assured Forwarding 12

**af13**: assured Forwarding 13

**af21**: assured Forwarding 21

**af22**: assured Forwarding 22

**af23**: assured Forwarding 23

**af31**: assured Forwarding 31

**af32**: assured Forwarding 32

**af33**: assured Forwarding 33

**af41**: assured Forwarding 41

**af42**: assured Forwarding 42

**af43**: assured Forwarding 43

**ef**: expedited forwarding

**sc1**: selector class 1

**sc2**: selector class 2

**sc3**: selector class 3

**sc4**: selector class 4

**sc5**: selector class 5

**sc6**: selector class 6

**sc7**: selector class 7

**Usage Guidelines**

Use this command to configure Quality of Service (QoS) for a subscriber session to allow a Differentiated Services (DiffServ) Code Point (DSCP) marker in the header of each IP packet that prompts network routers to apply differentiated grades of service to various packet streams.

This command uses **class** and type of marker (**rt-marking** for reverse tunnels) for configuration with **max-class** maximum code point that a subscriber session may mark its packets with.

### Example

The following command will allow *o* packets for experimental or local use with best effort forwarding *be*:

```
ip allowed-dscp class o max-class be
```

# ip context-name

Configures the context to which the subscriber is assigned upon authentication. The assigned context is considered the destination context that provides the configuration options for the services the subscriber is allowed to access.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] ip context-name** *name*

### no

Removes the current assigned context from the subscriber's data.

### ip context-name *name*

Specifies the name of the context to assign the subscriber to once authenticated. *name* must be an alphanumeric string of 1 trough 79 characters.

**Usage Guidelines**

Set the subscriber IP context to a common context when all subscribers from one or more contexts will use the same egress context.

### Example

The following command specifies the IP context name *egress2*:

```
ip context-name egress2
```

# ip header-compression

Configures the IP packet header compression options for the current subscriber. Although this command configures IP header compression algorithms, the Internet Protocol Control Protocol (IPCP) negotiations determine when the header compression algorithm is applied.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**ip header-compression { rohc [ any [ mode { optimistic | reliable | unidirectional } ] | cid-mode { { large | small } [ marked-flows-only | max-cid | max-hdr** *value* **| mrru** *value* **] } | marked flows-only | max-hdr** *value* **| mrru** *value* **| downlink | uplink ] | vj } +**

**[ default | no ] ip header-compression**

#### default

Restores this command's default setting to the Van Jacobsen (VJ) header compression algorithm.

#### no

Disables all IP header compression.

**ip header-compression { rohc [ any [ mode { optimistic | reliable | unidirectional } ] | cid-mode { { large | small } [ marked-flows-only | max-cid | max-hdr *value* | mrru *value* ] } } | marked flows-only | max-hdr *value* | mrru *value* | downlink | uplink ] | vj }**

Specifies that the Robust Header Compression (ROHC) algorithms is used for data.

**Important** ROHC is only supported for use with the PDSN.

**any**: Apply ROHC header compression in both the uplink and downlink directions.

**mode { optimistic | reliable | unidirectional }**:

- **optimistic**: Sets the ROHC mode to Bidirectional Optimistic mode (O-mode). In this mode packets are sent in both directions. A feedback channel is used to send error recovery requests and (optionally) acknowledgments of significant context updates from decompressor to compressor. Periodic refreshes are not used in the Bidirectional Optimistic mode.
- **reliable**: Sets the ROHC mode to Bidirectional Reliable mode (R-mode). This mode applies an intensive usage of a feedback channel and a strict logic at both the compressor and the decompressor that prevents loss of context synchronization between the compressor and the decompressor. Feedback is sent to acknowledge all context updates, including updates of the sequence number field.
- **unidirectional**: Sets the ROHC mode to Unidirectional mode (U-mode). With this mode packets are sent in one direction only, from the compressor to the decompressor. This mode therefore makes ROHC usable over links where a return path from the decompressor to the compressor is unavailable or undesirable.

**cid-mode { { large | small } [ marked-flows-only | dm | max-hdr** *value* **| mrru** *value* **] }**: Specifies the ROHC packet type to be used.

- **large | small [ marked-flows-only | max-cid | max-hdr** *value* **| mrru** *value* **]**: Defines the ROHC packet type as large or small and optionally sets the following parameters for the packet type selected:
- **marked-flows-only**: Specifies that ROHC is to be applied only to marked flows.
- **max-cid** *integer*: Default: 0 The highest context ID number to be used by the compressor. *integer* must be an integer from 0 through 15 when small packet size is selected and must be an integer from 0 through 31 when large packet size is selected.
- **max-hdr** *value*: Specifies the maximum header size to use. Default: 168. *value* must be an Integer from 0 through 65535.
- **mrru** *value*: Specifies the maximum reconstructed reception unit to use. Default: 65535. *value* must be an Integer from 0 through 65535.

**marked-flows-only**: Specifies that ROHC is to be applied only to marked flows.

**max-hdr** *value*: Specifies the maximum header size to use. Default: 168. *value* must be an Integer from 0 through 65535.

**mrru** *value*: Specifies the maximum reconstructed reception unit to use. Default: 65535. *value* must be an Integer from 0 through 65535.

**downlink**: Apply the ROHC algorithm only in the downlink direction.

**uplink**: Apply the ROHC algorithm only in the uplink direction.



**Important** When ROHC is enabled for downlink or uplink only the operational mode is Unidirectional.

**vj**

Specifies that the VJ algorithm is used for header compression.

**+**

Either one or both of the keywords may be entered in a single command.

If both **vj** and **rohc** are specified, **vj** must be specified first.

**Important** If both VJ and ROHC header compression are specified, the optimum header compression algorithm for the type of data being transferred is used for data in the downlink direction.

**Usage Guidelines** Header compression can be used to provide a higher level of security in IP traffic enhance bandwidth usage and lower bit errors.

By default the header compression algorithm is set to **vj**.

### Example

The following command disables all IP packet header compression:

```
no ip header-compression
```

The following command sets IP header compression to default vj algorithm:

```
default ip header-compression
```

The following command also sets the IP header compression to the vj algorithm:

```
ip header-compression vj
```

The following command enables the Internet Protocol Control Protocol (IPCP) to determine which protocol is the optimum algorithm for data in the downlink direction and use either VJ or ROHC as needed:

```
ip header-compression vj rohc
```

The following command enables ROHC for the downlink direction only:

```
ip header-compression rohc downlink
```

The following command enables ROHC in any direction using Bidirectional Optimistic mode:

```
ip header-compression rohc any mode Optimistic
```

# ip hide-service-address

Hides the IP address of the service from the subscriber.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no ] ip hide-service-address
```

**no**

Does not hide the IP address of the service from the subscriber. This is the default behavior.

**ip hide-service-address**

Hides the IP address of the service from the subscriber.

**Usage Guidelines**

Use this command to prevent subscribers from using traceroute to discover the network addresses that are in the public domain and configured on services. This prevent users from pinging such addresses.

**Example**

The following command hides the IP address of the service from the subscriber:

```
ip hide-service-address
```

# ip local-address

Configures the local-side IP address of the subscriber's point-to-point connection.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
ip local-address ip_address
no ip local-address
```

**no**

Removes a previously configured IP local-address.

**ip_address *ip_address***

Specifies an IP address configured in a destination context on the system through which a packet data network can be accessed. *ip_address* is entered using IPv4 dotted-decimal notation.

**Usage Guidelines**

This parameter specifies the IPv4 address on the system that the MS uses as the remote-end of the PPP connection. If no local address is configured, the system uses an "unnumbered" scheme for local-side addresses.

### Example

The following command configures a local address of 192.168.1.23 for the MS:

```
local-address 192.168.1.23
```

# ip multicast discard

Configures the IP multicast discard packet behavior.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no ] ip multicast discard
```

#### no

Does not discard IP multicast packets.

#### ip multicast discard

Discards IP multicast packets.

**Usage Guidelines**

This command specifies if IP multicast packets will be discarded.

### Example

The following command discards IP multicast packets:

```
ip multicast discard
```

# ip qos-dscp

Configures quality of service (QoS) options for the current subscriber using the differentiated services code point (DSCP) method. This functionality is disabled by default.

**Product**

All

**Privilege**

Security Administrator, Administrator

## Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

## Syntax Description

**ip qos-dscp** *option*
**no ip qos-dscp**

### no

Sets the quality of service option to its default value.

### ip qos-dscp *option*

Default: be (Best Effort)

Specifies the subscriber's per hop quality of service setting as one of:

- **af11**: assured Forwarding 11
- **af12**: assured Forwarding 12
- **af13**: assured Forwarding 13
- **af21**: assured Forwarding 21
- **af22**: assured Forwarding 22
- **af23**: assured Forwarding 23
- **af31**: assured Forwarding 31
- **af32**: assured Forwarding 32
- **af33**: assured Forwarding 33
- **af41**: assured Forwarding 41
- **af42**: assured Forwarding 42
- **af43**: assured Forwarding 43
- **be**: best effort forwarding
- **ef**: expedited forwarding

## Usage Guidelines

Set the quality of service for a subscriber based upon the service level agreements.

### Example

The following command specifies the QoS as expedited forwarding:

**ip qos-dscp ef**

# ip route

Configures the static route to use to reach the subscriber's network.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] ip route** *ip_address ip_mask* **[** *gateway_address* **]**

**no**

Removes the configured route information from the subscriber data.

**ip route *ip_address***

Specifies the target IP address for which the route information applies using IPv4 dotted-decimal notation.

***ip_mask***

Specifies the networking mask for the route.

1 bits in the *ip_mask* indicate that bit position in the *ip_address* must also have a value of 1.

0 bits in the *ip_mask* indicate that bit position in the *ip_address* does not need to match, such as the bit can be either a 0 or a 1.

For example, if the IP address and mask were specified as 172.168.10.0 and 255.255.255.224, respectively, the network mask will be 172.168.0.0 (obtained by logically ANDing the IP address with the IP mask).

***gateway_address***

Default: assigned remote IP address will be used as the gateway address.

Specifies the IP address of the next hop gateway for the route using IPv4 dotted-decimal notation.

**Usage Guidelines**

The static routes are also known as framed IP routes for subscribers. Static routes are typically applicable for subscribers connecting via other networks or when the mobile device acts as a gateway to a network on the far side of the device.

For example, if the mobile device is assigned IP address 10.2.3.4 and it acts as a gateway for the network 10.2.3.0 (with a network mask of 255.255.255.0) a static route would be configured with the *ip_address* being 10.2.3.0, *ip_mask* being 255.255.255.0, and *gateway_address* being 10.2.3.4.

**Example**

The following command disables the static route at IP address *10.2.3.4 255.255.255.0*.

```
no ip route 10.2.3.4 255.255.255.0
```

# ip source-validation

Enables or disables packet source validation for the current subscriber. Source validation requires that the source address of the received packets match the IP address assigned to the subscriber (either statically or dynamically) during the session.

If an incorrect source address is received from the mobile node, the system attempts to renegotiate the PPP session. The parameters for IP source validation can be set by the **ip source-violation** command.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] ip source-validation**

**no**

Disables source validation.

**ip source-validation**

Enables source validation.

**Usage Guidelines**

Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

**Example**

The following command enables IP source validation:

```
ip source-validation
```

The following command disables IP source validation:

```
no ip source-validation
```

# ip user-datagram-tos copy

Controls copying of the IP TOS octet value from IPv4/IPv6 datagrams to the IP header in tunnel encapsulation. This is disabled by default.

**Product**

PDSN

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**ip user-datagram-tos copy [ access-link-tunnel | both | data-tunnel ]**

**no ip user-datagram-tos copy**

**no**

Disable copying of the IP TOS octet value to all tunnel encapsulation IP headers.

**ip user-datagram-tos copy**

Enables copying of the IP TOS octet value to all tunnel encapsulation IP headers.

**access-link-tunnel**

Copies the IP TOS octet value to the tunnel encapsulation IP header on the access side (RP) tunnel.

**both**

Uses both the access-link-tunnel and data-tunnel.

**data-tunnel**

Copies the IP TOS octet value to the tunnel encapsulation IP header on the MIP data tunnel or L3 tunnel (IP-in-IP, GRE).

**Usage Guidelines**

Use this command to enable the copying of the IP TOS octet value to the tunnel encapsulation IP header.

This functionality allows PCF to detect special TOS marking in the outer IP header of A11 packets and to identify certain packets as QChat control messages. The Base Station Controller/Packet Control Function (BSC/PCF) must give higher priority to QChat control messages.

**Example**

The following command enables copying of the IP TOS octet value to the tunnel encapsulation IP header for the access side tunnel:

**ip user-datagram-tos copy access-link-tunnel**

The following command disables copying of the IP TOS octet value to all tunnel encapsulation IP headers:

**no ip user-datagram-tos copy**

# ip vlan

Configures subscriber-to-Virtual LAN (VLAN) associations.

**Product**

PDSN

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**ip vlan** *vlan-id*

**[ default | no ] ip vlan**

**default**

Resets the VLAN ID to the default setting.

**no**

Disables the VLAN ID for the subscriber.

**ip vlan *vlan-id***

Specifies the VLAN ID that is associated with the IP address for that session. *vlan-id* is an integer from 1 through 4094.

**Usage Guidelines**

This command configures the subscriber vlan ID which is used with the assigned address for the subscriber session to receive packets. If the IP pool from which the address is assigned is configured with a VLAN ID, this subscriber configured VLAN ID overrides it.

Subscriber traffic can be routed to specific VLANs based on the configuration of their user profile. Using this functionality provides a mechanism for routing all traffic from a subscriber over the specified VLAN. All packets destined for the subscriber must also be sent using only IP addresses valid on the VLAN or they will be dropped.

**Example**

Set the vlan ID to the default setting by entering the following command:

```
default ip vlan
```

# ipv6 access-group

Configures the IPv6 access group for a subscriber.

**Product**

PDSN

GGSN

ASN-GW

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**ipv6 access-group** *name* **[ in | out ]**

**ipv6 access-group *name***

Defines the access group name. *name* is an alphanumeric string of 1 through 47 characters.

**in**

Defines the access group as inbound.

**out**

Defines the access group as outbound.

**Usage Guidelines**

Used to create an access group for a subscriber.

**Example**

The following command provides an example of an IPv6 access group with the name *list_1*:

**ipv6 access-group list_1**

# ipv6 address

Configures a static IP address for use by the subscriber.

**Product**

PDSN

GGSN

ASN-GW

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**`[ no ] ipv6 address { prefix`** *`address`* **`| prefix-pool`** *`name`* **`}`**

**no**

Deletes a previously configured ipv6 address.

**ipv6 address *address***

Specifies an IPv6 address. *address* is entered using IPv6 colon-separated-hexadecimal notation.

**prefix**

Specifies a static IPv6 address.

**prefix-pool *name***

Specifies an IPv6 prefix pool name. *name* is an alphanumeric string of 1 through 31 characters.

**Usage Guidelines**

Use this command to assign a static IPv6 address to the subscriber. This address will be used each time the subscriber establishes data sessions.

**Example**

The following command configures a static IP address of *2001:4A2B::1f3F* with a mask length of *24* to the subscriber:

```
ipv6 address 2001:4A2B::1f3F/24
```

# ipv6 dns

Configures the IPv6 Domain Name Service (DNS) servers.

**Product**

PDSN

GGSN

ASN-GW

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**`[ no ] ipv6 dns { primary | secondary } {`** *`ipv6_dns_address`* **`}`**

**no**

Deletes a previously configured DNS server.

**ipv6 dns *ipv6_dns_address***

Specifies an IP address for the DNS server. *ipv6_dns_address* is entered using IPv6 colon-separated-hexadecimal notation.

**primary**

Configures the primary DNS server for the subscriber.

**secondary**

Configures the secondary DNS server for the subscriber. Only one secondary DNS server can be configured.

***ipv6_dns_address***

Configures the IP address of the DNS server.

**Usage Guidelines**

DNS servers are configured on a per subscriber basis. This allows each subscriber to use specific servers.

**Example**

The following command provides an example of setting the primary IPv6 DNS server:

```
ipv6 dns primary fe80::c0a8:a04
```

# ipv6 dns-proxy

Configures the system to act as a domain name server proxy for the current subscriber.

**Product**

PDSN

GGSN

ASN-GW

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ default | no ] ipv6 dns-proxy**

**default**

Disables IPv6 DNS proxy functionality for a subscriber.

**no**

Removes the pre-enabled functionality of IPv6 DNS proxy for a subscriber.

**ipv6 dns-proxy**

Enables IPv6 DNS proxy functionality for a subscriber. If enabled, the system will act as a proxy DNS server.

Default: disabled.

**Usage Guidelines**

Used to enable or disable IPv6 DNS proxy for the subscriber. When enabled, the PDSN acts as a proxy DNS server for DNS IPv6 queries coming from the mobile station to the PDSN's local PPP link address.

**Example**

The following command disables the IPv6 DNS proxy function for the subscriber:

```
no ipv6 dns-proxy
```

# ipv6 egress-address-filtering

Configures the system to perform egress address filtering for the subscriber.

**Product**

PDSN

GGSN

ASN-GW

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure** > **context** *context_name* > **subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no ] ipv6 egress-address-filtering
```

**no**

Disables IPv6 egress address filtering.

**ipv6 egress-address-filtering**

Enables IPv6 egress address filtering.

**Usage Guidelines**

Used to enable the filtering of packets that arrive from the Internet to a particular site.

**Example**

The following command disables egress address filtering:

```
no ipv6 egress-address-filtering
```

# ipv6 initial-router-advt

Creates an IPv6 initial router advertisement interval for the subscriber.

**Product**

PDSN

GGSN

ASN-GW

HSGW

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure** > **context** *context_name* > **subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
ipv6 initial-router-advt { interval value | num-advts value |
router-solicit-wait-timeout value }
default ipv6 initial-router-advt { interval | num-advts |
router-solicit-wait-timeout }
no ipv6 initial-router-advt router-solicit-wait-timeout
```

**default**

Resets the command to its default settings.

**no ipv6 initial-router-advt router-solicit-wait-timeout**

Disables running timer to wait for router solicit and sends the initial router advertisement immediately once session is up.

**ipv6 initial-router-advt**

Enables an initial router advertisement interval in milliseconds.

**interval *value***

Default: 3000

The time interval the initial IPv6 router advertisement is sent to the mobile node in milliseconds.

*value* is an integer between 100 and 16000 milliseconds.

**num-advts value *value***

Default: 3

The number of initial IPv6 router advertisements sent to the mobile node. *value* is an integer between 1 to 16.

**router-solicit-wait-timeout *value***

Default: 3000

The time interval to wait for router solicit before sending the initial IPv6 router advertisement.

*value* is an integer between 1 and 30000 milliseconds.

**Usage Guidelines**

This command is used to set the advertisement interval and the number of advertisements. Using a smaller advertisement interval increases the likelihood of router being discovered more quickly when it first becomes available.

If timer is enabled and router solicit is received before timeout, then RA will be sent in response to RS and no further RA will be sent. If timer is enabled and no router solicit is received after timeout, initial RAs will be sent as configured and IPv6 capability indication will be sent in S2a to P-GW to indicate that P-GW should drop any IPv6 traffic for this PDN.

**Example**

The following command specifies the initial ipv6 router interval to be 2000ms:

```
ipv6 initial-router-advt interval 2000
```

# ipv6 interface-id

Provides an IPv6 interface identifier for the subscriber.

**Product**

PDSN

GGSN

ASN-GW

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**ipv6 interface-id** *ifid*

**[ default | no ] ipv6 interface-id**

**default**

No interface ID set for IPv6CP negotiation to subscriber.

**no**

Deletes a previously configured IPv6 interface ID.

**interface-id *ifid***

Specifies the interface ID assigned to the Mobile during IPv6 Control Protocol (IPv6CP) negotiation. *ifid* is a 64-bit unsigned integer.

**Usage Guidelines**

Used to provide a IPv6 ifid for the subscriber when using IPv6-to-IPv4 (6to4) routing.

**Example**

The following command provides an example of assigning an IPv6 interface ID of *00-00-00-05-47-00-37-44* to the subscriber:

**ipv6 interface-id 00-00-00-05-47-00-37-44**

# ipv6 minimum-link-mtu

Configures the IPv6 minimum link maximum transmission unit (MTU) value.

**Product**

PDSN

GGSN

ASN-GW

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**ipv6 minimum-link-mtu** *value*

**default ipv6 minimum-link-mtu**

**default**

Resets minimum link MTU to its default setting: 1280.

**ipv6 minimum-link-mtu *value***

Specifies the MTU (in bytes) as a minimum link value. *value* is an integer between 100 and 2000.

**Usage Guidelines**

Used to override the IPv6 minimum link MTU values recommended by the standard.

**Example**

The following command provides an example of assigning an IPv6 minimum link MTU to *1580* to the subscriber:

```
ipv6 minimum-link-mtu 1580
```

# ipv6 secondary-address

Configures additional IPv6 4-bit prefixes to the subscriber session.

**Product**

PDSN

GGSN

ASN-GW

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] ipv6 secondary-address { prefix** *ipv6_address_prefix* **| prefix-pool** *pool_name* **}**

**no**

Deletes a previously configured ipv6 secondary address.

**ipv6 secondary-address *ipv6_address_pref***

Specified the secondary IPv6 address using IPv6 colon-separated-hexadecimal notation.

***pool_name***

Specifies the name given to the secondary address prefix pool as an alphanumeric string of of 1 through 31 characters.

**Usage Guidelines**

An IPv6 prefix pool name may be configured for a dynamic prefix, while the prefix is static. This command may be executed multiple times to configure multiple prefixes.

**Example**

The following command assigns an IPv6 secondary address prefix-pool name of *eastcoast* to the subscriber:

```
ipv6 secondary-address prefix-pool eastcoast
```

# l2tp send accounting-correlation-info

Enables the sending of accounting correlation information (Correlation-Id, NAS-IP-Address and NAS-ID) by the L 2TP Access Concentrator (LAC) in L2TP control messages (ICRQ) during session setup to an L2TP Network Server (LNS).

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no | default ] l2tp send accounting-correlation-info**

**no**

Disables the sending of accounting correlation information by the LAC.

#### default

Sets the setting to default mode: disable.

#### l2tp send accounting-correlation-info

Enables the sending of accounting correlation information by the LAC.

**Usage Guidelines**

Use this command to enable the LAC to send accounting correlation information (Correlation-Id, NAS-IP-Address and NAS-ID) in L2TP control message (ICRQ) during session setup to LNS for this subscriber. LNS can be configured to include this information in ACS billing records, so that billing servers can easily correlate accounting records from PDSN/LAC and LNS.

By default, this mode is disabled.

#### Example

The following command disables the inclusion of accounting correlation information in control messages during session setup to an LNS for a subscriber:

```
default l2tp send accounting-correlation-info
```

# l3-to-l2-tunnel address-policy

Configures the subscriber address allocation/validation policy, when subscriber Layer 3 (IPv4) sessions are tunneled using Layer 2 tunneling protocol (L2TP).

**Product**

HA

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**l3-to-l2-tunnel address-policy { alloc-only | alloc-validate | no-alloc-validate }**

**default l3-to-l2-tunnel address-policy**

#### default

Restores the default value for Layer 3-to-Layer 2 tunnel addressing: **no-alloc-validate**.

#### l3-to-l2-tunnel address-policy

Sets the policy for Layer 3-to-Layer 2 sessions to one of the following options.

#### alloc-only

Only allocates an address in the case of dynamic address assignment. Does not validate static addresses.

#### alloc-validate

Locally allocates and validates the subscriber addresses.

#### no-alloc-validate

Does not allocate or validate subscriber addresses locally for current subscribers sessions. Passes the address between the remote tunnel terminator and the Mobile Node. This is the default behavior.

### Usage Guidelines

Use this command to configure the L3 to L2 tunnel address policy for MIP HA sessions tunneled from the system using L2TP tunnels or for GGSN IP Context sessions tunneled using L2TP to a remote LNS. Also refer to the **resource** keyword of the Context Configuration mode **ip pool** command.

#### Example

the following command sets the L3-to-L2 tunnel address policy so that the current subscriber must have IP addresses allocated and validated locally on the system:

```
l3-to-l2-tunnel address-policy alloc-validate
```

# loadbalance-tunnel-peers

Configures the load balancing of traffic bound for L2TP tunnels configured on the system for the selected subscriber.

### Product

L2TP

### Privilege

Security Administrator, Administrator

### Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

### Syntax Description

```
loadbalance-tunnel-peers { balanced | prioritized | random }
```

#### loadbalance-tunnel-peers

Enables load balancing of L2TP traffic using one of the methods described below.

#### balanced

Enables the equal use of all configured tunnel peers (LNSs) for the selected subscriber.

**prioritized**

Enables the use of all configured tunnel peers (LNSs) for the selected subscriber based on the preference number assigned to the peer address.

**random**

Default: Enabled

Enables the random use of all configured tunnel peers (LNSs) for the selected subscriber.

**Usage Guidelines**

Use to manage traffic loads on L2TP Access Concentrator (LAC) ports and their respective L2TP Network Servers (LNSs).

**Example**

Use the following command to randomly use all configured tunnel peers (LNSs):

```
loadbalance-tunnel peers random
```

# long-duration-action

Specifies what action is taken when the long duration timer expires.

**Product**

All

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
long-duration-action { detection | disconnection [ dormant-only ] [
suppress-notification ] }
```

**detection**

Default: Enabled

Detects long duration sessions and sends SNMP TRAP and CORBA notification. This is the default behavior.

Use this command to detect a session exceeding the limit set by the long duration timer.

**disconnection [ dormant-only ] [ suppress-notification ]**

Default: Disabled

Detects a long duration session and disconnects the session after sending SNMP trap and CORBA notification.

**suppress-notifiaction**: Suppresses the SNMP trap and CORBA notification after detecting and disconnecting a long duration session. Default: Disabled

**dormant only**: Disconnects the dormant sessions after long duration timer and inactivity time with idle time-out duration expires. If the long duration timeout is fired and the call is not dormant, the call is disconnected when the call later moves to dormancy.



**Important** For HA calls, the inactivity-time is considered as gauge for dormancy.

It sends the SNMP trap and CORBA notification after disconnecting a long duration session. Default: Disabled

**Usage Guidelines** Use this command to determine what action is taken when a session exceeds the limit set by the long duration timer.

### Example

Use the following command to enable disconnecting sessions that exceed the long duration timer:

```
long-duration-action disconnection
```

Use the following command to disconnect the session that exceed the long duration timer without sending SNMP trap and CORBA notification:

```
long-duration-action disconnection suppress-notification
```

Use the following command to disconnect the session that is in dormant and exceed the long duration timer and send SNMP trap and CORBA notification:

```
long-duration-action disconnection dormant-only
```

Note that in case of HA calls, the inactivity-time is considered as gauge for dormancy.

# max-pdn-connections

Specifies the maximum number of connections to packet data networks (PDNs) supported per eHRPD session.

**Product** HSGW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**max-pdn-connections** *eHRPD_PDNs*

**default max-pdn-connections**

### default

Resets the maximum number of PDN connections supported per eHRPD session to 3.

#### max-pdn-connections *eHRPD_PDNs*

Specifies the maximum number of PDN conceitedness allowed per eHRPD session. *eHRPD_PDNs* must be an integer from 1 to 14. Default is 3.

**Usage Guidelines**

This command is used to specify the maximum number of PDN connections supported per eHRPD session.

#### Example

The following command specifies a maximum of 5 PDNs per eHRPD session:

```
max-pdn-connections 5
```

# mediation-device

Enables the use of a mediation device for subscribers, and specifies the system context to use for communicating with the device. A mediation device can be the initial point of contact for all IT systems that need to receive Charging Data Records (CDRs). Mediation devices can also be deep-packet inspection servers or transaction control servers.

**Product**

GGSN

P-GW

PDG/TTG

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**mediation-device context-name** *<context-name>* **[ no interims ]**

**[ no | default ] mediation-device**

#### no

Deletes the mediation-device configuration.

#### default

Changes the mediation device to no context-name configured and restores the mediation device's default properties.

#### mediation-device context-name *context-name*

Default: The subscriber's destination context.

Configures the mediation VPN context for the subscriber.

*context-name* must be an alphanumeric string of 1 through 79 characters that is case sensitive. If not specified, the mediation context is same as the destination context of the subscriber.

**no-interims**

Disables sending of Interim messages to the mediation device.

Default: Disabled

**Usage Guidelines**

This command is used to enable mediation device support for subscribers.

Keywords to this command can be used in combination to each other, depending on configuration requirements.

**Example**

The following command enables mediation device support for the subscriber and uses the protocol configuration located in an system context called *ggsn1*:

**mediation-device context-name ggsn1**

# mobile-ip

Enables or disables access to mobile IP services by the subscriber.

**Product**

HA

FA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] mobile-ip { allow-aaa-address-assignment | dns-address source-priority { aaa | home-agent } | gratuitous-arp aggressive | home-agent** *ip_address* **[alternate] | match-aaa-assigned-address | min-reg-lifetime-override [***value* **| infinit ] | mn-aaa-removal-indication | mn-ha-hash-algorithm { hmac-md5 | md5 | rfc2002-md5 } | mn-ha-shared-key** *key* **| mn-ha-spi** *spi_num* **| reverse-tunnel | security-level { ipsec | none } | send {access-technology | accounting-correlation-info bsid | dns-address | host-config | imsi | terminal-verification } }**

**no**

Disables the mobile IP option specified.

**allow-aaa-address-assignment**

Default: Disabled.

Enables the FA to accept a home address assigned by an AAA server. This should only be configured on the FA side.

**dns-address source-priority { aaa | home-agent }**

Sets the priority behavior on the FA to use either the DNS IP address information from the HA or the AAA server to include in the RRP to the MN.

When the **no** keyword is used in conjunction with the **dns-address** keyword, information received from both the home-agent and the AAA server is sent if available.

DNS IP address information from the HA comes from the DNS Normal Vendor/Organization Specific Extension (NVSE) in the Registry Registrar Protocol (RRP).

DNS IP address information from the AAA server is in the access accept message.

**home-agent**: If the DNS address is received from the home-agent only that information is sent to the MN. Otherwise the DNS address received from the AAA server is sent.

**aaa**: If the DNS address is received from the AAA server only that information is sent to MN. Otherwise the DNS address received from the home-agent is sent.

**gratuitous-arp aggressive**

Default: Disabled.

When enabled, this mode will cause the HA to send out gratuitous ARP (Address Resolution Protocol) messages for all Mobile IP (MIP) registration renewals and handoffs.

To disable this mode, use the **no** form of this command.



**Important** This mode will only work for IP addresses that have been assigned from a static IP address pool.

**home-agent *ip_address* [alternate]**

Specifies the IP address of the mobile IP user's home agent. *ip_address* must be entered using IPv4 dotted-decimal or IPv6 colon -separated notation.

**alternate** - Specifies the secondary, or alternate, Home Agent to use when Proxy Mobile IP HA Failover is enabled.

**match-aaa-assigned-address**

Default: Disabled.

Enables the FA to validate the home address in the RRQ against the one assigned by AAA server. This should only be configured on the FA side.

**min-reg-lifetime-override [*value* | infinit ]**

Default: 0.

Configures the subscriber for minimum registration lifetime parameter on HA service. By default it uses the value configured on HA service where *value* must be the minimum registration lifetime that the HA service allows in any Registration Request message from the mobile node. An infinite registration lifetime can be configured by setting the value as "infinite".

*value* is a minimum registration lifetime value in seconds and must be an integer between 1 through 65534.

**mn-aaa-removal-indication**

Default: Disabled.

When enabled, the MN-FA challenge and MN-AAA Authentication extensions are removed when relaying a Registration Request (RRQ) to the Home Agent (HA)

**mn-ha-hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }**

Speechifies the encryption algorithm to use.

Default: **hmac-md5**

**hmac-md5**: Uses HMAC-MD5 hash algorithm, as defined in RFC-2002bis. This is the default algorithm.

**md5**: Uses the MD-5 hash algorithm.

**rfc2002-md5**: Uses the MD-5 hash algorithm variant as defined in RFC-2002.

**mn-ha-shared-key *key***

Verifies the MN-HA Authentication for a local subscriber in the current context. *key* is an alphanumeric string or a hexadecimal number beginning with "0x" up to 127 bytes

**mn-ha-spi *spi_num***

Specifies the Security Parameter Index (SPI) number. *spi_num* must be an integer from 256 through 4294967295.

**reverse-tunnel**

Default: enabled.

All the mobile IP user to use reverse IP tunnels. The **no** keyword disables this option.

**security-level { ipsec | none }**

Default: none

Configures the security level needed for the subscriber's traffic.

**ipsec**: secures both MIP control and data traffic with IPSec.

**none**: none of the traffic is secured



**Important** This keyword corresponds to the 3GPP2-Security-Level RADIUS attribute. This attribute indicates the type of security that the home network mandates on the visited network.

**Important** For this attribute, the integer value "3" enables IPSec for tunnels and registration messages, "4" Disables IPSec

**send {access-technology | accounting-correlation-info bsid | dns-address | host-config | imsi | terminal-verification }**

**access-technology**: Configures FA to sends the access-technology type extension in the RRQ, by default it is disabled.

**accounting-correlation-info**: Configures whether the FA sends the correlation info to the NVSE in the RRQ. Default is disabled.

**dns-address**: Enables the HA to send the DNS address NVSE in the RRP. Default is disabled. This should only be enabled on the HA side.

**host-config**: Configures by sending the Host Config NVSE in RRQ. By default it is disabled.

**imsi**: Configures sending the IMSI NVSE in the RRQ. Default is sending IMSI in custom-1 format.

**terminal-verification**: Enables the FA to send the terminal verification NVSE in the RRQ. Default is disabled. This should only be enabled on the FA side.

**Important** **send dns-address** is a proprietary feature developed for a specific purpose and requires the MN to be able to renegotiate IPCP for DNS addresses and reregister MIP if necessary. Since this feature needs the MN to support certain PPP/MIP behavior, and not all MNs support that particular behavior, **send dns-address** should be enabled only after careful consideration.

**Usage Guidelines** Use as subscriber service contracts change.

### Example

The following command specifies the Home Agent at *10.2.3.4* for this subscriber:

```
mobile-ip home-agent 10.2.3.4
```

# mobile-ip ha

Accommodates two Mobile IP (MIP) Home Agent (HA) options in subscriber mode.

**Product** PDSN

HA

ASN-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] mobile-ip ha { assignment-table** *name* **| ignore-unknown-ha-addr-error }**

**no**

Disables the mobile IP HA option specified.

**assignment-table *name***

Specifies the name of an existing MIP HA Assignment table. *name* must be an alphanumeric string of 1 through 63 characters.

**ignore-unknown-ha-addr-error**

Default is disabled.

Enables or disables the HA to accept or reject the RRQ from a particular subscriber.

**Usage Guidelines**

Use this command to assign a MIP HA Assignment table to the current subscriber.

Use this command to disable or enable the HA to accept or reject the RRQ from a particular subscriber when the HA address in the incoming MIP RRQ is not the same as the HA service address. The feature is off by default which causes the RRQ to be rejected with the error code UNKNOWN_HOME_AGENT.

**Example**

The following command assigns the MIP HA Assignment table named *Atable1* to the current subscriber:

```
mobile-ip ha assignment-table Atable1
```

The following command sets **ignore-unknown-ha-addr-error** to its default disabled state:

```
no mobile-ip ha ignore-unknown-ha-addr-error
```

# mobile-ip reg-lifetime-override

Overrides the Mobile IP (MIP) registration lifetime from HA with value configured for subscriber.

**Product**

PDSN

HA

ASN-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**mobile-ip reg-lifetime-override [ *dur* | infinite ]**

**[ default | no ] mobile-ip reg-lifetime-override**

**mobile-ip reg-lifetime-override*dur***

Default: 100 seconds.

Overrides the MIP registration lifetime from HA for the specified period of time in seconds. *dur* must be an integer from 1 through 65534.

**infinite**

Sets the MIP registration lifetime override value to infinite for a particular subscriber.

**default**

Sets the value of mobile IP registration lifetime override option to 100 seconds.

**no**

Disables the MIP registration lifetime override option.

**Usage Guidelines**

Use this command to configure MIP registration-lifetime per realm/domain. This value overrides the default lifetime configured under HA service.

**Example**

The following command overrides the MIP registration lifetime value from HA service and defaults the MIP registration lifetime to 100 seconds for the current subscriber:

**default mobile-ip reg-lifetime-override**

# mobile-ip send access-technology

Enables the sending of the RAT (Radio Access Technology) of the MS to the HA in a PMIP RRQ (Proxy MIP Register Request) message.

**Product**

PDIF

PDSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description** **`[ default | no ] mobile-ip send access-technology`**

**default**

Disables the support for sending the RAT to the HA in a PMIP RRQ.

This is the default mode.

**no**

Removes the configured support for sending the RAT to the HA in a PMIP RRQ.

**Usage Guidelines** Use this command to send the RAT to the HA in a PMIP RRQ.

**Example**

The following command enables sending the RAT to the HA in a PMIP RRQ:

**`mobile-ip send access-technology`**

# mobile-ip send accounting-correlation-info

Enables the sending call correlation information Normal Vendor/Organization Specific Extensions (NVSEs) to the HA in the MIP Registry Registrar Protocol (RRP).

**Product** PDSN

HA

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description** **`[ default | no ] mobile-ip send accounting-correlation-info`**

**default**

Disables the support for sending call correlation information NVSEs to the HA in MIP RRQ.

This is the default mode.

**no**

Removes the configured support for sending call correlation information.

**Usage Guidelines** Use this command to support PDSN-Correlation-ID VSE and send the call correlation information.

### Example

The following command enables sending call correlation information NVSEs to the HA in MIP RRQ:

```
mobile-ip send accounting-correlation-info
```

# mobile-ip send bsid

Enables the sending of the BSID (Base Station Identifier) of the WiFi access point/Radio Access Network (RAN) to the HA in a PMIP RRQ (Register Request) message.

**Product**

PDIF

PDSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**mobile-ip send bsid [ custom-2 ]**

**[ default | no ] mobile-ip send bsid**

#### default

Disables the support for sending the BSID to the HA in a PMIP RRQ.

This is the default mode.

#### no

Removes the configured support for sending the BSID to the HA in a PMIP RRQ.

#### custom-2

NVSE to send service option attribute in the PMIP RRQ.



**Important** This is a customer-specific keyword and needs customer-specific license to use this feature.

**Usage Guidelines**

Use this command to send the BSID to the HA in a PMIP RRQ.

### Example

The following command enables sending the BSID to the HA in a PMIP RRQ:

```
mobile-ip send bsid
```

# mobile-ip send pcf-address

Configures whether the FA sends the PCF address NVSE in the RRQ.

**Product**



**Important** This command is customer specific. For more information contact your Cisco account representative.

HA

PDSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**mobile-ip send pcf-address [ custom-2 ]**

**[ default | no ] mobile-ip send pcf-address**

#### default

Disables the support for sending the PCF address to the HA in a PMIP RRQ.

This is the default mode.

#### no

Removes the configured support for sending the PCF address to the HA in a PMIP RRQ.

#### custom-2

NVSE to send PCF address attribute in the PMIP RRQ.

**Usage Guidelines**

Use this command to send the PCF address to the HA in a PMIP RRQ.

### Example

The following command enables sending the PCF address to the HA in a PMIP RRQ:

```
mobile-ip send pcf-address
```

# mobile-ip send service-option

Configures whether the FA sends the service option NVSE in the PMIP RRQ.

## Product

**Important** This command is customer specific. For more information contact your Cisco account representative.

HA

PDSN

## Privilege

Security Administrator, Administrator

## Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

## Syntax Description

**mobile-ip send service-option [ custom-2 ]**

**[ default | no ] mobile-ip send service-option**

### default

Disables the support for sending the service option to the HA in a PMIP RRQ.

This is the default mode.

### no

Removes the configured support for sending the service option to the HA in a PMIP RRQ.

### custom-2

NVSE to send service option attribute in the PMIP RRQ.

## Usage Guidelines

Use this command to send the service option to the HA in a PMIP RRQ.

### Example

The following command enables sending the service option to the HA in a PMIP RRQ:

```
mobile-ip send service-option
```

# mobile-ip send subnet-id

Configures whether the FA sends the subnet-id NVSE in the PMIP RRQ.

**Product**



**Important** This command is customer specific. For more information contact your Cisco account representative.

HA

PDSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
mobile-ip send subnet-id [ custom-2 ]
[ default | no ] mobile-ip send subnet-id
```

**default**

Disables the support for sending the subnet-id to the HA in a PMIP RRQ.

This is the default mode.

**no**

Removes the configured support for sending the subnet-id to the HA in a PMIP RRQ.

**custom-2**

NVSE to send subnet-id attribute in the PMIP RRQ.

**Usage Guidelines**

Use this command to send the subnet-id to the HA in a PMIP RRQ.

**Example**

The following command enables sending the subnet-id to the HA in a PMIP RRQ:

```
mobile-ip send subnet-id
```

# mobile-ipv6

Configures Mobile IPv6 related parameters for a subscriber.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ default | no ] mobile-ipv6 { home-address** *ipv6_address* **| home-agent** *ipv6_address* **| home-link-prefix** *ipv6_address* **| tunnel mtu** *value* **}**

**default**

Disables the support for sending call correlation information NVSEs to the HA in MIP RRQ.

This is the default mode.

**no**

Removes the configured support for sending call correlation information.

**home-address *ipv6_address***

Specifies the home address for the subscriber. *ipv6_address* must be entered using IPv6 colon-separated-hexadecimal notation.

**home-agent *ipv6_address***

Specifies the IPv6 address of the mobile IP user's home agent. *ipv6_address* must be entered using IPv6 colon-separated-hexadecimal notation.

**home-link-prefix *ipv6_address***

Specifies the IPv6 address of the mobile IP user's home link. *ipv6_address* must be entered using IPv6 colon-separated-hexadecimal notation.

**tunnel mtu *value***

Configures the tunnel MTU (in bytes) for the IPv6 tunnel between the HA and the mobile node. *value* must be an integer from 1024 through 2000. The default is 1500.

**Usage Guidelines**

This command sets the mobile-ipv6 parameters for a subscriber. Use this command to set the home-address, home-agent, and home-link prefix

**Example**

Use the following command to set the tunnel MTU value to *1800*:

```
mobile-ipv6 tunnel mtu 1800
```

# nai-construction-domain

After authentication, the domain name specified by this command replaces the Network Access Identifier (NAI) constructed for the subscriber.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**`nai-construction-domain`** *`domain_name`*

**`no nai-construction-domain`**

**nai-construction-domain *domain_name***

Defines the domain name to use to replace the NAI constructed domain name. *domain_name* must be an alphanumeric string of 1 through 79 characters.

**no**

Deletes the defined domain name.

**Usage Guidelines**

Define or delete a domain name to use to replace the NAI constructed domain name after authentication.

**Example**

the following command sets the domain name to *private1*:

**`nai-construction-domain private1`**

To delete the previously configured domain name, use the following command:

**`no nai-construction-domain`**

# nbns

Configures and enables use of NetBIOS Name Service (NBNS) for the subscriber.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure** > **context** *context_name* > **subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] nbns { primary** *IPv4-address* **| secondary** *IPv4-address* **}**

**nbns primary**

Designates primary NBNS server. Must be followed with IPv4 address in dotted-decimal notation.

**nbns secondary**

Designates secondary/failover NBNS server. Must be followed with IPv4 address in dotted-decimal notation.

***IPv4-address***

Specifies the IP address used for this service using IPv4 dotted-decimal notation.

**no**

Removes/disables use of a previously configured NetBios Name Service.

**Usage Guidelines**

This command specifies NBNS parameters. The NBNS option is present for both PDP type IP and PDP type PPP for GGSN.

The system can be configured to use of NetBIOS Name Service for the Access Point Name (APN).

**Example**

The following command configures the subscriber's NetBIOS Name Service to primary IP *192.168.1.15*:

```
nbns primary 192.168.1.15
```

# nexthop-forwarding-address

Configures the next hop forwarding address for the subscriber.

**Product**

PDSN

GGSN

ASN-GW

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure** > **context** *context_name* > **subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**nexthop-forwarding-address** *ip_address*

**no nexthop-forwarding-address**

**nexthop-forwarding-address *ip_address***

Configures the IP address of the nexthop forwarding address. *ip_address* must be entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**no**

Disables this function. This is the default setting.

**Usage Guidelines**

Use this command to configure the next hop forwarding address for the subscriber.

**Example**

The following command configures the next hop forwarding address to *209.165.200.225* (IPv4):

```
nexthop-forwarding-address 209.165.200.225
```

# npu qos

Configures an Network Processing Unit (NPU) QoS priority queue for packets from the subscriber.

**Product**

PDSN

GGSN

ASN-GW

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**npu qos traffic priority { best-effort | bronze | derive-from-packet-dscp | gold | silver }**

**best-effort**

Assigns the best-effort queue priority. This is the lowest priority.

**bronze**

Assigns the bronze queue priority. This is the third-highest priority.

**derive-from-packet-dscp**

Default: Enabled

Specifies that the priority is to be determined from the DS field in the packet's TOS octet.

**gold**

Assigns the gold queue priority. This is the highest priority.

**silver**

Assigns the silver queue priority. This is the second-highest priority.

**Usage Guidelines**

This command is used in conjunction with the Network Processing Unit (NPU) Quality of Service (QoS) functionality.

The system can be configured to determine the priority of a subscriber packet either based on the configuration of the subscriber, or from the differentiated service (DS) field in the packet's TOS octet (representing the differentiated service code point (DSCP) value).

Refer to the *System Administration Guide* for additional information on NPU QoS functionality.



**Important** This functionality is not supported for use with the PDSN at this time.

**Example**

The following command configures the subscriber's priority queue to be gold:

```
npu qos traffic priority gold
```

# nw-reachability-server

Binds the name of a configured network reachability server to the current subscriber and enables network reachability detection.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**nw-reachability server** *server_name*

**no nw-reachability server**

**nw-reachability server *server_name***

Specifies the name of a network reachability server that has been defined in the current context. *server_name* is an alphanumeric string of 1 through 16 characters.

**no nw-reachability server**

Deletes the name of the network reachability server from the current subscribers configuration and disable network reachability failure detection for the current subscriber.

**Usage Guidelines**

Use this command to define the network reachability server for the current subscriber and enable network reachability failure detection for the current subscriber. If a network reachability server is defined in an IP pool, that setting takes precedence over this command.

**Important** Refer to the HA configuration mode command **policy nw-reachability-fail** to configure the action that should be taken when network reachability fails.

**Important** Refer to the context configuration mode command **nw-reachability server** to configure network reachability servers.

**Important** Refer to the **nw-reachability server server_name** keyword of the **ip pool** command in the *Context Configuration Mode Commands* chapter to bind the network reachability server to an IP pool.

**Example**

To bind a network reachability server named *InternetDevice* to the current subscriber, enter the following command:

```
nw-reachability server InternetDevice
```

# outbound

Configures the subscriber host password for use when authenticating PPP sessions.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure** > **context** *context_name* > **subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**outbound [ encrypted ] password** *pwd*

**no outbound password**

**[ outbound encrypted ] password *pwd***

Specifies the password to use for point-to-point protocol session host authentication. The **encrypted** keyword indicates the password specified uses encryption.

The password specified as *pwd* must be an alphanumeric string of 1 through 63 characters without encryption, or 1 through 127 characters with encryption.

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

**no outbound password**

Clears the outbound password configuration from the subscriber data.

**Usage Guidelines**

Sets the outbound (egress) password for increased security.

**Example**

**outbound password** *secretPwd*

**outbound encrypted password** *scrambledPwd*

**no outbound password**

# overload-disconnect

Sets the threshold parameter for overload disconnect.

**Product**

ASN-GW

HA

PDIF

PDSN

PHSGW

PDG/TTG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**overload-disconnect [ threshold { inactivity-time** *inactivity_time_threshold* **| connect-time** *connect_time_threshold* **} ]**

**[ default | no ] overload-disconnect [ threshold { inactivity-time | threshhold connect-time } ]**

**threshold inactivity-time *inactivity_time_threshold***

Sets the inactivity time threshold (in seconds) as an integer from 0 through 4294967295. The default value of zero disables this feature. If *inactivity-time* for the subscriber's session is greater than *inactivity_time_threshold*, the session becomes a candidate for disconnection.

**threshold connect-time *connect_time_threshold***

Sets the connection time threshold (in seconds) as an integer from 0 through 4294967295. A value of zero disables this feature. If connect-time for the subscriber's session is greater than *connect_time_threshold*, the session becomes a candidate for disconnection.

**default**

Enables the default condition for this subscriber.

**no**

Disables the overload disconnect feature for this subscriber. This is the default condition for PDIF.

**Usage Guidelines**

Set a subscriber's overload disconnect threshold in seconds, based on either inactivity or connection time. When this threshold is exceeded during a session, the subscriber's session becomes a candidate for disconnection. To set overload-disconnect policies for the entire chassis, see **congestion-control overload-disconnect** in the *Global Configuration Mode Commands* chapter.

**Example**

```
overload-disconnect threshold inactivity-time 120
default overload disconnect threshold connect-time
no overload-disconnect threshold connect-time
no overload disconnect
```

# password

Configures the subscribers password for the current context.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ encrypted ] password** *pwd*

**no password**

**encrypted**

Indicates the password provided is encrypted.

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

***pwd***

Specifies the user's password for authentication. *pwd* must be an alphanumeric string of 1 through 63 characters without encryption, or from 1 through 127 characters with encryption. A "null" password is allowed and is entered as consecutive double quotes (" "). See Example(s) for correct syntax.

**Important** Subscribers configured with a null password will be authenticated using PAP and CHAP (MD5) only. Subscribers configured without a password (**no password**) will only be able to access services if the service is configured to allow no authentication.

**no**

Used to clear the subscriber password configuration from the subscriber data.

**Important** Subscribers with no password will only be able to access services if the service is configured to grant access with no authentication.

**Usage Guidelines**

Password management is critical to system security and all precautions should be taken to ensure passwords are not shared or to easily deciphered.

**Example**

**password** *secretPwd*

**password ""**

**no password**

# pdif mobile-ip

Configures PDIF subscriber call setup parameters.

**Product**

PDIF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ default | no ] pdif mobile-ip { release-tia | required | simple-ip-fallback }**

**[ default | no ]**

Disables the option specified.

**release-tia**

Specifies that after subscriber call setup is complete, the tunnel inner address (TIA) is released. If SImple IP is enabled, the TIA becomes the principal communications tunnel and the restriction that it is only to be used to set up a Mobile-IP call is lifted. This parameter is disabled by default.

**required**

Specifies that Mobile IP is required for this subscriber whenever a call is set up. This parameter is disabled by default.

**simple-ip-fallback**

Specifies that Simple IP should be used when Mobile IP could not be established. This parameter is disabled by default.

**Usage Guidelines**

Use this command to configure specific behavior for the PDIF subscriber during call setup.

**Example**

The following command enables the system to fall back to Simple IP when Mobile IP fails for this subscriber during call setup:

**pdif mobile-ip simple-ip-fallback**

# permission

Enables or disables the subscriber's ability to access wireless data services.

**Product**

PDSN

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] permission { ha-mobile-ip | pdsn-mobile-ip | pdsn-simple-ip | pmipv6-interception }**

**default permission**

**no | default**

Disables the usage of the specified service.

**ha-mobile-ip | pdsn-mobile-ip | pdsn-simple-ip**

**ha-mobile-ip**: Enables or disables the Home Agent (HA) support for Mobile IP (MIP) service.

**pdsn-mobile-ip**: Enables or disables packet data and Foreign Agent (FA) support for MIP service.

**pdsn-simple-ip**: Enables or disables packet data support for simple IP service.

**pmipv6-interception**: Allows subscribers to access the external Local Mobility Anchor (LMA) over PMIPV6.

**Usage Guidelines**

Grants the subscriber access to services in the current context.

**Example**

The following command Grants the subscriber access to PDSN/HA services:

**permission pdsn-mobile-ip**

# policy ipv6 tunnel

Sets maximum transmission unit (MTU) behavior for the IPv6 tunnel between the HA and Mobile Node.

**Product**

PDSN

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**`policy ipv6 tunnel mtu exceed { fragment | notify-sender }`**

**mtu exceed { fragment | notify-sender }**

**fragment**: Adjusts tunnel MTU for fragmented packets

**notify-sender**: Sends an ICMPv6 Packet Too Big message to the original sender

**Usage Guidelines**

Use this command to configure MTU behavior for an IPv6 tunnel between the HA and Mobile Node.

**Example**

The following command configures adjustments to tunnel MTU for fragmented packets:

**`policy ipv6 tunnel mtu exceed fragment`**

# policy-group

Assigns or removes a flow-based traffic policy group to a subscriber.

**Product**

PDSN

HA

ASN-GW

HSGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**`[ no ] policy-group`** *`policy_group_name`* **`direction { in | out }`**

**no**

Removes assigned policy group from a subscriber configuration.

**policy-group *policy_group_name***

Specifies the traffic policy group name for a subscriber session flow pre-configured within a destination context. *policy_group_name* is an alphanumeric string of 1 through 15 characters that is case sensitive.

**direction { in | out }**

Specifies the direction of flow in which the traffic policies need to be applied.

- **in**: specifies the incoming traffic
- **out**: specifies the outgoing traffic

**Usage Guidelines** Use this command to assign a traffic policy group to a subscriber for traffic policing.

**Example**

The following command assigns inbound traffic policy group *tp-group1* to this subscriber:

```
policy-group tp-group1 direction in
```

# ppp

Configures the point-to-point protocol (PPP) options for the current subscriber.

**Product** PDSN

PDSN Closed R-P

GGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
ppp { accept-peer-ipv6-ifid | always-on-vse-packet | data-compression {
mode { normal | stateless } | protocols { protocols [ protocols ] } |
ip-header-compression negotiation { detect | force | vj compress-slot-id
 { both | none | receive | transmit } } | ipv4 { disable | enable | passive
 } | ipv6 { disable | enable | passive } | keepalive seconds |
min-compression-size min_octets | mtu max_octets | remote-renegotiation
disconnect { always | nai-prefix-msid-mismatch } }
```

```
default ppp { accept-peer-ipv6-ifid | always-on-vse-packet |
data-compression { mode | protocols } | ip-header-compression negotiation
 [ vj compress-slot-id ] | ipv4 | ipv6 | keepalive | min-compression-size
 | mtu | remote-renegotiation disconnect }
```

```
no ppp { accept-peer-ipv6-ifid | always-on-vse-packet | data-compression
 protocols | ipv4 | ipv6 | keepalive | mtu | remote-renegotiation
disconnect }
```

**default**

Restores the default value for the option specified.

**no**

Resets the option specified to its default.

**always-on-vse-packet**

Default: Enabled

If this feature is enabled, the PDSN sends special 3GPP2 VSE PPP packets to the Mobile Node with a maximum inactivity timer value. This configuration is applicable only for PDSN or PDSNCLOSED-RP sessions.

**accept-ipv6-peer-ifield**

Default: None

Configures an IPv6-to-IPv4 (6to4) tunnel and controls the behavior of IPv6CP negotiation for the Interface ID. If enabled, PDSN will accept a valid interface-id proposed by the peer.

**data-compression { mode { normal | stateless } | protocols { *protocols* [ *protocols* ] }**

Default: all protocols enabled.

Specifies the subscriber's mode of data compression or the compression protocol to use.

**mode**: sets the mode of compression where *modes* must be one of:

- **normal**: Packets are compressed using the packet history for automatic adjustment for best compression.
- **stateless**: Each packet is compressed individually.

**protocols** *protocols*: sets the compression protocol where *protocols* must be one of:

- **deflate**: DEFLATE algorithm
- **mppc**: Microsoft PPP algorithm
- **stac**: STAC algorithm

**ip-header-compression negotiation { detect | force | vj compress-slot-id { both | none | receive | transmit } }**

Default: **force**

**detect**: The local side does not include the Van Jacobson (VJ) Compression option in its IPCP configuration request unless the peer sends an Internet Protocol Control Protocol (IPCP) NAK including a VJ compression option. If the peer requests the VJ compression option in its IPCP request the local side will ACK/NAK.

**force**: The IP header compression negotiation in IPCP happens normally. The local side requests the VJ compression option in its IPCP configure request. If the peer side requests VJ compression in its IPCP request, the local side will ACK/NAK the option.

**vj compress-slot-id [ both | none | receive | transmit ]**: Configures the direction in which VJ slotid compression should be negotiated.

- **both** - If the client proposes VJ slotid compression, accept it and propose slotid compression for the downlink and uplink.
- **none** - If the client proposes VJ slotid compression, NAK the offer, do not propose slotid compression for the downlink.
- **receive** - (Default) If the client proposes VJ slotid compression in the uplink direction accept the configuration.
- **transmit** - Propose VJ slotid compression for uplink.

**ipv4 { disable | enable | passive }**

Default: enable

Controls IPCP negotiation during PPP negotiation.

**disable**: The PDSN does not negotiate IPCP with the mobile.

**enable**: The PDSN negotiates IPCP with the mobile.

**passive**: The PDSN initiates IPCP only when the mobile sends an IPCP request.

**ipv6 { disable | enable | passive }**

Default: enable

Controls IPv6CP negotiation during PPP negotiation.

**disable**: The PDSN does not negotiate IPCP with the mobile.

**enable**: The PDSN negotiates IPCP with the mobile.

**passive**: The PDSN initiates IPCP only when the mobile sends an IPCP request.

**keepalive *seconds***

Default: 30

Specifies the frequency of sending the Link Control Protocol keepalive messages. *seconds* must be either 0 or an integer from 5 through 14400. The special value 0 disables the keepalive messages entirely.

**min-compression-size *min_octets***

Default: 128

Specifies the smallest packet (in octets) to which compression may be applied. *min_octets* must be an integer from 0 through 2000.

**mtu *max_octets***

Default: 1500

Specifies the maximum transmission unit (MTU) [in octets] for packets. *max_octets* must be an integer from 100 through 2000.

**remote-renegotiation disconnect { always | nai-prefix-msid-mismatch }**

Default: Disabled

Terminates the already established PPP sessions if they are renegotiated by the remote side by sending LCP Conf-req/nak/ack. The following termination conditions are available:

- **always**: Automatically disconnects the session.
- **nai-prefix-msid-mismatch**: Disconnects the session only if the MSID of the session does not match NAI-Prefix (prefix before "@" for the NAI). The configuration of the renegotiated (new) NAI is used for the matching process.

**Usage Guidelines**

Adjust packet sizes and compression to improve bandwidth utilization. Each network may have unique characteristics such that determining the best packet size and compression options may require system monitoring over an extended period of time.

**Example**

The following sequence of CLI commands sets PPP parameters for this subscriber:

```
ppp data-compression protocols mode stateless
ppp mtu 500
no ppp data-compression protocols
no ppp keepalive
```

# prepaid 3gpp2

Enables 3GPP2 compliant prepaid billing support for a subscriber to be configured by 3GPP2 attributes sent from a RADIUS server. If not enabled, prepaid attributes received from the RADIUS server are ignored.

**Product**

PDSN

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
prepaid 3gpp2 { accounting [ no-final-access-request ] | duration-quota
final-duration-algorithm { current-time | last-airlink-activity-time |
last-user-layer3-activity-time } | preference { duration | volume } }
default prepaid 3gpp2 { duration-quota final-duration-algorithm |
preference }
no prepaid 3gpp2 accounting
```

**default prepaid 3gpp2 { duration-quota final-duration-algorithm | preference }**

Sets the 3GPP2 Pre-paid settings to the default values.

**duration-quota final-duration-algorithm**: Resets the end of billing duration quota algorithm to the default of current-time.

**preference**: Resets the preference to duration, If both duration and volume attributes are present.

**no prepaid 3gpp2 accounting**

Disables 3GPP2 prepaid accounting. All 3GPP2 Prepaid attributes received from a RADIUS server are ignored.

**accounting [ no-final-access-request ]**

Default: Disabled

Enables 3GPP2 prepaid accounting behavior.

Sets the low-watermark for remaining byte credits. *percentage* is a percentage of the subscriber sessions total credits. When the low-watermark is reached a new RADIUS access-request is sent to the RADIUS server to retrieve more credits. *percentage* must be an integer from 1 through 99.

**no-final-access-request**: Stops sending final online access-request on termination of 3GPP2 prepaid sessions. By default, this option is disabled.

**duration-quota final-duration-algorithm { current-time | last-airlink-activity-time | last-user-layer3-activity-time }**

Defines what behavior marks the end of the billing duration for duration-based quota usage accounting. The default behavior sets the duration quota algorithm to current-time.

Default: current-time

**current-time**: Selects the duration quota as the difference between the session termination timestamp and the session setup timestamp.

**last-airlink-activity-time**: Selects the duration quota as the difference between the last-user-activity timestamp (G17) and the session setup timestamp.

**last-user-layer3-activity-time**: Selects the duration quota as the difference between the timestamp of the last layer-3 packet sent to or received from the user and the session setup timestamp.

**preference { duration | volume }**

If both duration and volume RADIUS attributes are present this keyword specifies which attribute has precedence.

Default: duration

**duration**: The duration attribute takes precedence.

**volume**: The volume attribute takes precedence

## Usage Guidelines

Use this command to enable prepaid support for a default user or for the default user of a domain alias.

### Example

The following command enables 3GPP2 prepaid support for the default user:

```
prepaid 3gpp2 accounting
```

# prepaid custom

Enables custom prepaid billing support for a subscriber to be configured by attributes sent from a RADIUS server. If not enabled, prepaid attributes received from the RADIUS server are ignored. The keywords set prepaid values that are used if the corresponding RADIUS attribute is not present. If the RADIUS attribute is present, it takes precedence over these values.

**Product**

PDSN

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**prepaid custom { accounting | byte-count compressed | low-watermark percent** *percentage* **| renewal interval** *seconds* **} | preference { duration | volume }**

**default prepaid custom { byte-count | low-watermark }**

**no prepaid custom { accounting | byte-count compressed | low-watermark | renewal }**

#### default prepaid custom { byte-count | low-watermark }

Resets custom prepaid settings to the default values.

**byte-count**: Resets to the default of basing the prepaid byte credits on the flow of uncompressed traffic.

**low-watermark**: Disables sending an access request to retrieve more credits when a low watermark is reached.

#### no prepaid custom { accounting | byte-count compressed | low-watermark | renewal}

**byte-count compressed**: The prepaid byte credits are based on the flow of uncompressed traffic. This is the default.

**low-watermark**: Disables the low watermark feature. An access-request is not sent to the RADIUS server until the credits granted for the subscriber session are depleted.

**renewal**: Disables time-based renewals for prepaid accounting.

**accounting**

Default: Disabled

Enables custom prepaid accounting behavior.

**byte-count compressed**

Default: uncompressed.

When compression is used, the prepaid byte credits are based on the flow of compressed traffic. The default is to base the prepaid byte credits on the flow of uncompressed traffic.

**low-watermark percent *percentage***

Default: Disabled.

Sets the low-watermark for remaining byte credits. *percentage* is a percentage of the subscriber sessions total credits. When the low-watermark is reached a new RADIUS access-request is sent to the RADIUS server to retrieve more credits. *percentage* must be an integer from 1 through 99.

**renewal interval *seconds***

Default:

The time in seconds to wait before sending a new RADIUS access-request to the RADIUS server to retrieve more credits. *seconds* must be an integer from 60 through 65535.

**preference { duration | volume }**

If both duration and volume RADIUS attributes are present this keyword specifies which attribute has precedence.

Default: duration

**duration**: The duration attribute takes precedence.

**volume**: The volume attribute takes precedence

**Usage Guidelines**

Use this command to enable prepaid support for a default user or for the default user of a domain alias.

**Example**

The following command enables custom prepaid support for the default user:

```
prepaid custom accounting
```

# prepaid unclassify

This command provides customer specific functionality.

# prepaid voice-push

This command provides customer specific functionality.

# prepaid wimax

Enables WiMAX prepaid accounting for this subscriber. This feature is disabled by default.

**Product**

ASN-GW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**`[ no ] prepaid wimax accounting`**

**no**

Disables WiMAX prepaid accounting for this subscriber.

**Usage Guidelines**

Use this command to enable WiMAX prepaid accounting for this subscriber.

**Example**

The following command enables WiMAX prepaid accounting for this subscriber:

**`prepaid wimax accounting`**

# proxy-dns intercept list-name

Identifies a proxy DNS intercept rules list for the selected subscriber.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description** `[ no ] proxy-dns intercept list-name name`

**no**

Removes the intercept list from the subscribers profile.

**proxy-dns intercept list-name *name***

Specifies a name of a proxy DNS intercept list used for the selected subscriber.

*name* is the name of the intercept list expressed as an alphanumeric string of 1 through 63 characters.

**Usage Guidelines** Use this command to identify a proxy DNS rules list for the selected subscriber. For a more detailed explanation of the HA Proxy DNS Intercept feature, see the **proxy-dns intercept-list** command in the *Context Configuration Mode Commands* chapter.

**Example**

The following command specifies the proxy DNS intercept list named *dns-Intercept-list*:

```
proxy-dns intercept list-name dns-Intercept-list
```

# proxy-mip

Configures support for Proxy Mobile IP for the subscriber.

**Product** PDSN

GGSN

ASN-GW

PDIF

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description** `[ no ] proxy-mip required`

**no**

Disables support for Proxy Mobile IP.

**required**

Enables support for Proxy Mobile IP.

**Usage Guidelines**

When enabled through the session license and feature use key, the system supports Proxy Mobile IP to provide a mobility solution for subscribers with mobile nodes (MNs) capable of supporting only Simple IP.

For subscriber sessions using Proxy Mobile IP, R-P and PPP sessions are established as they would for a Simple IP session. However, the AGW/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN while the MN performs only Simple IP processes.

### Example

The following command enables proxy mobile IP for the current subscriber:

```
proxy-mip required
```

# qos apn-ambr

Configures the rate limit according to the APN-AMBR to do the session level bandwidth control per direction, according to the QoS information provided by the PCRF on the Gx interface.

**Product**

**Important** This command is customer specific. For more information contact your Cisco account representative.

PDSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**qos apn-ambr rate-limit** { **downlink** | **uplink** } [ **burst-size** *bytes* ] [ **violate-action** { **drop** | **lower-ip-precedence** | **transmit** } ] ]

**no qos apn-ambr rate-limit**

### no

Disables the QoS data rate limit configuration for the subscriber.

### downlink

Applies the specified limits and actions to the downlink (to the data coming from the GGSN over the Gn' interface).

### uplink

Applies the specified limits and actions to the uplink (to the data coming from the UE over the IPSec tunnel).

**Important** If this keyword is omitted, the same values are used for all classes.

**burst-size *bytes***

Default: See the *Usage* section for this command

The burst size allowed (in bytes) for peak data rate and committed data rate.

*bytes* must be an integer from 1 through 6000000.

**Important** The minimum value of this parameter should be configured to the greater of the following two values: 1) three times greater than the packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the "bucket" for the configured peak-data-rate. If the committed-data-rate parameter is specified, the burst-size is applied to both the committed and peak rates.

**violate-action { drop | lower-ip-precedence | transmit }**

Default: See the *Usage* section for this command

Specifies the action to take on packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

- **drop**: Drops the packets.
- **lower-ip-precedence**: Transmits the packets after lowering the IP precedence.
- **transmit**: Transmits the packet.

## Usage Guidelines

This command configures the rate limit according to the APN-AMBR to do the session level bandwidth control per direction, according to the QoS information provided by the PCRF on the Gx interface. This command specifies the actions to take on subscriber flows exceeding or violating allowed peak or committed data rates.

### Example

The following example configures the rate limit and burst size according to the APN-AMBR for the uplink direction. Policing is done for the traffic based on PCRF value recieved and traffic is dropped as the violate action is specified as drop.

```
qos apn-ambr rate-limit direction uplink burstsize 1 violate-action drop
```

# qos rate-limit

Configure the action on subscriber traffic flow that violates or exceeds the peak/committed data rate under traffic policing functionality. When configured, the PDG/TTG performs traffic policing for the subscriber session. If the GGSN changes the QoS via an Update PDP Context Request, the PDG/TTG uses the new QoS values for traffic policing.

**Product**

PDG/TTG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**qos rate-limit** { **downlink** | **uplink** } [ **qci** *qci_val* ] [ **burst-size** { *bytes* | **auto-readjust** [ **duration** *dur* ] } ] [ **exceed-action** { **drop** | **lower-ip-precedence** | **transmit** } [ **violate-action** { **drop** | **lower-ip-precedence** | **shape** [ **transmit-when-buffer-full** ] | **transmit** } ] ] | [ **violate-action** { **drop** | **lower-ip-precedence** | **shape** [ **transmit-when-buffer-full** ] | **transmit** } [ **exceed-action** { **drop** | **lower-ip-precedence** | **transmit** } ] ] +

**no qos rate-limit direction { downlink | uplink }** [ **qci** *qci_val* ]

**no**

Disables the QoS data rate limit configuration for the subscriber.

**downlink**

Applies the specified limits and actions to the downlink (to the data coming from the GGSN over the Gn' interface).

**uplink**

Applies the specified limits and actions to the uplink (to the data coming from the UE over the IPSec tunnel).



**Important** If this keyword is omitted, the same values are used for all classes.

**qci *qci_val***

*qci_val* is the QoS Class identifier (QCI) for which the negotiate limit is being set expressed as an integer from 1 through 9. If no qci-val is configured, it will be taken as undefined-qci (same as undefined-qos class).

**burst-size { *bytes* | auto-readjust [ duration *dur* ] }**

Default: See the *Usage* section for this command

The burst size allowed (in bytes) for peak data rate and committed data rate.

*bytes* must be an integer from 1 through 6000000.



**Important** The minimum value of this parameter should be configured to the greater of the following two values: 1) three times greater than the packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the "bucket" for the configured peak-data-rate. If the committed-data-rate parameter is specified, the burst-size is applied to both the committed and peak rates.

**auto-readjust [ duration** *dur* **]** provides the option to calculate the Burst size dynamically while configuring rate-limit. When enabled. the system calculates the burst size using the GGSN QoS-negotiated rate that will be enforced.

Every time there is a change in the rates (due to an updated QoS), the burst sizes will be updated accordingly.

This keyword also provides two different burst sizes. One burst size for peak rate and another for committed rate.

By default this keyword is disabled.

**duration** *dur* specifies the duration of burst in seconds. If the duration is not specified, the default is 1 second. *dur* must be an integer from 1 through 30.

**exceed-action { drop | lower-ip-precedence | transmit }**

Default: See the *Usage* section for this command

Specifies the action to take on packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:

- **drop**: Drops the packets.
- **lower-ip-precedence**: Transmits the packets after lowering the ip-precedence.
- **transmit**: Transmits the packets.

**violate-action { drop | lower-ip-precedence | transmit }**

Default: See the *Usage* section for this command

Specifies the action to take on packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

- **drop**: Drops the packets.
- **lower-ip-precedence**: Transmits the packets after lowering the IP precedence.
- **transmit**: Transmits the packet after lowering the IP precedence.

**shape [transmit-when-buffer-full]**: Enables traffic shaping and buffers user packets when subscriber traffic violates the allowed peak/committed data rate. The **[transmit-when-buffer-full]** keyword allows the packets to be transmitted when buffer memory is full.

**transmit**: Transmits the packet

## Usage Guidelines

This command configures APN quality of service (QoS) data rate shaping through traffic policing. This command specifies the actions to take on subscriber flows exceeding or violating allowed peak or committed data rates. The shaping function also provides an enhanced function to buffer the excessive user packets and send them to the subscriber when subscriber traffic drops below the committed or peak data rate limit.

**Important** The buffering of user packets in traffic shaping does not apply for real-time traffic.

**Important** If the exceed/violate action is set to "lower-ip-precedence", this command may override the configuration of the **ip qos-dscp** command in the GGSN service Configuration mode for packets from the GGSN to the PDG/TTG. In addition, the GGSN service **ip qos-dscp** command configuration can override the APN setting for packets from the GGSN to the Internet. Therefore, it is recommended that this command not be used in conjunction with this action.

The command can be entered multiple times to specify different combinations of direction and class. If this command is not configured at all, the GGSN does not perform traffic policing or QoS negotiation with the PDG/TTG; it accepts all of the PDG/TTG-provided values for the PDP context.

**Important** This command should be used in conjunction with the max-contexts command to limit the maximum possible bandwidth consumption by the APN.

For additional information on QoS traffic shaping and policing, see the *System Administration Guide.*

### Default Values

The following table displays the default values for each of the traffic classes:

| | |
|---|---|
| **Class: Conversational** | |
| Downlink Traffic: Disabled<br>Peak Data Rate (in bps): 16000000<br>Committed Data Rate (in bps): 16000000<br>Exceed Action: lower-ip-precedence<br>Violate Action: drop | Uplink Traffic: Disabled<br>Peak Data Rate (in bps): 8640000<br>Committed Data Rate (in bps): 8640000<br>Exceed Action: lower-ip-precedence<br>Violate Action: drop |
| **Class: Streaming** | |
| Downlink Traffic: Disabled<br>Peak Data Rate (in bps): 16000000<br>Committed Data Rate (in bps): 16000000<br>Exceed Action: lower-ip-precedence<br>Violate Action: drop | Uplink Traffic: Disabled<br>Peak Data Rate (in bps): 8640000<br>Committed Data Rate (in bps): 8640000<br>Exceed Action: lower-ip-precedence<br>Violate Action: drop |
| **Class: Interactive, Traffic Handling Priority: 1** | |

| | |
|---|---|
| Downlink Traffic: Disabled<br>Peak Data Rate (in bps): 16000000<br>Committed Data Rate (in bps): n/a<br>Exceed Action: n/a<br>Violate Action: drop | Uplink Traffic: Disabled<br>Peak Data Rate (in bps): 8640000<br>Committed Data Rate (in bps): n/a<br>Exceed Action: n/a<br>Violate Action: drop |
| **Class: Interactive, Traffic Handling Priority: 2** | |
| Downlink Traffic: Disabled<br>Peak Data Rate (in bps): 16000000<br>Committed Data Rate (in bps): n/a<br>Exceed Action: n/a<br>Violate Action: drop | Uplink Traffic: Disabled<br>Peak Data Rate (in bps): 8640000<br>Committed Data Rate (in bps): n/a<br>Exceed Action: n/a<br>Violate Action: drop |
| **Class: Interactive, Traffic Handling Priority: 3** | |
| Downlink Traffic: Disabled<br>Peak Data Rate (in bps): 16000000<br>Committed Data Rate (in bps): n/a<br>Exceed Action: n/a<br>Violate Action: drop | Uplink Traffic: Disabled<br>Peak Data Rate (in bps): 8640000<br>Committed Data Rate (in bps): n/a<br>Exceed Action: n/a<br>Violate Action: drop |
| **Class: Background** | |
| Downlink Traffic: Disabled<br>Peak Data Rate (in bps): 16000000<br>Committed Data Rate (in bps): n/a<br>Exceed Action: n/a<br>Violate Action: drop | Uplink Traffic: Disabled<br>Peak Data Rate (in bps): 8640000<br>Committed Data Rate (in bps): n/a<br>Exceed Action: n/a<br>Violate Action: drop |

## Usage Guidelines

This command configures the APN quality of service (QoS) data rate shaping through traffic policing/shaping. This command specifies the actions to take on subscriber flows exceeding or violating allowed peak/committed data rates. The shaping function also provides an enhanced function to buffer the excessive user packets and send them to the subscriber when subscriber traffic drops below the committed or peak data rate limit.

**Important** The buffering of user packets in traffic shaping does not apply for real-time traffic.

**Important** If the exceed/violate action is set to "lower-ip-precedence", this command may override the configuration of the **ip qos-dscp** command in the GGSN service configuration mode for packets from the GGSN to the SGSN. In addition, the GGSN service **ip qos-dscp** command configuration can override the APN setting for packets from the GGSN to the Internet. Therefore, it is recommended that command not be used in conjunction with this action.

The command can be entered multiple times to specify different combinations of direction and class. If this command is not configured at all, the GGSN does not perform traffic policing or QoS negotiation with the SGSN (i.e. it accepts all of the SGSN-provided values for the PDP context.

**Important** This command should be used in conjunction with the **max-contexts** command to limit the maximum possible bandwidth consumption by the APN.

For additional information on QoS traffic shaping and policing, see the *System Administration Guide*.

### Default Values:

The following table displays the default values for each of the traffic classes:

***Table 1: no title 754***

| | |
|---|---|
| **Class: Conversational** | |
| Downlink Traffic: Disabled<br>Peak Data Rate (in bps): 16000000<br>Committed Data Rate (in bps): 16000000<br>Burst Size (in bytes): 65535<br>Exceed Action: lower-ip-precedence<br>Violate Action: drop | Uplink Traffic: Disabled<br>Peak Data Rate (in bps): 8640000<br>Committed Data Rate (in bps): 8640000<br>Burst Size (in bytes): 65535<br>Exceed Action: lower-ip-precedence<br>Violate Action: drop |
| **Class: Streaming** | |
| Downlink Traffic: Disabled<br>Peak Data Rate (in bps): 16000000<br>Committed Data Rat (in bps): 16000000<br>Burst Size (in bytes): 65535<br>Exceed Action: lower-ip-precedence<br>Violate Action: drop | Uplink Traffic: Disabled<br>Peak Data Rate (in bps): 8640000<br>Committed Data Rate (in bps): 8640000<br>Burst Size (in bytes): 65535<br>Exceed Action: lower-ip-precedence<br>Violate Action: drop |
| **Class: Interactive, Traffic Handling Priority: 1** | |

| | |
|---|---|
| Downlink Traffic: Disabled<br>Peak Data Rate (in bps): 16000000<br>Committed Data Rate (in bps): n/a<br>Burst Size (in bytes): 65535<br>Exceed Action: n/a<br>Violate Action: drop | Uplink Traffic: Disabled<br>Peak Data Rate (in bps): 8640000<br>Committed Data Rate (in bps): n/a<br>Burst Size (in bytes): 65535<br>Exceed Action: n/a<br>Violate Action: drop |
| **Class: Interactive, Traffic Handling Priority: 2** | |
| Downlink Traffic: Disabled<br>Peak Data Rate (in bps): 16000000<br>Committed Data Rate (in bps): n/a<br>Burst Size (in bytes): 65535<br>Exceed Action: n/a<br>Violate Action: drop | Uplink Traffic: Disabled<br>Peak Data Rate (in bps): 8640000<br>Committed Data Rate (in bps): n/a<br>Burst Size (in bytes): 65535<br>Exceed Action: n/a<br>Violate Action: drop |
| **Class: Interactive, Traffic Handling Priority: 3** | |
| Downlink Traffic: Disabled<br>Peak Data Rate (in bps): 16000000<br>Committed Data Rate (in bps): n/a<br>Burst Size (in bytes): 65535<br>Exceed Action: n/a<br>Violate Action: drop | Uplink Traffic: Disabled<br>Peak Data Rate (in bps): 8640000<br>Committed Data Rate (in bps): n/a<br>Burst Size (in bytes): 65535<br>Exceed Action: n/a<br>Violate Action: drop |
| **Class: Background** | |
| Downlink Traffic: Disabled<br>Peak Data Rate (in bps): 16000000<br>Committed Data Rate (in bps): n/a<br>Burst Size (in bytes): 65535<br>Exceed Action: n/a<br>Violate Action: drop | Uplink Traffic: Disabled<br>Peak Data Rate (in bps): 8640000<br>Committed Data Rate (in bps): n/a<br>Burst Size (in bytes): 65535<br>Exceed Action: n/a<br>Violate Action: drop |

**Important** If a "Subscribed" traffic class is received, the system changes the class to "Background" and sets the following parameters: The uplink and downlink guaranteed data rates are set to 0. If the received uplink or downlink data rates are 0 and traffic policing is disabled, the default of 64 kbps is used. When enabled, the APN configured values are used. If the configured value for downlink max data rate is larger than can fit in an R4 QoS profile, the default of 64 kbps is used. If either the received uplink or downlink max data rates is non-zero, traffic policing is employed if enabled for the "Background" class. The received values are used for responses when traffic policing is disabled.

To calculate the burst size dynamically a new optional keyword **auto-readjust** [ **duration** *dur* ] is provided with **burst-size** keyword. By default the burst size is fixed if defined in bytes with this command. In other words irrespective of the rate being enforced, burst-size fixed as given in the **burst-size** *bytes* parameter.

For the need of variable burst size depending on the rate being enforced this new keyword **auto-readjust** [ **duration** *dur* ] is provided. Use of this keyword enables the calculation of burst size as per token bucket algorithm calculation as T=B/R, where T is the time interval, B is the burst size and R is the Rate being enforced.

It also provides different burst size for Peak and Committed data rate-limiting.

If **auto-readjust** keyword is not used a fixed burst size must be defined which will be applicable for peak data rate and committed data rate irrespective of rate being enforced.

If **auto-readjust** keyword is provided without specifying the duration a default duration of 1 second will be taken for burst size calculation.

### Example

The following command lowers the IP precedence when the committed-data-rate and the peak-data-rate are violated in uplink direction:

```
qos rate-limit direction uplink violate-action lower-ip-precedence
```

The following command buffers the excess user packets when the subscriber traffic violates the configured peak or committed data-rate bps in uplink direction. Once the peak/committed data rate for that subscriber goes below the configured limit it transmit them. It also transmits them if buffer memory is full:

```
qos rate-limit direction uplink violate-action shape
transmit-when-buffer-full
```

# qos traffic-police

Enables and configures traffic policing through bandwidth limitations and action for the subscriber traffic if it exceeds or violates the peak or committed data rate. Uplink and downlink limits are configured separately.

**Product**

PDSN

HA

GGSN

ASN-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
qos traffic-police direction { downlink | uplink } [ burst-size bytes ] [
 committed-data-rate bps ] [ exceed-action { drop | lower-ip-precedence |
 transmit } ] [ peak-data-rate bps ] [ violate-action { drop |
lower-ip-precedence | transmit } ]
```

```
no qos traffic-police direction { downlink | uplink }
```

**downlink**

Applies the specified limits and actions to the downlink (data to the subscriber).

**uplink**

Apply the specified limits and actions to the uplink (data from the subscriber).

**burst-size *bytes***

Default: 3000

Specifies the allowed peak burst size allowed in bytes.

*bytes* must be an integer from 0 through 4294967295.

**Important** This parameter should be configured to at least the greater of the following two values: 1) three times greater than packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the "bucket" for the configured peak-data-rate.

**committed-data-rate *bps***

Default: 144000

Specifies the committed data rate (guaranteed-data-rate) in bits per second (bps).

*bps* must be an integer from 0 through 4294967295.

**exceed-action { drop | lower-ip-precedence | transmit }**

Default: lower-ip-precedence

Specifies the action to take on packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:

**drop**: Drops the packet

**lower-ip-precedence**: Transmits the packet after lowering the ip-precedence

**transmit**: Transmits the packet

**peak-data-rate *bps***

Default: 256000

Specifies the peak data-rate for the subscriber in bits per second (bps).

*bps* must be an integer from 0 through 4294967295.

**violate-action { drop | lower-ip-precedence | transmit }**

Default: drop

Specifies the action to take on packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

**drop**: Drops the packet

**lower-ip-precedence**: Transmits the packet after lowering the IP precedence

**transmit**: Transmits the packet

**no**

Disables traffic policing in the specified direction for the current subscriber.

**Usage Guidelines**

Use this command to limit the bandwidth a subscriber uses in the uplink and downlink directions.

**Important** If the exceed/violate action is set to "lower-ip-precedence", the TOS value for the outer packet becomes "best effort" for packets that exceed/violate the traffic limits regardless of what the **ip user-datagram-tos copy** command is configured to. In addition, the "lower-ip-precedence" option may also override the configuration of the **ip qos-dscp** command. Therefore, it is recommended that command not be used when specifying this option.

Details on the QoS traffic policing can be found in the *System Administration Guide*.

**Example**

The following command sets an uplink peak data rate of *128000* bps and lowers the IP precedence when the committed-data-rate and the peak-data-rate are exceeded:

```
qos traffic-police direction uplink peak-data-rate 128000 violate-action
 lower-ip-precedence
```

The following command sets a downlink peak data rate of *256000* bps and drops packets when the committed-data-rate and the peak-data-rate are exceeded:

```
qos traffic-police direction downlink peak-data-rate 256000 violate-action
 drop
```

# qos traffic-shape

Enables and configures traffic shaping functionality when buffering the data packets during congestion or when the subscriber exceeds the configured peak or committed data rate limit. The system buffers the data

packets during an instantaneous burst and deliver them to the subscriber when traffic flow drops below the peak or committed data rate. Uplink and downlink traffic shaping are configured separately.



**Important** This feature is NOT supported for real-time traffic.

**Product**

PDSN

HA

GGSN

ASN-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**qos traffic-shape direction { downlink | uplink } [ burst-size** *bytes* **] [ committed-data-rate** *bps* **] [ exceed-action { drop | lower-ip-precedence | transmit } ] [ peak-data-rate** *bps* **] [ violate-action { drop | lower-ip-precedence | buffer [ transmit-when-buffer-full ] | transmit } ] +**

**no qos traffic-shape direction { downlink | uplink }**

**downlink**

Applies the specified limits and actions to the downlink (data to the subscriber).

**uplink**

Applies the specified limits and actions to the uplink (data from the subscriber).

**burst-size *bytes***

Default: 3000

Specifies the allowed peak burst size in bytes.

*bytes* must be an integer from 0 through 4294967295.



**Important** It is recommended that this parameter be configured to at least the greater of the following two values: 1) three times greater than packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the "bucket" for the configured peak-data-rate.

**committed-data-rate *bps***

Default: 144000

Specifies the committed data rate (guaranteed-data-rate) in bits per second (bps).

*bps* must be an integer from 0 through 4294967295.

**exceed-action { drop | lower-ip-precedence | transmit }**

Default: lower-ip-precedence

Specifies the action to take on packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:

**drop**: Drops the packet

**lower-ip-precedence**: Transmits the packet after lowering the ip-precedence

**transmit**: Transmits the packet

**peak-data-rate *bps***

Default: 256000

Specifies the peak data-rate for the subscriber in bits per second (bps).

*bps* must be an integer from 0 through 4294967295.

**violate-action { drop | lower-ip-precedence | buffer [transmit-when-buffer-full] | transmit }**

Default: See the *Usage* section for this command

The action to take on the packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

**drop**: Drops the packet

**lower-ip-precedence**: Transmits the packet after lowering the IP precedence

**buffer [transmit-when-buffer-full]**: Enables traffic shaping and buffers user packets when subscriber traffic violates the allowed peak/committed data rate. The **[transmit-when-buffer-full]** keyword allows the packet to be transmitted when buffer memory is full.

**transmit**: Transmits the packet

**+**

More than one of the above keywords can be entered within a single command.

**no**

Disables traffic policing for the specified direction for the current subscriber.

## Usage Guidelines

Use this command to provide the traffic shaping function to a subscriber in the uplink and downlink directions. This feature is providing a traffic flow control different to QoS traffic policing. When a subscriber violates or exceeds the peak data rate instead of dropping the packets, as in QoS traffic policing, this feature buffers subscriber data packets and sends the buffered data when the traffic flow is low or not in congestion state.

**Important** If the exceed or violate action is set to "lower-ip-precedence", the TOS value for the outer packet becomes "best effort" for packets that exceed or violate the traffic limits regardless how the **ip user-datagram-tos copy** command is configured. In addition, the "lower-ip-precedence" option may also override the configuration of the **ip qos-dscp** command. Therefore, this command should not be used when specifying this option.

Details on the QoS traffic policing functionality is located in the System Administration Guide.

### Example

The following command sets an uplink peak data rate of *128000* bps and lowers the IP precedence when the committed-data-rate and the peak-data-rate are exceeded:

```
qos traffic-shape direction uplink peak-data-rate 12800 violate-action
lower-ip-precedence
```

The following command buffers the excess user packets when the subscriber traffic violates the configured peak-data-rate *256000* bps in downlink direction. Once the peak/committed data rate for that subscriber goes below the configured limit it transmit them. It also transmits them if buffer memory is full:

```
qos traffic-shape direction downlink peak-data-rate 256000 violate-action
 buffer transmit-when-buffer-full
```

# radius accounting

Sets the RADIUS accounting parameters for the subscriber or domain. This command takes precedence over the similar Context Configuration command and is disabled by default.

**Product**

All

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
radius accounting { interim { interval-timeout timeout | normal | suppress
 } | ip remote-address list-id list_id | mode { session-based |
access-flow-based { none | auxillary-flows | all-flows | main-a10-only }
 } | start { normal | suppress } | stop { normal | suppress } }
```

```
no radius accounting { ip remote-address list-id list_id | interim [
interval-timeout ] }
```

**interim { interval-timeout *timeout* | normal | suppress }**

**interval-timeout** *timeout*: Indicates the time (in seconds) between updates to session counters (log file on RADIUS or AAA event log) during the session. *timeout* must be an integer from 50 to 40000000.



**Caution** Interim interval settings received from the RADIUS server take precedence over this setting on the system. While the low limit of this setting on the system is a minimum of 50 seconds, the low limit setting on the RADIUS server can be as little as 1 second. To avoid increasing network traffic unnecessarily and potentially reducing network and system performance, do not set this parameter to a value less than 50 on the RADIUS server.

**normal**: If RADIUS accounting is enabled, sends this Acct-Status-Type message when required by normal operation

**suppress**: If RADIUS accounting is enabled, suppresses the sending of this Acct-Status-Type message.

**ip remote-address list-id *list_id***

Specifies the identification number of the IP address list to use for the subscriber for remote address-based accounting.

*list_id*: Specifies the RADIUS accounting remote IP address list identifier for remote-address accounting for the subscriber. *list_id* must be an integer from 1 through 65535.

This command is used as part of the Remote Address-based accounting feature and associates the subscriber with a list of remote addresses. Remote address accounting data is collected each time the subscriber communicates with any of the addresses specified in the list.

Remote address lists are configured using the **list** keyword in the **radius accounting ip remote-address** command in the Context Configuration mode.

**mode { session-based | access-flow-based { none | auxillary-flows | all-flows | main-a10-only } }**

Default: **session-based**

Specifies if the radius accounting mode is either session-based or access-flow-based.

**session-based**: configures session-based RADIUS accounting behavior for the subscriber - which means a single radius accounting message generated for the subscriber session not separate accounting messages for individual A10 connections or flows.

**access-flow-based**: configures access-flow-based RADIUS accounting behavior for the subscriber. This offers flexibility by generating separate accounting messages for flows and A10 sessions.

- **all-flows**: Generates separate RADIUS accounting messages per access flow. Separate accounting messages are not generated for data path connections. (For example, separate messages are not sent for the main A10 or auxiliary connections.).
- **auxillary-flows**: Generates RADIUS accounting records for the main data path connection and for access-flows for all auxiliary data connections. (For example, separate RADIUS accounting messages are generated for the main A10 session and for access-flows within auxiliary A10 connections. The main A10 session accounting does not include octets or other accounting information from the auxiliary flows.)
- **main-a10-only**: Configures access-flow-based single accounting messages (for example only single start/interim/stop) are generated for the main A-10 flows only.

- **none**: Generates separate RADIUS accounting messages for all data path connections (for example, PDSN main or auxiliary A10 connections) but not for individual access-flows. This is essentially A10 connection-based accounting.

**start { normal | suppress }**

**normal**: If RADIUS accounting is enabled, sends this Acct-Status-Type message when required by normal operation

**suppress**: If RADIUS accounting is enabled, suppresses the sending of this Acct-Status-Type message.

**stop { normal | suppress }**

**normal**: If RADIUS accounting is enabled, sends this Acct-Status-Type message when required by normal operation

**suppress**: If RADIUS accounting is enabled, suppresses the sending of this Acct-Status-Type message.

**no**

**ip remote-address list-id** *list_id*: Deletes the entry for the specified *list_id.*

**interim [ interval-timeout ]**: Disables the interim interval setting.

**Usage Guidelines**

Use this command to allow a per-domain setting for the RADIUS accounting.

**Example**

Set the accounting interim interval to one minute (*60* seconds) for all sessions that use the current subscriber configuration:

```
radius accounting interim interval-timeout 60
```

Do not send RADIUS interim accounting messages:

```
radius accounting interim suppress
```

Sets the accounting message start normal for main A-10 flows only.

```
radius accounting mode main-a10-only start normal
```

# radius group

Applies a RADIUS server group at the subscriber level for AAA functionality.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**radius group** *group_name*

**{ default | no } radius group**

**radius *group_name***

Specifies the name of the server group that is used for authentication and/or accounting for the specific subscriber. *group_name* must be an alphanumeric string of 1 through 63 characters. It must have been preconfigured within the same context of subscriber.

**default**

Sets or restores the default RADIUS server group specified at the context level or in the default subscriber profile.

**no**

Disables the applied RADIUS group for specific subscriber.

**Usage Guidelines**

This feature provides the RADIUS configurables under radius group node. Instead of having a single list of servers per context, this feature configures multiple server groups within a context and applies individual RADIUS server group for subscriber in that context. Each server group consists of a list of AAA servers.

IF no RADIUS group is applied for this subscriber or the default subscriber profile, the default server group available at context level is used for accounting and authentication of the subscriber.

**Example**

Following command applies a previously configured RADIUS server group named *star1* to a subscriber within the specific context:

```
radius group star1
```

Following command disables the applied RADIUS server group for the specific subscriber.

```
no radius group
```

# radius returned-framed-ip-address

Sets the policy whether or not to reject a call when the RADIUS server supplies 255.255.255.255 as the framed IP address and the MS does not supply an address.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**radius returned-framed-ip-address 255.255.255.255-policy { accept-call-when-ms-ip-not-supplied | reject-call-when-ms-ip-not-supplied }**

**default radius returned-framed-ip-address 255.255.255.255-policy**

**accept-call-when-ms-ip-not-supplied**

Accepts calls when the RADIUS server supplies framed IP address as 255.255.255.255 and the MS does not supply an address.

**reject-call-when-ms-ip-not-supplied**

Rejects calls when the RADIUS server supplies framed IP address as 255.255.255.255 and the MS does not supply an address.

**default**

Sets the policy to its default of rejecting calls when the RADIUS server supplies framed IP address as 255.255.255.255 and the MS does not supply an address.

**Usage Guidelines**

Use this command to set the behavior for the current subscriber when the RADIUS server supplies 255.255.255.255 as the framed IP address and the MS does not supply an address.

**Example**

The following command sets the subscriber profile to reject calls when the RADIUS server supplies framed IP address as 255.255.255.255 and the MS does not supply an address:

**radius returned-framed-ip-address 255.255.255.255-policy reject-call-when-ms-ip-not-supplied**

# radius rulebase-format

This command enables/disables the Rulebase Concatenation feature at subscriber level. This feature is used to merge the prepaid attribute and SN1-Rulebase as a new rulebase and then apply the new rulebase to the session. If the Rulebase Concatenation feature is not enabled, the last received rulebase is applied to the session.

**Important** This command is license dependent. For more information, contact your Cisco account representative.

**Product**

GGSN

PDSN

P-GW

**Privilege**

Security Administrator, Administrator

## Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

## Syntax Description

**radius rulebase-format { custom1 | standard }**

**default radius rulebase-format standard**

### default

Disables the Rulebase Concatenation feature. The default setting is **standard**.

### custom1

Specifies the rulebase as a custom value derived from multiple RADIUS attributes in the RADIUS Access-Accept response message.

### standard

Specifies the rulebase as a single attribute value as obtained in RADIUS Access-Accept response message. This is the default setting.

## Usage Guidelines

Currently, the Wireless Mobile Private Network (MPN) configures a dedicated rulebase per service. The Enterprise that utilizes this service has the rulebase per subscriber in 3G or signaled from AAA server with SN1-Rulebase attribute. In the case of a prepaid service, the rulebase name will be the customer-specific prepaid policy attribute received from the AAA server.

When both the RADIUS attributes are received, the last received attribute is considered and applied to the subscriber session. This CLI command is used to merge prepaid attribute and SN1-Rulebase as a new rulebase and then apply the new rulebase to the session on the gateway.



**Important** Rulebase Concatenation is a customer-specific feature and it requires a valid license to enable the feature. For more information, contact your Cisco account representative.

In 18 and earlier releases, rulebase was a single attribute value as obtained in the RADIUS Access-Accept response message. That is, only one rulebase can be applied with either SN1-Rulebase AVP or customer-specific prepaid policy AVP, whichever comes last.

In 19 and later releases, when both the attributes are received, the rulebase name will be a concatenation of the attributes as received in the Access-Accept response message. If only one of the attributes is received, the current behavior is applicable i.e. the last received attribute will be selected as the rulebase and it will be applied to the session.

If the concatenated rulesbase is not matching with the rulebase configured on the gateway, and/or if both the attributes are present more than once, then the session is rejected.

This feature implementation helps the MPN to customize the rulebase and combine prepaid service with additional services like Service Based Access (SBA).

### Example

The following command merges the RADIUS attributes and installs the new concatenated rulebase.

```
radius rulebase-format custom1
```

# rohc-profile-name

Identifies the robust header compression (RoHC) profile configuration that will be applied to bearer sessions belonging to this subscriber.

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**rohc-profile-name** *name*

***name***

Specifies the name of the RoHC profile that the system will use to apply header compression and decompression parameters to bearer session data for this subscriber. *name* must be an existing RoHC profile expressed as an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to specify a RoHC configuration profile to be applied to bearer sessions belonging to this subscriber. RoHC profiles are configured through the Global Configuration Mode using the **rohc-profile** command.

### Example

The following command specifies that the RoHC profile named *rohc-cfg1* is to be applied to all bearer sessions belonging to this subscriber:

```
rohc-profile-name rohc-cfg1
```

# secondary ip pool

Specifies a secondary IP pool to be used as backup pool for Network Address Translation (NAT).

**Important** This command requires the purchase and installation of a license. Please contact your Cisco sales representative for more information.

**Product** NAT

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**`secondary ip pool`** *`pool_name`*

**`no secondary ip pool`**

**no**

Removes the previous secondary IP pool configuration.

**secondary ip pool *pool_name***

Specifies the secondary IP pool name.

*pool_name* must be an alphanumeric string of 1 through 31 characters.

**Usage Guidelines** Use this command to configure a secondary IP pool for NAT subscribers, which is not overwritten by the RADIUS supplied list. The secondary pool will be appended to the RADIUS supplied IP pool list or subscriber template provided IP pool list, as applicable, during call setup.

**Example**

The following command configures a secondary IP pool named *test123*:

**`secondary ip pool test123`**

# send-destination-pgw

Configures how the HSGW selects a P-GW address for the "Destination-PGW" AVP.

**Product** HSGW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**send-destination-pgw { all | explicit-only | implicit-only }**

**no send-destination-pgw**

**no**

Removes the configuration for this command.

**all**

P-GW address is obtained either by explicit or implicit mechanism.

**explicit-only**

The UE performs LCP/PPP procedures, and attaches with a specific APN. The HSGW queries the AAA over the STa interface and receives a MIP6-Agent-Info AVP that includes a sub AVP of Destination-Host. The HSGW copies the value of the Destination-Host AVP in the Destination-PGW AVP which is sent in the CCR-I to the PCRF.

**implicit-only**

The UE performs LCP/PPP procedures, and attaches with a specific APN. The AAA does not return the P-GW to use, so the HSGW performs NAPTR procedures to determine the P-GW which will be used.

**Usage Guidelines**

Use this command to configure how the HSGW selects a P-GW address for the "Destination-PGW" AVP. This AVP is sent over Gxa to the PCRF.

**Example**

Configures the HSGW to select either implicit or explicit selection method.

**send-destination-pgw all**

# service-option

**Product**

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] service-option** *number*

**no**

Removes the specified service option from the subscriber configuration.

***number***

Specifies the service option the subscriber is allowed to use. *number* must be a legitimate service option and be an integer value from 0 through 1000.

**Usage Guidelines** Up to seven service options can be specified for this subscriber.

**Example**

# simultaneous

Enables or disables the simultaneous use of both Mobile and Simple IP services.

**Product** PDSN

FA

HA

ASN-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description** **[ no ] simultaneous simple-and-mobile-ip**

**no**

Disables the simultaneous use.

**Usage Guidelines** Subscribers with mobile devices that concurrently support mobile and simple IP services require this option to be set.

**Example**

The following command enables simultaneous use of both Simple and Mobile IP services:

**simultaneous simple-and-mobile-ip**

# timeout absolute

Configures the maximum duration of the session before the system automatically terminates the session.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**`timeout absolute`** *`seconds`*

**`{ default | no } timeout absolute`**

**default | no**

Indicates the timeout specified is to be returned to its default behavior. If a timeout value is not specified, all timeouts are set to their default values.

**timeout absolute**

Default: 0

Specifies the absolute maximum time a session may exist (in seconds) in any state (active or dormant).

***seconds***

Specifies the maximum amount of time (in seconds) before the specified timeout action is activated. *seconds* must be an integer from 0 through 4294967295. The special value 0 disables the timeout specified.

**Usage Guidelines**

Use this command to set the absolute maximum time a session may exist in any state.

**Example**

The following command configures the absolute maximum timeout to 18000 seconds (300 minutes):

**`timeout absolute 18000`**

# timeout idle

Configures the idle timeout duration for the long duration timer associated with a subscriber session.

**Product**

All

**Privilege**

Security Administrator, Administrator

## Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

## Syntax Description

**timeout idle** *idle_dur* **[ micro-checkpoint-deemed-idle** *[ time_in_seconds ]* **| micro-checkpoint-periodicity** *time_in_seconds* **]**

**{ default | no } timeout idle**

### default | no

Indicates the timeout specified is to be returned to its default behavior. If no specific timeout is specified, then all are set to their default behavior.

### timeout idle

Default: 0

Specifies the maximum duration of the session (in seconds) can remain idle before the system automatically terminates the session due to inactivity.

### *idle_dur*

Specifies the maximum amount of time (in seconds) before the specified timeout action is activated. *idle_dur* must be an integer from 0 through 2147483647. The special value 0 disables the timeout specified.

### micro-checkpoint-deemed-idle *time_in_seconds*

Configures micro-checkpoint duration when UE transitions from Idle to Active and vice versa. *time_in_seconds* must be an integer from 10 through 1000. Default: 180.



**Important** Micro-checkpoint-deemed-idle value should be less than idle timeout value.

### micro-checkpoint-periodicity *time_in_seconds*

Configures periodic idle seconds micro checkpoint timer on a per-subscriber basis. Idle seconds micro checkpoints are sent at the configured regular intervals to the standby chassis; otherwise, they are sent at intervals of 10 seconds, which is the default value.*time_in_seconds* must be an integer value in the range from 10 through 10000.Default: 10.



**Important** Micro-checkpoint-periodicity value should be less than idle timeout value.

## Usage Guidelines

Use this command to set the idle time duration, micro-checkpoint-deemed-idle and micro-checkpoint-periodicity timer for a subscriber session to identify a dormant session.

**Important** On the fly change from **micro-checkpoint-deemed-idle** to **micro-checkpoint-periodicity**, and vice-versa, is not supported.

### Example

The following command sets the idle timeout duration to 60 seconds:

```
timeout idle 60
```

The following command sets the idle timeout duration to 20 seconds and micro-checkpoint-deemed-idle to 15 seconds:

```
timeout idle 20 micro-checkpoint-deemed-idle 15
```

# timeout long-duration

Configures the long duration timeout and optionally the inactivity duration of HA subscriber session.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**timeout long-duration** *ldt_timeout* **[ inactivity-time** *inact_timeout* **]**

**[ no | default ]timeout long-duration**

#### no

Indicates the timeout specified is to be returned to its default behavior. If no specific

timeout is specified then all are set to their default behavior.

#### long-duration *ldt_timeout*

Default: 0

Designates the maximum duration of the session (in seconds) before the system automatically reports/terminates the session.

*ldt_timeout* must be a value in the range from 0 through 4294967295. The special value 0 disables the timer.

#### inactivity-time *inact_timeout*

Specifies the maximum amount of time (in seconds) before the specified session is marked as dormant.

*inact_timeout* must be a value in the range from 0 through 4294967295. The special value 0 disables the inactivity time specified.

**Usage Guidelines**

Use this command to set the long duration timeout period and inactivity timer for subscriber sessions. Reduce the idle timeout to free session resources faster for use by new requests.

Refer to the **long-duration-action detection** and **long-duration-action disconnection** commands for more information.

### Example

The following command sets the long duration timeout duration to *300* seconds and inactivity timer for subscriber session to *45* seconds:

```
timeout long-duration 300 inactivity-time 45
```

# tpo policy

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

# tunnel address-policy

Specifies the policy for address allocation and validation for all tunneled calls (IP-IP, IP-GRE) except L2TP calls. With this command enabled, GGSN IP address validation could be disabled for specified incoming calls.

For GGSN systems, this command can also be specified in the APN Configuration mode (**tunnel address-policy**) which would mean the system defers to the old **l3-to-l2-tunnel address policy** command for calls coming through L2TP tunnels.

**Product**

PDSN

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**tunnel address-policy { alloc-only | alloc-validate | no-alloc-validate }**

**default tunnel address-policy**

### alloc-only

Allocates IP addresses locally without validation.

#### alloc-validate

Default.

The VPN Manager allocates and validates all incoming IP addresses from a static pool of IP addresses.

#### no-alloc-validate

No IP address assignment or validation is done for calls coming in via L3 tunnels. Incoming static IP addresses are passed. This option allows for the greatest flexibility.

#### default

Resets the tunnel address-policy to **alloc-validate**.

**Usage Guidelines**

This command supports scalable solutions for Corporate APN deployment as many corporations handle their own IP address assignments. In some cases this is done to relieve the customer or the mobile operators from the necessity of reconfiguring the range of IP addresses for the IP pools at the GGSN.

#### Example

The following command resets the IP address validation policy to validate against a static pool of address:

```
default tunnel address-policy
```

The following command disables IP address validation for calls coming through tunnels:

```
tunnel address-policy no-alloc-validate
```

# tunnel gre

Configures Generic Routing Encapsulation (GRE) tunnel parameters for the current subscriber.

**Product**

PDSN

GGSN

ASN-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**tunnel gre peer-address** *peer_address* **local-address** *local_addr* **[ preference** *num* **]**

**no tunnel gre peer-address** *peer_address*

**peer-address *peer_address***

Specifies the IP address of the external gateway terminating the GRE tunnel.

**local-address *local_addr***

Specifies the IP address of the interface in the destination context originating the GRE tunnel.

**preference *num***

Default: 1

Assigns a preference to the tunnel.

*num* can be an integer from 1 through 128.

**Important** Only one GRE tunnel per subscriber is supported. Therefore, the preference should always be set to "1".

**no**

Disables GRE tunneling for the current subscriber.

**Usage Guidelines** Subscriber IP payloads are encapsulated with IP/GRE headers and tunneled by the AGW to an external gateway.

**Example**

The following command configures the system to encapsulate subscriber traffic using GRE and tunnel it from a local address of *192.168.1.100* to a gateway with an IP address of *192.168.1.225*:

```
tunnel gre peer-address 192.168.1.225 local-address 192.168.1.100
preference 1
```

# tunnel ipip

Configures IP-in-IP tunnelling parameters for the current subscriber.

**Product** PDSN

GGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**tunnel ipip peer-address** *peer_address* **local-address** *local_addr* **[ preference** *num* **]**

**no tunnel ipip**

**peer-address *peer_address***

Specifies the IP address of the external gateway terminating the IP-in-IP tunnel.

**local-address *local_addr***

Specifies the IP address of the interface in the destination context originating the IP-in-IP tunnel.

**preference *num***

Default: 1

If multiple tunnels will be configured, this option assigns a preference to the tunnel.

*num* can be an integer from 1 through 128.

**no**

Disables IP-in-IP tunneling for the current subscriber.

**Usage Guidelines**

Subscriber IP payloads are encapsulated with IP-in-IP headers and tunneled by the GGSN or PDSN to an external gateway.

**Example**

The following command configures the system to encapsulate subscriber traffic using IP-in-IP and tunnel it from a local address of *192.168.1.100* to a gateway with an IP address of *192.168.1.225*:

```
tunnel ipip peer-address 192.168.1.225 local-address 192.168.1.100
preference 1
```

# tunnel ipsec

Configures sessions for the current subscriber to use an IPSec tunnel based on the IP pool corresponding to the subscriber's assigned IP address.

**Product**

PDSN

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**tunnel ipsec use-policy-matching-ip-pooler-address**

**no tunnel ipsec use-policy-matching-ip-pooler-address**

**no**

Disables the use of the IPSec policy that matches the IP pool that the assigned IP address relates to.

**Usage Guidelines**

Use this command to set the current subscribers sessions to use an IPSec policy that is assigned to the IP pool that the subscribers assigned IP address relates to.

**Example**

The following command enables the use of the policy that matches the IP pool address:

**tunnel ipsec use-policy-matching-ip-pooler-address**

# tunnel l2tp

Configures L2TP tunnel parameters for the subscriber.

**Product**

All products supporting L2TP

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

*[context_name]host_name*(config-subscriber)#

**Syntax Description**

**tunnel l2tp [ peer-address** *ip address* **[ [ encrypted ] [secret** *secret*] ] [ **preference** *number*] **[ tunnel-context** *context* **] [ local-address** *ip_address* **] [ crypto-map** *map_name* **{ [ encrypted ] isakmp-secret** *secret* **} ] ]**

**no tunnel l2tp [ peer-address** *ip_address* **]**

**peer-address *ip_address***

A peer L2TP Network Server (LNS) associated with this LAC (L2TP Access Concentrator). *ip_address* must be an IP address entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal format.

**[ encrypted ] secret *secret***

Specifies the shared key (secret) between the L2TP Network Server (LNS) associated with this LAC (L2TP Access Concentrator). *secret* must be an alphanumeric string of 1 through 63 characters that is case sensitive.

**encrypted**: Specifies the encrypted shared key between the L2TP Network Server (LNS) associated with this LAC (L2TP Access Concentrator). *secret* must be an alphanumeric string of 1 through 128 characters that is case sensitive.

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

**preference *number***

Default: 1

Specifies the order in which a group of tunnels configured for this subscriber will be tried. *number* must be an integer from 1 through 65535.

**tunnel-context *context***

Specifies the name of the context containing ports through which this subscriber's data traffic is to be communicated between this LAC and the LNS. *context* must be an alphanumeric string of 1 through 79 characters.

**local-address *ip_address***

Specifies a LAC service bind address which is given as a hint that is used to select a particular LAC service. *ip_address* must be an IP address entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**crypto-map *map_name* { [encrypted] isakmp-secret *secret* }**

Specifies the name of a crypto map that has been configured in the current context. *map_name* must be an alphanumeric string from 1 to 127 alphanumeric characters.

**isakmp-secret** *secret*: Specifies the pre-shared key for the Internet Key Exchange (IKE). *secret* must be an alphanumeric string of 1 through 127 characters.

**encrypted isakmp-secret** *secret*: Specifies the pre-shared key for IKE. Encryption must be used when sending the key. *secret* must be an alphanumeric string of 1 through 127 characters.

**no**

Disables tunneling for the current subscriber. When peer-address is included, the tunneling for that specific L2TP Network Server (LNS) is disabled but tunneling to other configured LNSs is still enabled.

## Usage Guidelines

Use this command to configure specific L2TP tunneling parameters for the current subscriber.

### Example

To specify L2tp tunneling to the LNS peer at the IP address *198.162.10.100* with a shared secret of *bigco* and preference of *1*, enter the following command:

```
tunnel l2tp peer-address 198.162.10.100 secret bigco preference 1
```

# w-apn

This command allows you to configure the default APN to be used for the UE connections when the AAA server does not return the subscriber APN name in the service-selection AVP in RADIUS Access-Accept message.

**Product**

eWAG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context** *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**w-apn** *apn_name*

**no w-apn**

**no**

If previously configured, removes the specified configuration.

**apn-name *apn_name***

Specifies the APN name.

*apn_name* must be the name of an APN and must be a string of 1 to 62 characters in length consisting of alphabetic characters (A-Z and a-z), digits (0-9), dot(.) and the dash (-).

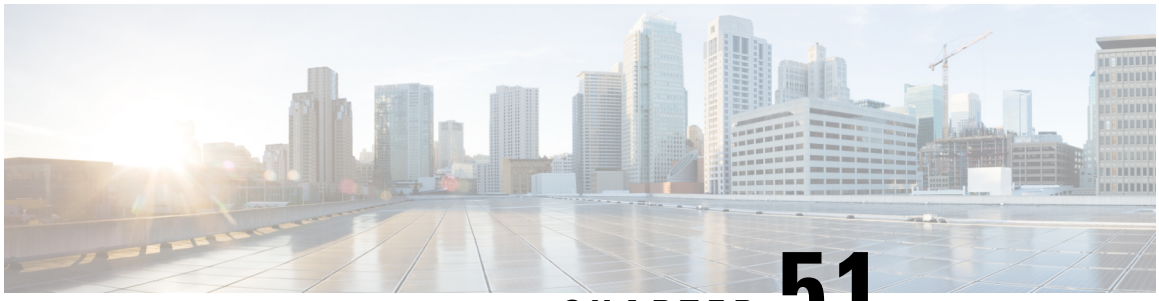
**Usage Guidelines**

Use this command to configure the default APN to be used for UE connections when the AAA server does not return the subscriber APN name in the Service-Selection AVP in RADIUS Access-Accept message. This APN will be considered as the network to which the UE is connecting and used in the CPC request message towards GGSN.

**Example**

The following command configures an APN named *apn123*:

**w-apn apn123**



CHAPTER 51

# Sx Service Configuration Mode Commands

The Sx Service Configuration Mode is used to associate with the SAEGW service at the Control Plane, and User-Plane service at the User Plane. There is one-to-one mapping of the Sx service with the Control-Plane and User Plane.

**Command Modes**

Exec > Global Configuration > Context Configuration > Sx Service Configuration

**configure > context** *context_name* **> sx-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name( config-sx-service )#
```

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


- bind, on page 679
- instance-type, on page 680
- sx-protocol association release-timeout, on page 681
- sx-protocol heartbeat, on page 681
- sx-protocol pdi-optimization, on page 683
- sx-protocol supported-features, on page 684
- sx-service exclude-user-plane, on page 685
- sxa, on page 686
- sxab, on page 686
- sxb, on page 687


# bind

Use this command to bind the specified Sx service to an IP address.

**Product**

CUPS

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Sx Service Configuration

**configure** > **context** *context_name* > **sx-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sx-service)#
```

**Syntax Description**

```
[ no ] bind { ipv4-address ipv4_address | ipv6-address ipv6_address }
```

**no**

Disables the command.

**ipv4-address**

Designates an IPv4 address of the Sx service.

**ipv6-address**

Designates an IPv6 address of the Sx service.

**Usage Guidelines**

Use this command to bind the specified Sx service to an IPv4 or IPv6 address.

# instance-type

Configures the instance type for which the Sx service with Sx Demux is used under Sx Service Configuration Mode.

**Product**

CUPS

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Sx Service Configuration

**configure** > **context** *context_name* > **sx-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sx-service)#
```

**Syntax Description**

```
[ no ] instance-type { controlplane | userplane }
```

**no**

Disables the command.

**controlplane**

Configures Sx service with Demux on the Control-Plane instance.

**userplane**

Configures Sx service with Demux on the User-Plane instance.

**Usage Guidelines** Use this command to configure the instance type for which the Sx service with Sx Demux is used under Sx Service Configuration Mode. Only one instance type can be configured at a given time.

# sx-protocol association release-timeout

Configures association release-timeout for Sx interface.

**Product** UPF

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Sx Service Configuration

**configure** > **context** *context_name* > **sx-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-sx-service)#`

**Syntax Description** **sx-protocol association release-timeout** *seconds*

**release-timeout *seconds***

Configures the association release interval (in seconds) for Sx Service. *seconds* must be an integer in the range of 1 to 30.

**Usage Guidelines** Use this command to configure association release-timeout for Sx interface.

**Example**

The following command sets the association release-timeout to *20* seconds:

**sx-protocol association release-timeout 20**

# sx-protocol heartbeat

Configures heartbeat parameters for Sx interface.

**Product** CUPS

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Sx Service Configuration

**configure** > **context** *context_name* > **sx-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-sx-service)#`

**Syntax Description** **[ default ] sx-protocol heartbeat { interval** *seconds* **| max-retransmissions** *mx_value* **| path-failure detection-policy { control-recovery-timestamp-change**

```
 | heartbeat-retry-failure | heartbeat-recovery-timestamp-change } |
retransmission-timeout seconds }
no sx-protocol heartbeat { interval | path-failure detection-policy {
control-recovery-timestamp-change | heartbeat-retry-failure |
heartbeat-recovery-timestamp-change }
```

**default**

Sets/restores default value assigned for specified parameter.

**no**

Disables the followed option.

**heartbeat**

Configures Sx heartbeat parameters.

**interval *seconds***

Configures heartbeat interval (in seconds) for Sx Service. *seconds* must be an integer in the range of 1 to 3600.

**max-retransmissions *mx_value***

Configures maximum retries for Sx heartbeat request. Must be followed by integer, ranging from 0 to 15. Default is 4.

**retransmission-timeout *seconds***

Configures the heartbeat retransmission timeout for Sx Service, in seconds, ranging from 1 to 20. Default is 5.

**path-failure**

Specifies policy to be used when path failure happens via heartbeat request timeout.

**detection-policy**

Specifies the policy to be used. Default action is to do cleanup upon heartbeat request timeout.

**control-recovery-time-stamp-change**

Path failure is detected when the recovery timestamp in control request/response message changes.

**heartbeat-retry-failure**

Path failure is detected when the retries of heartbeat messages times out.

**heartbeat-recovery-timestamp-change**

Path failure is detected when the recovery timestamp in heartbeat request/response message changes.

## Usage Guidelines

Use this command to configure heartbeat parameters for Sx interface.

### Example

The following command sets the heartbeat interval to *60* seconds:

```
sx-protocol heartbeat interval 60
```

# sx-protocol pdi-optimization

Enables Packet Detection Information (PDI) Optimization feature. This feature allows the optimization of PFCP signaling through Sx Establishment and Sx Modification messages between the Control Plane and the User Plane function.

**Product**

CUPS

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Sx Service Configuration

**configure > context** *context_name* **> sx-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sx-service)#
```

**Syntax Description**

```
[ no ] sx-protocol pdi-optimization
```

**no**

Disables PDI optimization. By default, the CLI command is disabled.

**Usage Guidelines**

Use this command to enable the PDI Optimization feature.

- PDI Optimization is enabled or disabled at PDN level. PDI Optimization is enabled for each PDN based on the configuration in sx-service. The PDN is PDI Optimization-enabled if the configuration is enabled while processing Sx Establishment Request on the Control Plane.
- Configuration changes will not have any effect on the PDN. The configuration that is applied while processing Sx Establishment Request will be maintained throughout the lifetime of the PDN. In a multi-PDN call, each PDN has the configuration applied while PDN is set up.
- On the User Plane, there is no separate configuration to determine whether the PDN has PDI Optimization-enabled. When Create Traffic Endpoint IE is received in Sx Establishment Request for a Sx session, then the Sx session is considered to have PDI Optimization-enabled throughout the lifetime of the session. This will not change dynamically midway, and validations are done accordingly. In case of any validation failures, Error Response is sent back to the Control Plane.
- When there are multiple Create Traffic Endpoint IEs with the same Traffic Endpoint ID, the first Create Traffic Endpoint IE is processed, and rest are ignored. The same behavior is applicable for Created Traffic Endpoint IE, Update Traffic Endpoint IE, and Remove Traffic Endpoint IE.

# sx-protocol supported-features

Configures various features for Sx interface.

**Product**

UPF

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Sx Service Configuration

**configure > context** *context_name* **> sx-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-sx-service)#`

**Syntax Description**

**`[ no ] sx-protocol supported-features { dbdm | ddnd | epfar | load-control | overload-control | udbc }`**

**no**

Disables the supported features.

**epfar**

Configures the Enhanced PFCP Association Release (epfar) feature.

**dbdm**

Configures the DBDM feature for Reduced Capability functionality.

**ddnd**

Configures the DDND feature for Reduced Capability functionality.

**udbc**

Configures the UDBC feature for Reduced Capability functionality.

**load-control**

Configures the load control feature.

**overload-control**

Configures the overload control feature.

**Usage Guidelines**

Use this command to configure the Enhanced PFCP Association Release (epfar) feature for Sx interface.

**Example**

The following command enables the EPFAR feature:

```
sx-protocol supported-features epfar
```

# sx-service exclude-user-plane

Configures the rejection parameters to exclude a specific User Plane when it crosses a threshold.

**Product**

CUPS

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Sx Service Configuration

**configure > context** *context_name* **> sx-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sx-service)#
```

**Syntax Description**

**[ no ] exclude-user-plane minimum-call-failures** *min_callfail_range* **failure-threshold-percentage** *fail_threshold_percentage* **failure-rejection-interval** *fail_reject_int*

**exclude-user-plane**

Excludes a User Plane when it crosses the threshold.

**minimum-call-failures *min_callfail***

Configures the minimum number of call failures within failure-rejection-interval to exclude a specific UP. The value for minimum-call-failures ranges between 1 to 5000. The suggested value is 200.

**failure-threshold-percentage *fail_threshold_percentage***

Configures the failure threshold percentage to exclude a specific UP. The value for failure-threshold-percentage ranges between 80 to 100. The suggested value is >=90%

**failure-rejection-interval *fail_reject_int***

Configures the failure rejection interval to exclude a specific UP. The value for failure-rejection-interval ranges between 10 to 600. The suggested value is 120 seconds.

**[ no ]**

This is an optional command. It disables the exclusion of the UP.

**Usage Guidelines**

Use this command to configure the rejection parameters to exclude a specific User Plane post crossing a threshold.

**Example**

```
exclude-user-plane minimum-call-failures 200 failure-threshold-percentage
 90 failure-rejection-interval 120
```

# sxa

Configures Sxa parameters for the Sx control packets on the S-GW.

**Product**

CUPS

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Sx Service Configuration

**configure > context** *context_name* **> sx-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sx-service)#
```

**Syntax Description**

**sxa { max-retransmissions** *mx_value* **| retransmissions-timeout-ms** *rt_value* **}**

By default, this command is disabled.

**max-retransmissions *mx_value***

Configures the maximum retries for Sx control packets on the S-GW. Enter an integer. The valid value range from 0 to 15. The default value is 4.

**retransmissions-timeout-ms *rt_value***

Configures the retransmission timeout for Sx control packets (on the S-GW), in milliseconds. Enter a value in multiples of 100. The valid values range from 1000 to 20000. The default value is 5000.

**Usage Guidelines**

Use this command to modify the Sxa parameters for the S-GW under Sx Service Configuration Mode.

**Example**

The following sets the maximum retries for Sx control packets to 5:

```
sxa max-retransmissions 5
```

# sxab

Configures Sxab parameters for the Sx control packets on the S-GW and P-GW.

**Product**

CUPS

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Sx Service Configuration

**configure > context** *context_name* **> sx-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sx-service)#
```

**Syntax Description**

**sxab { max-retransmissions** *mx_value* **| retransmissions-timeout-ms** *rt_value* **}**

By default, this command is disabled.

**max-retransmissions *mx_value***

Configures the maximum retries for Sx control packets on the S-GW and P-GW. Enter an integer. The valid value range from 0 to 15. The default value is 4.

**retransmissions-timeout-ms *rt_value***

Configures the retransmission timeout for Sx control packets (on the S-GW and P-GW), in milliseconds. Enter a value in multiples of 100. The valid values range from 1000 to 20000. The default value is 5000.

**Usage Guidelines**

Use this command to modify the Sxab parameters for the S-GW and P-GW under Sx Service Configuration Mode.

**Example**

The following sets the maximum retries for Sx control packets to 5:

```
sxab max-retransmissions 5
```

# sxb

Configures Sxb parameters for the Sx control packets on the P-GW.

**Product**

CUPS

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Sx Service Configuration

**configure > context** *context_name* **> sx-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sx-service)#
```

**Syntax Description**

**sxb { max-retransmissions** *mx_value* **| retransmissions-timeout-ms** *rt_value* **}**

By default, this command is disabled.

**max-retransmissions *mx_value***

Configures the maximum retries for Sx control packets on the P-GW. Enter an integer. The valid value range from 0 to 15. The default value is 4.

**retransmissions-timeout-ms *rt_value***

Configures the retransmission timeout for Sx control packets (on the P-GW), in milliseconds. Enter a value in multiples of 100. The valid values range from 1000 to 20000. The default value is 5000.

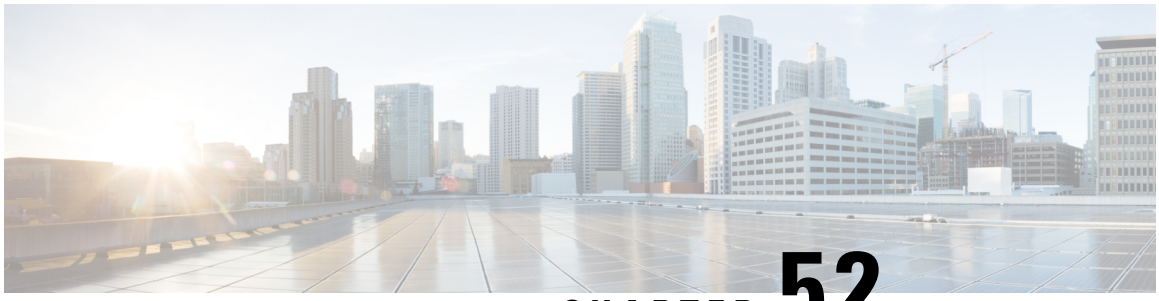
## Usage Guidelines

Use this command to modify the Sxb parameters for the P-GW under Sx Service Configuration Mode.

### Example

The following sets the maximum retries for Sx control packets to 5:

```
sxb max-retransmissions 5
```



CHAPTER 52

# TACACS+ Configuration Mode Commands

**Important** TACACS Configuration Mode is available in releases 11.0 and later.

## Command Modes

This chapter describes all commands available in the TACACS+ Configuration Mode. TACACS+ (Terminal Access Controller Access-Control System Plus) is a secure, encrypted protocol. By remotely accessing TACACS+ servers that are provisioned with the administrative user account database, the ASR 5500 support TACACS+ accounting and authentication services for system administrative users.

Exec > Global Configuration > TACACS+ Configuration

**configure > tacacs mode**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

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


- accounting, on page 690
- authorization, on page 691
- do show, on page 692
- end, on page 692
- exit, on page 692
- idle-session threshold, on page 693
- max-sessions, on page 694
- on-authen-fail, on page 694
- on-network-error, on page 695
- on-unknown-user, on page 696
- priv-lvl, on page 697
- rem_addr client-ip, on page 698
- server, on page 699
- user-id, on page 702

# accounting

Enables the recording of the start and the stop time each command issued during a TACACS+-authenticated CLI session.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > TACACS+ Configuration

**configure > tacacs mode**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

**Syntax Description**

```
[ no ] accounting { command | start-stop }
```

**no**

Disables a speicifed TACACS+ accounting setting.

**command**

Enables accounting on a command-by-command basis. The TACACS+ server is contacted prior to the execution of the command and the command which is about to be executed is recorded. Only commands which are valid for the user privilege and context (mode) in which they are about to be executed will be recorded. StarOS does not record whether the command itself succeeded or failed. For security reasons, some secure or restricted commands are not recorded. In such cases, the accounting record will record the command as three asterisks ("***").

**start-stop**

Records the time at which the session starts (the time at which the user passes authentication) and the time at which the user exits. If a user exits before passing authentication, only a stop time is recorded.

**Usage Guidelines**

Use this command to configure the accounting method for TACACS+-based CLI sessions.



**Important** *For releases after 15.0 MR4,* TACACS+ accounting (CLI event logging) will not be generated for Lawful Intercept users with privilege level set to 15 and 13.

**Example**

The following command enables TACACS+ accounting for commands:

```
accounting command
```

# authorization

Enables the authorization of TACACS+ CLI users on a command-by-command, command + command argument, or command prompt basis. If the user is not authorized to execute the command, the command will fail.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > TACACS+ Configuration

**configure > tacacs mode**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

**Syntax Description**

```
[ no ] authorization { arguments | command | prompt }
```

**no**

Disables a specified TACACS+ authorization type.

**arguments**

Enables per-command and command + argument authorization. The TACACS+ server authorizes each command and its arguments for the user. If the user is not authorized to execute the command and the corresponding arguments, the command fails. If the command does not contain any arguments, then the command only is passed to the authorization server.

**command**

Enables per-command authorization. The TACACS+ server is contacted for each command and each command is authorized for the user. If the user is not authorized to execute the command, then the command fails. If the user is authorized for the command, the command is executed.

**prompt**

Enables per-command authorization, as described for the **command** option above. However, since commands may be duplicated in different CLI modes, this version of the command authorization also passes the command prompt string to the server. The TACACS+ server is contacted for each prompt and command and must have a matching string for the prompt/command combination. Enabling **prompt** authorization supersedes **command** authorization, since the prompt and command must be authorized together.

**Usage Guidelines**

Use this command to configure the authorization method for TACACS+-based CLI sessions.

**Example**

The following command requires per-command TACACS+ authorization:

```
authorization command
```

# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
end
```

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
exit
```

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

# idle-session threshold

Configures the idle session threshold available for TACACS+ sessions.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > TACACS+ Configuration

**configure > tacacs mode**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

**Syntax Description**

**idle-session threshold** *number* **user-id** *tacacs_userid*
**default idle-session threshold user-id** *tacacs_userid*

**threshold *number***

Configures the idle sessions threshold value in minutes. If a session is idle, the CLI flags it as being in an idle state when it has been inactive for a specific amount of time. *number* specifies the idle-session threshold number in minutes. This setting must be an alphanumeric integer from 0 to 10 minutes. The default value is 5 minutes. 0 indicates that there is no idle session threshold for the user. When a CLI session has reached the threshold, then the session is in the idle state but it will not be in the idle state indefinitely.

**user-id *tacacs_userid***

Identifies a valid TACACS+ user as an alphanumeric string of 1 through 144 characters.

**default *tacacs_userid***

Configures the default number for idle sessions to 5 minutes.

**Usage Guidelines**

Use this command to configure the idle session threshold in minutes for a specific TACACS+ user.

The default value of 5 minutes is used if the idle-session threshold is not configured for a user.

After upgrading to 21.2.0, the default maximum sessions number is assigned to all users. After downgrading to a previous release, the maximum sessions configuration is lost.

While using the **user-id** *TACACS+ Configuration Mode* command without the **idle session threshold** command, the system will keep the existing configured value or the default value if nothing is configured.

**Example**

The following command configures the threshold for this user to be 5 minutes:

**idle-session threshold 5 user-id admin**

# max-sessions

Configures the maximum number of sessions available for a TACACS+ user.

**Product**

All products

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > TACACS+ Configuration

**configure > tacacs mode**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

**Syntax Description**

**max-sessions** *number* **user-id** *tacacs_userid*
**default max-sessions user-id** *tacacs_userid*

***number***

Specifics the maximum number of simultaneous CLI sessions. It must be alphanumeric integer from 0 to 100. The default number is 100.

**user-id *tacacs_userid***

Identifies a valid TACACS+ user as an alphanumeric string of 1 through 144 characters.

**default**

Configures the default number of simultaneous CLI sessions to 100.

**Usage Guidelines**

Use this command to configure the maximum number of sessions available for a TACACS+ user.

After upgrading to 21.2.0, the default maximum sessions number is assigned to all users. After downgrading to a previous release, the maximum sessions configuration is lost.

**Example**

The following command configures 50 CLI sessions for a specific TACACS user:

```
max-sessions 50 user-id admin
```

The following command configures 100 CLI sessions for a specific TACACS user:

```
default max-sessions user-id admin
```

# on-authen-fail

Defines system behavior when an administrative login fails due to a TACACS+ authentication failure. This command also can be used to configure system behavior separately for TACACS+ authentication failures for administrative users accessing the system via the StarOS Console port.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > TACACS+ Configuration

**configure > tacacs mode**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

**Syntax Description** **`on-authen-fail { continue | stop } [ tty console ]`**

**continue**

After a TACACS+ authentication failure, the system will continue with authentication using non-TACACS+ authentication services.

**stop**

After a TACACS+ authentication failure, the system forces the failed TACACS+ user to exit.

**tty console**

***Release 12 and later systems only***: Used after the **stop** or **continue** parameters to specify system behavior for users being authenticated via the StarOS Console port:

- **stop tty console**: Forces the failed TACACS+ user to exit.
- **continue tty console**: The system will continue with authentication using non-TACACS+ authentication services.

**Usage Guidelines** Use this command to configure system behavior for users that fail TACACS+ authentication.

**Example**

The following command instructs the system to stop upon TACACS+ authentication failure:

```
on-authen-fail stop
```

# on-network-error

Configures StarOS behavior when a TACACS+ login fails due to a network error. This command also can be used to configure system behavior separately for TACACS+ network error login failures for administrative users accessing the system via the Console port.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > TACACS+ Configuration

**configure > tacacs mode**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

**Syntax Description**

```
on-network-error { continue | stop } [ tty console ]
```

**continue**

The system will continue with authentication using non-TACACS+ authentication services.

**stop**

The system forces the failed TACACS+ user to exit.

**tty console**

***Release 12 and later systems only***: Can be used after the **continue** or **stop** options to specify system behavior for TACACS+ CLI users being authenticated via the StarOS Console port:

- **stop tty console**: Forces the failed user to exit when authentication fails.
- **continue tty console**: The system will continue with authentication using non-TACACS+ authentication services.

**Usage Guidelines**

Use this command to configure system behavior for users who fail TACACS+ authentication due to a network error.

**Example**

The following command conifgures the system to stop when a TACACS+ login fails due to a network error:

```
on-network-error stop
```

# on-unknown-user

Configures StarOS behavior when a TACACS+ server cannot authenticate a given user name. This command also can be used to configure system behavior separately for TACACS+ unknown user login failures for administrative users accessing the system via the StarOS console port.



**Important** Some TACACS+ server implementations will not send a Reply message indicating that the user name is invalid. Instead, these types of implementations will accept the username, whether valid or not, and then examine the username and password in combination before sending a Reply message indicating a failed TACACS+ login. In these cases, specifying **on-unknown-user** will continue the login process. To avoid this scenario, determine the method the configured TACACS+ servers will use to validate user names before deciding whether specifying the **on-unknown-user** command will provide the desired result.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > TACACS+ Configuration

**configure > tacacs mode**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

**Syntax Description**

```
on-unknown-user { continue | stop } [ tty console ]
```

**continue**

The system will continue with authentication using non-TACACS+ authentication services.

**stop**

The system forces the failed TACACS+ user to exit.

**tty console**

***Release 12 and later systems only***: Can be used after the **continue** or **stop** options to specify the behavior of the system for TACACS+ CLI users being authenticated via the StarOS console port.

- **stop tty console**: The system forces the failed user to exit when authentication fails.
- **continue tty console**: The system will continue with authentication using non-TACACS+ authentication services.

**Usage Guidelines**

Use this command to configure StarOS behavior for users who fail TACACS+ user name authentication.

TACACS+ authentication is also performed on non-local VPN context logins, if TACACS+ is configured and enabled. If TACACS+ is enabled with the **on-unknown-user stop** option, the VPN context name into which the user is attempting a login must match the VPN name specified in the username string. If the context name does not match, the login fails and exits out.

**Example**

The following command forces users who fail TACACS+ user name authentication to exit StarOS:

```
on-unknown-user stop
```

# priv-lvl

Configures authorized StarOS privileges for a specified TACACS+ privilege level.

**Product**

All products

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > TACACS+ Configuration

**configure > tacacs mode**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

**Syntax Description**

```
priv-lvl lvl_number authorization-level { administrator | inspector |
operator | security-admin } [ cli | ecs | ftp | li-administration | nocli
 | noecs | noftp | nocli-administration ]
```

***lvl_number***

Specifies the TACACS+ privilege level with which StarOS authorizations will be associated. as an integer from 1 through 15.

**authorization-level { administrator | inspector | operator | security-admin }**

Specifies the StarOS administrative authorization level for this privilege level.

- **administrator** – Allows user to execute Administrator level configuration commands.
- **inspector** – Allows user to execute Inspector commands.
- **operator** – Allows user to execute Operator commands.
- **security-admin** – Allows user to execute Security Administrator commands

For detailed information about StarOS administration levels, refer to the *System Settings* chapter of the *System Administration Guide*.

**[ cli | ecs | ftp | li-administration | nocli | noecs | noftp | nocli-administration ]**

Specifies a set of access privileges or restrictions for this TACACS+ privilege level. Multiple options may be specified.

- **cli** – Permits access to the StarOS command line interface.
- **ecs** – Permits access to Enhanced Charging Services (ECS) commands.
- **ftp** – Permits of File Transfer Protocol (FTP).
- **li-administration** – Permits access to Lawful Intercept (LI) administrative commands.
- **nocli** – Denies access to the StarOS CLI.
- **noecs** – Denies access to ECS commands
- **noftp** – Denies use of FTP.
- **nocli-administration** – Denies access to StarOS Administrator and Security Administrator commands.

**Usage Guidelines**

Use this command to customize StarOS access authorization for users at various TACACS+ privilege levels.

**Example**

The following command sequence authorizes a TACACS+ priv-level 13 user to execute StarOS Administrator commands but denies access to LI administrative commands and FTP.

```
priv-lvl 13 authorization-level administrator cli noftp
```

# rem_addr client-ip

Sends a remote client IPv4 address field in the TACACS+ protocol for use by a Cisco Secure ACS server.

**Product**

All products

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > TACACS+ Configuration

**configure > tacacs mode**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

**Syntax Description**

**[ default | no ] rem_addr client-ip**

**default**

Disables the sending of a remote client IP address field to a Cisco Secure ACS server for a TACACS+ login request.

**no**

Disables the sending of a remote client IP address field to a Cisco Secure ACS server for a TACACS+ login request.

**Usage Guidelines**

A Cisco Secure ACS server can be configured to explicitly check the NAS source address for TACACS+ connections. StarOS may not properly set the rem_addr field in the TACACS+ protocol packet when initiating a connection with the Cisco Secure ACS server. This may cause the Cisco Secure ACS server to reject the TACACS+ login request.

**Important** The default behavior is to not fill in the rem_addr field.

This CLI command enables the setting and sending of the remote address to the IPv4 address associated with the local context management interface for customers who require this field to be verified via the Cisco Secure ACS server.

When enabled the rem_addr field contains the ssh client IP address in ASCII form. If the IP address cannot be retrieved, the length is set to zero.

**Example**

The following command enables the sending of the rem_addr field to a Cisco Secure ACS server for a TACACS+ login request:

**rem_addr client-ip arg1**

# server

Configures TACACS+ AAA service-related parameters for use in authenticating StarOS administrative users via a TACACS+ server.



**Important** Once a TACACS+ server is configured with the **server** command, TACACS+ AAA services for StarOS must be enabled using the **aaa tacacs+** command in Global Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > TACACS+ Configuration

**configure > tacacs mode**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

**Syntax Description**

**server priority** *priority_number* **ip-address** *ip_address* **[ { encrypted password** *shared_secret* **] [ key** *text_password* **] [ nas-source-address** *ip_address* **] [ password** *text_password* **] [ port** *port_number* **] [ retries** *num_retries* **] [ service { accounting |authentication | authorization } ] ] [ timeout** *seconds* **]**
**no server priority** *priority_number*

**no**

Removes a specified server (by priority number) from the TACACS+ server list.

**priority *priority_number***

Specifies the order in which TACACS+ servers are to be tried. The priority number corresponds to a configured TACACS+ server.

*For releases prior to 18.2*, *priority_number* can be an integer from 1 (highest priority) to 3 (lowest priority).

*For releases 18.2+*, *priority_number* can be an integer from 1 (highest priority) to 4 (lowest priority).

If no server with priority 1 is specified, the next highest priority is used. If the specified priority matches that of a TACACS+ server already configured, any previously defined server configuration parameter(s) for that priority are returned to the default setting(s).

**ip-address**

Specifies the IP address of the TACACS+ server in IPv4 or IPv6 dotted-decimal notation. Only one IP address can be defined for a given **server priority**

**encrypted password *shared_secret***

Specifies the encrypted value of the shared secret key. The server-side configuration must match the decrypted value for the protocol to work correctly. If **encrypted password** is specified, specifying **password** is invalid. No encryption is used if this value is null (""). The encrypted password can be an alphanumeric string of 1 through 100 characters. If neither an **encrypted password** or **password** is specified, StarOS will not use encryption

**key *text_password***

**Release 11.0 systems only**. Instead of using an encrypted password value, the user can specify a plain-text key value for the password. If the **key** keyword is specified, then specifying **encrypted password** is invalid. A null string represents no encryption. The password can be from 1 to 32 alphanumeric characters in length. If neither an **encrypted password** or **key** is specified, then StarOS will not use encryption.

**nas-source-address *ip_address***

***Release 12 and later systems only***: Sets the IPv4 or IPv6 address to be specified in the Source Address of the IP header in the TACACS+ protocol packet sent from the NAS to the TACACS+ server. *ip_address* is entered using IPv4 dotted-decimal notation and must be valid for the interface.

**password *text_password***

**Release 12.0 and later systems**. Instead of using an encrypted password value, the user can specify a plain-text value for the password. If the **password** keyword is specified, specifying **encrypted password** is invalid. A null string ("") represents no encryption. The password can be an alphanumeric string of 1 through 32 characters. If neither an **encrypted password** or **password** is specified, then StarOS will not use encryption.

**port *port_number***

Specifies the TCP port number to use for communication with the TACACS+ server. *port_number* can be an integer from 1 through 65535. If a port is not specified, StarOS will use port 49.

**retries *number***

***Release 12 and later systems only***: Specifies the number of retry attempts at establishing a connection to the TACACS+ server if the initial attempt fails. **retries** *number* can be an integer from 0 through 100. The default is 3. Specifying 0 (zero) retries results in StarOS trying only once to establish a connection. No further retries will be attempted.

**service { accounting | authentication | authorization }**

***Release 12 and later systems only***: Specifies one or more of the AAA services that the specified TACACS+ server will provide. Use of the **service** keyword requires that at lease one of the available services be specified. If the **service** keyword is not used, StarOS will use the TACACS+ server for all AAA service types. The default is to use authentication, authorization and accounting. Available service types are:

- **accounting**: The specified TACACS+ server should be used for accounting. If TACACS+ authentication is not used, TACACS+ accounting will not be used. If no accounting server is specified and the user is authenticated, no accounting will be performed for the user.
- **authentication**: The specified TACACS+ server should be used for authentication. If a TACACS+ authentication server is not available, TACACS+ will not be used for authorization or accounting.
- **authorization**: The specified TACACS+ server should be used for authorization. If TACACS+ authentication is not used, TACACS+ authorization will not be used. If no authorization server is specified and the user is authenticated, the user will remain logged in with minimum privileges (Inspector level).

**timeout *seconds***

Specifies the number of seconds to wait for a connection timeout from the TACACS+ server. *seconds* can be an integer from 1 through 1000. If no timeout is specified, StarOS0 will use the default value of 10 seconds.

**Usage Guidelines** Use this command to specify TACACS+ service parameters for a specified TACACS+ server.

**Example**

The following command configures a priority 2, TACACS+ authetication server at IP address 192.156.1.1:

```
server priority 2 ip-address 192.156.1.1 authentication
```

# user-id

Configures additional profile attributes for a specific TACACS+ user identifier.

**Product** All products

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > TACACS+ Configuration

**configure > tacacs mode**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

**Syntax Description**

```
user-id tacacs_userid [ li-admin | noli-admin ]
[ default ] user-id tacacs_userid
```

**user-id *tacacs_userid***

Identifies a valid TACACS+ user as an alphanumeric string of 1 through 144 characters.

**[ li-admin | noli-admin ]**

Grants or denies access to Lawful Intercept (LI) configuration commands.

**default**

Configures default profile attributes for a specific TACACS+ user identifier.

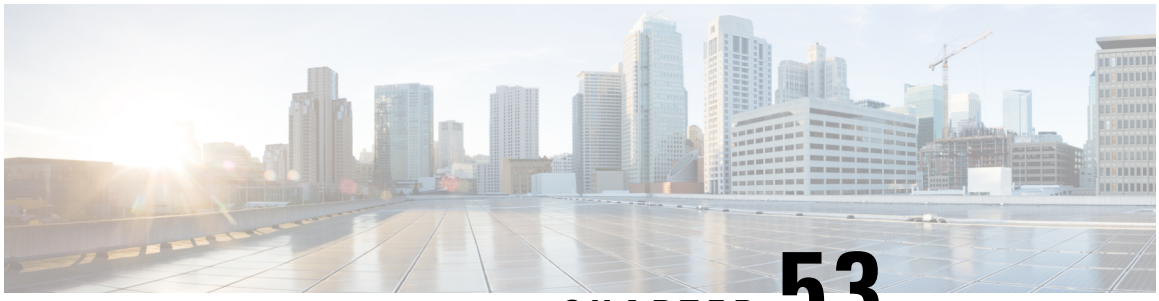
**Usage Guidelines** Use this command to grant LI access to a specified TACACS+ user identifier.

After upgrading to 21.2.0, the default maximum sessions number is assigned to all users. After downgrading to a previous release, the maximum sessions configuration is lost.

**Example**

The following command sequence grants TACACS+ user *victor134* access to LI administration commands:

```
user-id victor134 li-admin
```



CHAPTER 53

# TAC Profile Configuration Mode Commands

The Tracking Area Code (TAC) Profile Configuration Mode is used to configure TAC profiles on a per-context basis. This mode enables to select a Virtual APN (vAPN) based on TAC range and discrete values, and thereby a specific UP group and/or IP pool associated with vAPN.

**Command Modes**

Exec > Global Configuration > Context Configuration > TAC Profile Configuration

**configure > context** *context_name* **> tac-profile** *profile_name*

`[context_name]host_name(config-tac-profile)#`

**Important** Available commands or keywords/variables vary based on platform type, product version, and installed license(s).


- do show, on page 703
- end, on page 704
- exit, on page 704
- tac, on page 704


# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**do show**

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# tac

Configures Tracking Area Code (TAC) profile with discrete values and range.

**Product** SAEGW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > TAC Profile Configuration

**configure > context** *context_name* **> tac-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tac-profile)#
```

## Syntax Description

**[ no ] tac { range** *start_range* **to** *end_range* **|** *value* **}**

### no

Including **no** with the command disables the specified configuration.

### range *start_range* to *end_range*

Specifies the TAC start and end range of discrete integer value ranging from 0 to 65535.

### *value*

The number of discrete TAC values supported per CLI command is 16.

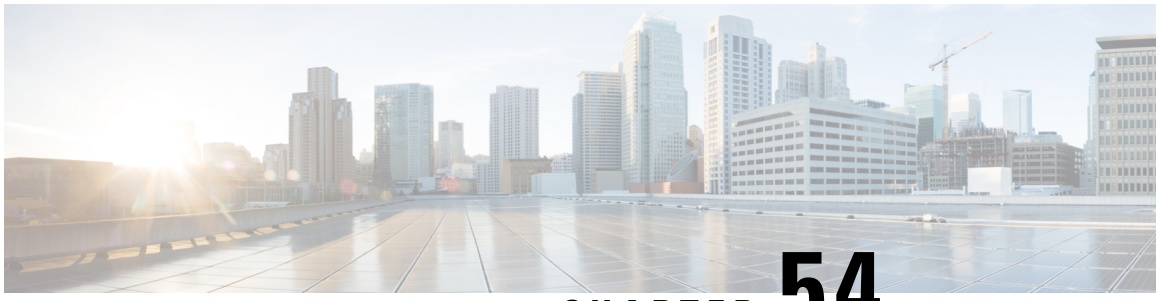
## Usage Guidelines

Use this command to configure TAC profiles per context. The maximum number of TAC discrete values supported in a profile are 100. Memory usage is fixed per profile. TAC range or discrete values can overlap between profiles to support maintenance activities like split existing profile or others. Multiple profiles can be associated with an APN.

### Example

The following command configures TAC range of 1 to 10:

```
tac range 1 to 10
```



CHAPTER 54

# Telnet Configuration Mode Commands

The Telnet Configuration Mode is used to manage the telnet server options for the current context.

**Command Modes**

Exec > Global Configuration > Context Configuration > Telnet Configuration

**configure > context** *context_name* **> server telnet**

Entering the above command sequence results in the following prompt:

`[local]host_name(config-telnetd)#`

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

**Caution** For maximum system security, you should not enable telnet functionality. SSH is the recommended remote access protocol. In release 20.0 and higher Trusted StarOS builds, telnet is not supported.

The global limit for utility service connections, including SSH, Telnet, and SFTP, is 201. This includes any inter-card communication that uses SSH.


- do show, on page 707
- end, on page 708
- exit, on page 708
- max servers, on page 708


# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# max servers

Configures the maximum number of telnet servers that can be started within any 60-second interval. If this limit is reached, the system waits two minutes before trying to start any more servers.

**Product** All

**Privilege** Security Administrator, Administrator

## Command Modes

Exec > Global Configuration > Context Configuration > Telnet Configuration

**configure > context** *context_name* **> server telnet**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-telnetd)#
```

## Syntax Description

**max servers** *count*

***count***

Specifies the maximum number of telnet servers that can be spawned in any 6- second interval. *count* must be an integer from 1 through 100. Default: 40

## Usage Guidelines

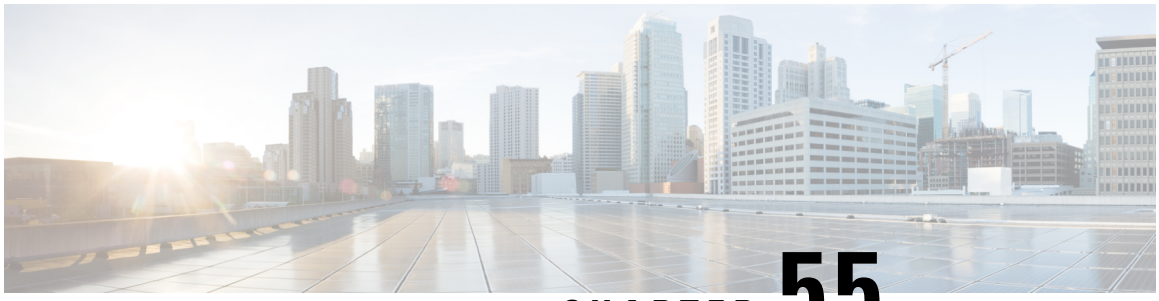
Use this command to set the number of telnet servers to tune the system response, as a heavily loaded system may need more servers to support the incoming requests.

The converse would be true in that a system can benefit by reducing the number of servers such that telnet services do not cause excessive system impact to other services.

### Example

The following command sets the maximum number of telnet servers to 30:

```
max servers 30
```



CHAPTER 55

# TFTP Configuration Mode Commands

The TFTP configuration mode is used to manage the TFTP (Trivial File Transfer Protocol) servers for the current context.

**Command Modes**

Exec > Global Configuration > Context Configuration > Tunnel TFTP Configuration

**configure > context** *context_name* **> server tftpd**

Entering the above command sequence results in the following prompt:

`[local]host_name(config-tftpd)#`

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


- do show, on page 711
- end, on page 712
- exit, on page 712
- max servers, on page 712


# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**do show**

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# max servers

Configures the maximum number of TFTP servers that can be started within any 60-second interval. If this limit is reached, the system waits two minutes before trying to start any more servers.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Tunnel TFTP Configuration

**configure > context** *context_name* **> server tftpd**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tftpd)#
```

## Syntax Description

**max servers** *count*

***count***

Specifies the maximum number of TFTP servers that can be spawned in any 60-second interval. *count* must be an integer from 1 through 100. Default: 40

## Usage Guidelines

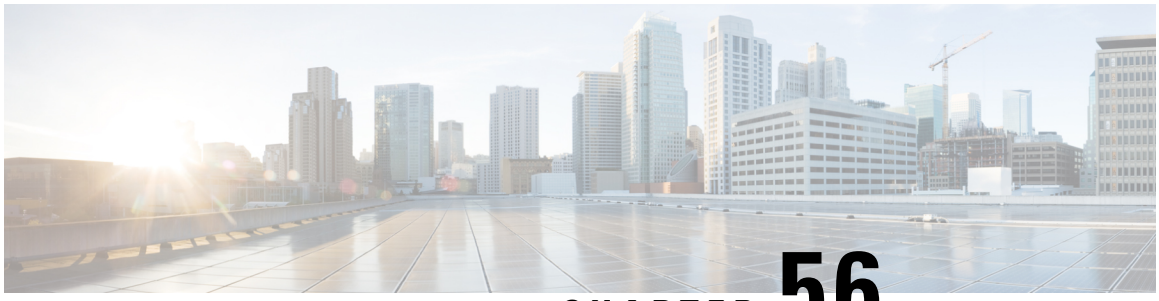
Use this command to set the number of servers to tune the system response, as a heavily loaded system may need more servers to support the incoming requests.

The converse would be true in that a system can benefit by reducing the number of servers such that TFTP services do not cause excessive system impact to other services.

### Example

The following command sets the maximum number of TFTP servers to 30:

```
max servers 30
```



CHAPTER 56

# Throttling Override Policy Configuration Mode Commands

Throttling Override Policy mode allows an operator to configure the Throttling Override Policy that can be used at the GGSN/P-GW nodes to selectively bypass throttling for a configured message type or for all messages in emergency call or priority call or call for the configured APN.

**Important** RLF Bypass Feature (enhancement to the GTP Throttling feature), used in the Throttling Override Policy config mode, is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

**Command Modes**

This chapter describes the GTPC Throttling Override Policy Configuration Mode commands.

Exec > Global Configuration > Throttling Override Policy

**configure > throttling-override-policy** *policy_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-throttling-override-policy)#
```

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


- do show, on page 715
- egress bypass-rlf, on page 716
- end, on page 718
- exit, on page 718


# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**do show**

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# egress bypass-rlf

Configures message types which can bypass the rate limiting function.

**Product**

GGSN

P-GW

**Privilege**

Administrator, Security Administrator

**Command Modes**

Exec > Global Configuration > Throttling Override Policy

**configure > throttling-override-policy** *policy_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-throttling-override-policy)#
```

**Syntax Description**

**egress bypass-rlf { ggsn { msg-type { dpc | ipca | nrupc | emergency-call | arp { 1 | 2 | 3 }+ | apn-names** *<apn-name1> <apn-name2> <apn-name3>* **} } | pgw { msg-type { cbr | dbr | ubr | emergency-call | earp-pl-list {1 | 2 | 3 | 4 | 5 ... | 15 }+ | apn-names** *<apn-name1> <apn-name2> <apn-name3>* **} } }**

**default egress bypass-rlf { ggsn { msg-type { dpc | ipca | nrupc | emergency-call | arp { 1 | 2 | 3 }+ | apn-names** *<apn-name1> <apn-name2> <apn-name3>* **} } | pgw { msg-type { cbr | dbr | ubr | emergency-call | earp-pl-list {1 | 2 | 3 | 4 | 5 ... | 15 }+ | apn-names** *<apn-name1> <apn-name2> <apn-name3>* **} } }**

**no egress bypass-rlf { ggsn { msg-type { dpc | ipca | nrupc | emergency-call | arp { 1 | 2 | 3 }+ | apn-names** *<apn-name1> <apn-name2> <apn-name3>* **} } | pgw { msg-type { cbr | dbr | ubr | emergency-call | earp-pl-list {1 | 2 | 3 | 4 | 5 ... | 15 }+ | apn-names** *<apn-name1> <apn-name2> <apn-name3>* **} } }**

**default**

Resets the default attribute values for egress bypass configuration. If an empty throttling-override-policy is created then the default values for all the configurables are zeros/disabled.

**no**

Disables the egress bypass rlf throttling configuration.

**ggsn**

Configures GGSN specific message types to bypass rlf throttling.

**pgw**

Configures P-GW specific message types to bypass rlf throttling

**msg-type**

Configures GGSN or P-GW message type to bypass rlf throttling.

**ggsn msg-type { dpc | ipca | nrupc | emergency-call | arp { 1 | 2 | 3 }+ | apn-names *<apn-name1> <apn-name2> <apn-name3>* } }**

Configures GGSN specific message types to bypass rlf throttling. Following are the message types that can be configured:

- **dpc:** Bypasses RLF throttling for network initiated Delete PDP Context message type. By default, dpc is not bypassed.
- **ipca:** Bypasses RLF throttling for network initiated Delete PDP Context message type. By default, dpc is not bypassed.
- **nrupc:** Bypasses RLF throttling for Network Requested Update PDP Context message type. By default, nrupc is not bypassed.
- **emergency-call:** Bypasses rlf throttling for all request messages initiated by GGSN emergency call. By default, emergency-call is NOT bypassed.
- **arp:** Configures Allocation-Retention-Policy (ARP) values associated with priority calls to be bypassed rlf throttling. By default, none of the ARP values are set. This option accepts the PL (Priority Level) values. The outgoing control messages of the calls with specified priority levels will bypass throttling.

  **+:** More than one of the previous keywords can be entered within a single command.
- **apn-names:** Configures GGSN APN names to bypass rlf throttling. You can configure upto three apn-names.

**pgw { msg-type { dpc | ipca | nrupc | emergency-call | earp-pl-list { 1 | 2 | 3 | 4 | 5 ... | 15 }+ | apn-names *<apn-name1> <apn-name2> <apn-name3>* } }**

Configures P-GW specific message types to bypass rlf throttling. Following are the message types that can be configured:

- **cbr:** Bypasses RLF throttling for create-bearer-request message type. By default, cbr is not bypassed.
- **dbr:** Bypasses RLF throttling for delete-bearer-request message type. By default, dbr is not bypassed.

- **ubr:** Bypasses RLF throttling for update-bearer-request message type. By default, ubr is not bypassed.
- **emergency-call:** Bypasses RLF throttling for all request messages initiated by P-GW emergency call. By default, emergency-call is NOT bypassed.
- **earp-pl-list:** Configures the list of Priority Levels(PL) associated with priority calls to be bypassed rlf throttling. By default none of the PLs are set. The outgoing control messages of the calls with specified priority levels will be bypassed throttling.

  **+:** More than one of the previous keywords can be entered within a single command.
- **apn-names:** Configures P-GW APN names to bypass rlf throttling. You can configure upto three apn-names.

**Usage Guidelines** Use this command to configure message types that can bypass throttling. If no parameters are specified, the system will use the default settings.

### Example

The following command configures Delete PDP message type at the GGSN node to bypass throttling.

```
egress bypass-rlf ggsn msg-type dpc
```

The following command configures create bearer request message type at the P-GW node to bypass throttling.

```
egress bypass-rlf pgw msg-type cbr
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
end
```

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

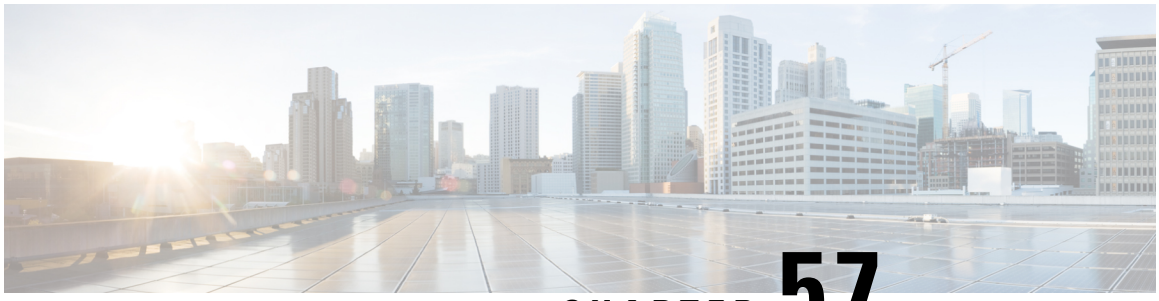
**Privilege** Security Administrator, Administrator

**Syntax Description**

```
exit
```

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

exit



CHAPTER 57

# Traffic Optimization Policy Confiugration


- bandwidth-mgmt, on page 721
- curbing-control, on page 722
- do show, on page 723
- end, on page 724
- exit, on page 724
- heavy-session, on page 724
- link-profile, on page 725
- session-params, on page 726


## bandwidth-mgmt

This command configures bandwidth management parameters for a traffic optimization policy.

**Product**

P-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Traffic Optimization Policy Configuration

**active-charging service** *service_name* > **traffic-optimization-policy** *policy_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-traffic-opt-policy)#
```

**Syntax Description**

```
bandwidth-mgmt { backoff-profile [ managed | unmanaged ] [
min-effective-rate effective_rate [ min-flow-control-rate flow_rate ] |
min-flow-control-rate flow_rate [ min-effective-rate effective_rate ] ] |
min-effective-rate effective_rate [ backoff-profile [ managed | unmanaged ]
 [ min-flow-control-rate flow_rate ] | min-flow-control-rate control_rate [
backoff-profile [ managed | unmanaged ] ] | min-flow-control-rate [ [
backoff-profile [ managed | unmanaged ] [ min-effective-rate effective_rate
 ] | [ min-effective-rate effective_rate ] [ backoff-profile [ managed |
unmanaged ] ] }
[ no ] bandwidth-mgmt
```

**no**

Overwrites the traffic-optimization configured parameter(s) with default values. Before deleting a policy profile, all policies associated to the policy profile should be removed. If policy associations are not removed before deletion, the following error message will be displayed:

```
Failure: traffic-optimization policy in use, cannot be deleted.
```

**backoff-profile**

Determines the overall aggressiveness of the back off rates.

**managed**

Enables both traffic monitoring and traffic optimization.

**unmanaged**

Only enables traffic monitoring.

**min-effective-rate *effective_rate***

Configures minimum effective shaping rate in Kbps. The shaping rate value is an integer ranging from 100 to 10000.

**min-flow-control-rate *flow_rate***

Configures the minimum rate allowed in Kbps to control the flow of heavy-session-flows during congestion. The control rate value is an integer ranging from 100 to 10000.

**Usage Guidelines** Use this command to configure bandwidth management parameters for a traffic optimization policy.

# curbing-control

This command configures curbing flow control related parameters.

**Product** P-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > ACS Configuration > Traffic Optimization Policy Configuration

**active-charging service** *service_name* **> traffic-optimization-policy** *policy_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-traffic-opt-policy)#
```

**Syntax Description** **curbing-control { max-phases** *max_phase_value* **[ rate** *curbing_control_rate* **[ threshold-rate** *threshold_rate* **[ time** *curbing_control_duration* **] ] ] | rate** *curbing_control_rate* **[ max-phases [ threshold-rate** *threshold_rate* **[ time** *curbing_control_duration* **] ] ] | threshold-rate [ max-phases** *max_phase_value* **[ rate** *curbing_control_rate* **[ time** *curbing_control_duration* **] ] ] | time [ max-phases** *max_phase_value* **[ rate** *curbing_control_rate* **[ threshold-rate** *threshold_rate*] **] ]**

```
}
[ no ] curbing-control
```

**no**

Overwrites the traffic-optimization configured parameter(s) with default values. Before deleting a policy profile, all policies associated to the policy profile should be removed. If policy associations are not removed before deletion, the following error message will be displayed:

```
Failure: traffic-optimization policy in use, cannot be deleted.
```

**max-phases *max_phase_value***

Configures consecutive phases where target shaping rate is below threshold-rate to trigger curbing flow control. The maximum phase value is an integer ranging from 2 to 10.

**rate *curbing_control_rate***

Configures the curbing flow-control at a fixed rate in Kbps instead of a dynamic rate. The control rate value is an integer ranging from 0 to 10000. To disable fixed flow control rate, set the flow control rate value to 0.

**threshold-rate *threshold_rate***

Configures the minimum target shaping rate in kbps to trigger curbing. The threshold rate is an integer ranging from 100 to 10000.

**time *curbing_control_detection***

Configures the duration of a flow control phase in milliseconds. The flow control duration value is an integer ranging from 0 to 600000. To disable flow control, set the flow control duration value to 0.

**Usage Guidelines** Use this command to configure curbing control parameters for a traffic optimization policy.

# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# heavy-session

This command configures heavy session detection parameters.

**Product** P-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > ACS Configuration > Traffic Optimization Policy Configuration

**active-charging service** *service_name* **> traffic-optimization-policy** *policy_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-traffic-opt-policy)#
```

**Syntax Description**

```
heavy-session { standard-flow-timeout [ threshold threshold_value | threshold
 threshold_value  seed-time seed_time_value[ standard-flow-timeout timeout_value ]
}
[ no ] heavy-session
```

**no**

Overwrites the traffic-optimization configured parameter(s) with default values. Before deleting a policy profile, all policies associated to the policy profile should be removed. If policy associations are not removed before deletion, the following error message will be displayed:

```
Failure: traffic-optimization policy in use, cannot be deleted.
```

**standard-flow-timeout *timeout_value***

Configures the idle timeout in milliseconds, for expiration of standard flows. The timeout value is an integer ranging from 100 to 3000.

**threshold *threshold_value***

Configures heavy-session detection threshold in bytes. On reaching the threshold, the flow will be monitored and potentially managed. The threshold value is an integer ranging from 0 to 100000000.

**seed-time *seed_time_value***

Configures time in ms for detection of elephant flow. Use this parameter in the enhanced detection mode.

**Usage Guidelines**

Use this command to configure heavy session detection for a traffic optimization policy.

# link-profile

This command configures link profile parameters for a traffic optimization policy.

**Product**

P-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Traffic Optimization Policy Configuration

**active-charging service** *service_name* **> traffic-optimization-policy** *policy_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-traffic-opt-policy)#
```

**Syntax Description**

```
link-profile { initial-rate initial_seed_value [ max-rate max_peak_rate_value [
peak-lock ] ] | max-rate [ initial-rate initial_seed_value [ peak-lock ] ] |
 peak-lock [ initial-rate initial_seed_value [ max-rate max_peak_rate_value ] ]
}
[ no ] link-profile
```

**no**

Overwrites the traffic-optimization configured parameter(s) with default values. Before deleting a policy profile, all policies associated to the policy profile should be removed. If policy associations are not removed before deletion, the following error message will be displayed:

```
Failure: traffic-optimization policy in use, cannot be deleted.
```

**initial-rate *initial_seed_value***

Configures the initial seed value of the acquired peak rate in Kbps for a traffic session. The initial seed value is an integer ranging from 100 to 30000.

**max-rate *max_peak_value_rate***

Configures the maximum learned peak rate allowed in Kbps for a traffic session. The max rate value is an integer ranging from 100 to 30000.

**peak-lock**

Confirms with the link peak rate available at the initial link peak rate setting.

**Usage Guidelines** Use this command to configure a link profile for a traffic optimization policy.

# session-params

This command configures session parameters for a traffic optimization policy.

**Product** P-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > ACS Configuration > Traffic Optimization Policy Configuration

**active-charging service** *service_name* **> traffic-optimization-policy** *policy_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-traffic-opt-policy)#
```

**Syntax Description**

```
session-params { tcp-ramp-up tcp_rampup_duration [ udp-ramp-up udp_rampup_duration
 ] | udp-ramp-up udp_rampup_duration [ tcp-ramp-up tcp_rampup_duration ] }
[ no ] session-params
```

**no**

Overwrites the traffic-optimization configured parameter(s) with default values. Before deleting a policy profile, all policies associated to the policy profile should be removed. If policy associations are not removed before deletion, the following error message will be displayed:

```
Failure: traffic-optimization policy in use, cannot be deleted.
```

**tcp-ramp-up *tcp_rampup_duration***

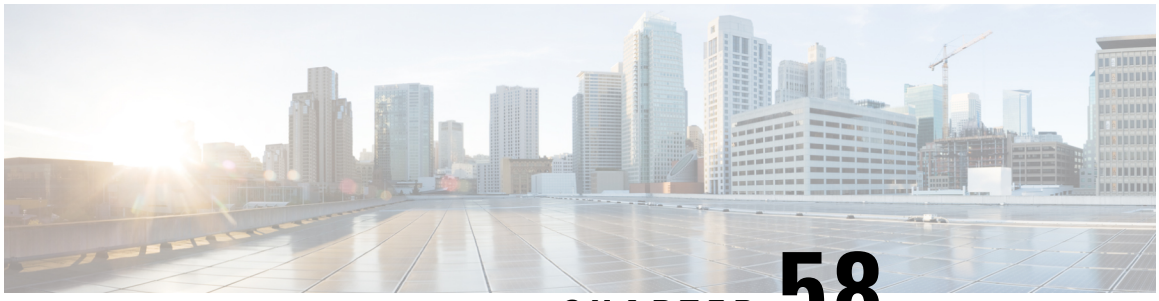
Configures the ramp-up-phase duration in milliseconds, for TCP traffic. The TCP ramp-up duration is an integer ranging from 0 to 5000.

**udp-ramp-up *udp_rampup_duration***

Configures the ramp-up-phase duration in milliseconds, for UDP traffic. The UDP ramp-up duration is an integer ranging from 0 to 5000.

## Usage Guidelines

Use this command to configure session parameters for a traffic optimization policy.



CHAPTER 58

# Traffic Optimization Profile Configuration Mode Commands

The Traffic Optimization Profile Configuration Mode allows you to configure and manage properties of Cisco Ultra Traffic Optimization solution.

**Command Modes**

Exec > ACS Configuration > Traffic Optimization Profile Configuration

**active-charging service** *service_name* **> traffic-optimization-profile**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-traffic-optim)#
```

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


- data-record, on page 729
- efd-flow-cleanup-interval, on page 730
- end, on page 731
- exit, on page 731
- heavy-session detection-threshold, on page 731
- mode, on page 732
- stats-interval, on page 733
- stats-options, on page 733


# data-record

This command enables Traffic Optimization Data Record (TODR) generation.

**Product**

P-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Traffic Optimization Profile Configuration

**active-charging service** *service_name* **> traffic-optimization-profile**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-traffic-optim)#
```

**Syntax Description**

```
data-record [ large-flows-only | managed-large-flows-only ]
no data record
```

**no**

If previously configured, disables generation of TODR.

**data-record**

Enables the Traffic Optimization Data Record (TODR) generation

- **large-flows-only**: Enables the traffic optimization data record generation for large flows.

  **managed-large-flows-only**: Enables the traffic optimization data record generation for managed large flows.

  The keywords - **large-flows-only** and **managed-large-flows-only** when configured along with **data-record** enables the CUTO library to stream the respective statistics as part of the **stats-options** command, to the external server. The user can configure a combination of the **stats-options** keywords **flow-trace** and **flow-analyst** and the **data-record** command to notify the CUTO library accordingly.

**Note** One of the above the two keywords can be configured as part of the data-record, which will enable the CUTO library to stream the respective statistics.

The default behavior of the **data-record** command is not affected with the above implementation . If it is configured without any of the options, then TODR's will be generated for all standard and large flows, which is the existing behavior.

**Usage Guidelines** Use this command to generate TODR.

# efd-flow-cleanup-interval

This configures EFD flow command cleanup interval.

**Product** P-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > ACS Configuration > Traffic Optimization Profile Configuration

**active-charging service** *service_name* **> traffic-optimization-profile**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-traffic-optim)#
```

**Syntax Description**

```
[ no ] efd-flow-cleanup-interval
```

**no**

If previously configured, disables EFD flow cleanup interval.

**efd-flow-cleanup-interval**

Configures EFD flow cleanup interval. The interval value is an integer that ranges from 10 to 5000 milliseconds.

**Usage Guidelines** Use this command to configure EFD flow cleanup interval.

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `end`

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `exit`

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

# heavy-session detection-threshold

Configures the threshold value for the TCP flow to be considered for the Traffic Optimization.

**Product** P-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > ACS Configuration > Traffic Optimization Profile Configuration

**active-charging service** *service_name* > **traffic-optimization-profile**

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-traffic-optim)#`

**Syntax Description** **heavy-session detection-threshold** *bytes*

**heavy-session**

Specifies the heavy session configuration for the Traffic Optimization.

**detection-threshold *bytes***

Specifies the detection threshold, in bytes. Beyond which, it is considered as heavy session. The *bytes* must be an integer from 1 to 4294967295.

To get optimum Traffic Optimization benefit, it is recommended to not set it less than 3 MB.

**Usage Guidelines** Use this command to set the threshold value for the TCP flow.

**Example**

The following command sets the threshold value to *3145728* bytes:

**heavy-session detection-threshold 3145728**

# mode

Configures the operating mode for the Cisco Ultra Traffic Optimization engine.

**Product** P-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > ACS Configuration > Traffic Optimization Profile Configuration

**active-charging service** *service_name* **> traffic-optimization-profile**

Entering the above command sequence results in the following prompt:

`[local]host_name(config-traffic-optim)#`

**Syntax Description** **mode [ active | passive ]**

**mode**

Sets the mode of operation for Traffic Optimization.

**trial-mode**

Enables the Crowd Sourcing Optimation feature in the Trial Mode.

**Syntax**

**trial-mode start-time**
*YYYYMMDDHHMM* **end-time** *YYYYMMDDHHMM* **mode-toggle-interval** *mode_toggle_interval*
**initial-mode** *initial_active | initial_passive*

**active**

The mode where both Traffic Optimization and flow monitoring is done on the packet.

**passive**

The mode where no flow-control is performed but monitoring is done on the packet.

**Usage Guidelines** Use this command to set the operating mode for the Cisco Ultra Traffic Optimization engine.

**Example**

The following command sets the operating mode to **active**:

```
mode active
```

# stats-interval

This command configures the flow statistics collection and reporting interval.

**Product** P-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > ACS Configuration > Traffic Optimization Profile Configuration

**active-charging service** *service_name* **> traffic-optimization-profile**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-traffic-optim)#
```

**Syntax Description** **`[ no ] stats-interval`**

**no**

If previously configured, disables collection of flow statistics.

**stats-interval**

Configures the flow statistics collection and reporting interval in seconds. The interval value is an integer that ranges from 1 to 60 seconds.

**Usage Guidelines** Use this command to collect and report flow statistics.

# stats-options

This command configures options to collect the flow statistics.

**Product** P-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Traffic Optimization Profile Configuration

**active-charging service** *service_name* > **traffic-optimization-profile**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-traffic-optim)#
```

**Syntax Description**

**`[ no ] stats-options { flow-analyst [ flow-trace ] | flow-trace [ flow-analyst ] }`**

**no**

If previously configured, disables trace collection and reporting.

**flow-analyst**

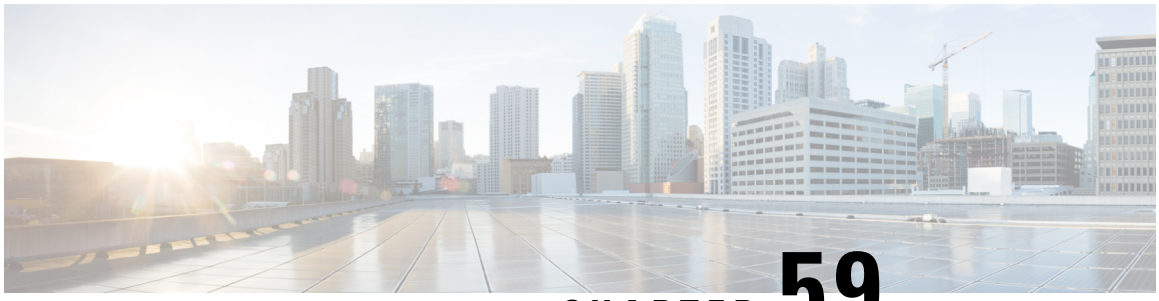
Enables flow analysis, and large trace collection and reporting.

**flow-trace**

Enables flow trace collection and reporting.

**Usage Guidelines**

Use this command to enable trace collectiona and reporting.



CHAPTER 59

# Traffic Policy-Map Configuration Mode Commands

A Policy-Map imposes a flow-based traffic policy for Traffic Policy feature within a destination context. It designates the flow treatment based on the classification rules configured in Class-Map mode for a subscriber session flow.

**Command Modes**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure > context** *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

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


- 3gpp2 data-over-signaling, on page 736
- access-control, on page 736
- accounting suppress, on page 737
- accounting trigger, on page 738
- class-map, on page 740
- description, on page 741
- do show, on page 741
- end, on page 742
- exit, on page 742
- flow-tp-trigger, on page 742
- ip header-compression, on page 743
- qos encaps-header, on page 744
- qos traffic-police, on page 745
- qos user-datagram dscp-marking, on page 747
- sess-tp-trigger, on page 748
- type, on page 749

# 3gpp2 data-over-signaling

Configures 3GPP2-related flow treatment policy for the flow-based traffic policing of subscriber sessions.

**Product**

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure > context** *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**3gpp2 data-over-signaling marking [ class-map** *class_name* **]**
**no 3gpp2 data-over-signaling marking**

**no**

Disables configured 3GPP2-related flow treatment policy.

**class-map *class_name***

Associates class map to be used for selective data over signaling (DOS) marking. *class_name* is an alphanumeric string of 1 through 15 characters.

**marking**

Indicates 3GPP2-related traffic flow for data over signaling channel.

**Usage Guidelines**

Use this command to mark traffic flows for 3GPP2-related policy.

**Example**

**3gpp2 data-over-signaling marking**

# access-control

Configures the access control action for traffic flows matching the Class-Map rules.

**Product**

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure > context** *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**`access-control { allow | discard }`**

**allow**

Allows the packets, if the policy matches with the criteria defined in the Class-Map assigned to the specific traffic policy.

**discard**

Discards the packets, if the policy matches with the criteria defined in the Class-Map assigned to the specific traffic policy.

**Usage Guidelines**

Configures the action or treatment for traffic flows match criteria specified in the assigned Class-Map.

**Example**

The following command allows the packets or traffic flow on matching with criteria specified in assigned Class-Map for specific traffic policy.

**`access-control allow`**

# accounting suppress

Suppresses accounting action for traffic flows matching the policy map.

**Product**

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure > context** *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**`[ no ] accounting suppress`**

**no**

Removes the suppression of accounting for traffic flow matching this policy map.

**Usage Guidelines**

Use this command to suppress accounting action on traffic flow matching this policy map.

Policy maps configured for accounting suppression are used to implement the QChat Billing Suppression feature that selectively starts and terminates accounting sessions based on the categorization of traffic as being interesting or non-interesting. See the **accounting trigger** command.

**Example**

The following command configures suppression of accounting on traffic flows matching this policy map:

**`accounting suppress`**

# accounting trigger

Configures an accounting trigger policy map to selectively start and terminate accounting sessions based on the categorization of traffic as being interesting or non-interesting. This command supports the QCHAT Billing Suppression feature.

**Product**

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure** > **context** *context_name* > **policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

## Syntax Description

**[ no | default ] accounting trigger { inactivity-timeout | interesting-traffic | intra-service-handoff }**

### default

Sets or restores the default value assigned for specified parameter.

### no

Disables previously configured triggers.

### inactivity-timeout

Generates an accounting Stop message if there has been no data activity on the session for the interim accounting timeout interval.

Default: disabled

### interesting-traffic

Generates an accounting Start message upon arrival of interesting traffic.

Default: disabled

### intra-service-handoff

Generates accounting Start and Stop messages during intra-service handoffs.

Default: enabled

If disabled, the messages are suppressed during the handoffs. The current accounting session continues and no Stop or Start messages are generated during the intra-service handoff.

## Usage Guidelines

Use this command to configure an accounting trigger policy map (ATPM) to selectively start and terminate accounting sessions based on the categorization of traffic as being interesting or non-interesting. This command supports the QChat Billing Suppression feature.

Interesting traffic is identified as traffic that does not match any of the other Accounting Policy Maps (APMs) configured for accounting suppression. See the **accounting suppress** command.

An ATPM is similar to an APM, but without the class map rules. The ATPM is configured as of type accounting using the **type accounting** command.

Optionally, timeout can be triggered when there is no data traffic for the interim accounting timeout interval using the **accounting trigger inactivity-timeout stop** command. On timeout, the accounting session is terminated and an Accounting Stop message is sent. A new accounting session is created if interesting traffic resumes.

In the ATPM, the trigger to start accounting for interesting traffic is configured using the **accounting trigger interesting-traffic** command. Accounting Start is triggered on arrival of interesting traffic, or change in airlink parameters conveyed through active-start airlink record. If an active-start record was included in the initial

connection setup, Accounting Start is not triggered. But if the active-start comes separately and is the first one for the session, it is treated as airlink change and an Accounting Start is sent.

The ATPM should have the lowest precedence among the APMs.

As the airlink events are generated on the ingress side, the ATPM must be included in a policy group that is applied to the ingress direction in the subscriber profile. The configuration is applicable only for standard trigger policy and session based accounting mode.

### Example

The following command sets the trigger to generate accounting start message upon arrival of interesting traffic:

```
accounting trigger interesting-traffic
```

# class-map

Assigns a traffic classification rule (Class-Map) to the policy map.

**Product**

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure > context** *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] class-map** *name*

***no***

Enables or disables **class-map**.

***name***

Specifies the name of the class map assigned for this policy map. The class map should have been preconfigured via the Class Map Configuration Mode.

*name* must be an alphanumeric a string of 1 through 15 characters.

**Usage Guidelines** Use this command to assign a class map to the policy map for traffic policing. The class map is configured in the Class Map Configuration Mode.

### Example

The following command assigns the class map *classification1* to the current policy map:

```
class classification1
```

# description

Allows you to enter descriptive text for this configuration.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
description text
no description
```

#### no

Clears the description for this configuration.

#### *text*

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

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

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

# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# flow-tp-trigger

This command specifies that the traffic volume will be calculated based on the traffic on the flow.

**Product** ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure > context** *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**flow-tp-trigger volume** *traffic_volume_threshold*
**no flow-tp-trigger volume**

***traffic_volume_threshold***

Specifies the volume threshold to trigger traffic policing. *volume* must be an integer from 1 through 4294967295.

**Usage Guidelines**

This command is available if you have purchased and installed the Intelligent Traffic Control License on your system. Use this command to calculate the traffic volume based on the traffic on the flow.

**Example**

**flow-tp-trigger volume 500**

# ip header-compression

Enables the system to mark IP flows for Robust Header Compression (RoHC).

**Product**

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure > context** *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] ip header-compression rohc flow-marking**

**no**

Disables the setting.

**rohc flow-marking**

Marks the IP flow for SO67 and PPP RoHC.

**Usage Guidelines**

Use this command to mark IP flows for SO67 and PPP RoHC.

**Example**

```
ip header-compression rohc flow-marking
```

# qos encaps-header

Enables and configures Quality of Service (QoS) policy to use Differentiated Service Code Point (DSCP) marking in IP header fields for the flow-based traffic policing to subscriber session flow.

**Product**

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure > context** *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
qos encaps-header dscp-marking { dscp_code | copy-from-user-datagram [
ignore-pcf-signaled-dscp ] | user-datagram }
no qos encaps-header dscp-marking { dscp_code | copy-from-user-datagram [
ignore-pcf-signaled-dscp ] }
```

**no**

Enables/Disables the **qos encaps-header**.

The value must be expressed as a hexadecimal value from 0x00 through 0x3F.

**dscp-marking *dscp_code***

Uses the DSCP code value marked in the IP header of packet/flow to determine the QoS for traffic policing. *dscp_code* must be expressed as a hexadecimal number from 0x00 through 0x3F.

**copy-from-user-datagram**

Uses the DSCP code value from the user datagram (UDP header) to determine the QoS for traffic policing.

**ignore-pcf-signaled-dscp**

Overrides the highest priority DSCP value signaled by the PCF.

**user-datagram**

Uses the DSCP value copied from the user datagram.

**Usage Guidelines** Use this command to apply the QoS policy based on the DSCP value encapsulated in the IP packet header to police subscriber session traffic flows.



**Important** For more information on the QoS traffic policing, see the *System Administration Guide*.

**Example**

The following command sets QoS policy with DSCP code value to *0x0C* for Class 1, silver (AF12):

```
qos encaps-header dscp-marking 0x0c
```

# qos traffic-police

Enables and configures Quality of Service (QoS) policy for flow-based traffic policing of subscriber session flows on a per-flow basis.

**Product**

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure > context** *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**qos traffic-police committed** *bps* **peak** *bps* **burst-size** *byte* **exceed-action { drop | lower-ip-precedence | allow } violate-action { drop | lower-ip-precedence | allow }**
**no qos traffic-police**

**no**

Enables/Disables the **qos traffic-police**

**Important** This parameter should be configured to be greater than the following two values: 1) three times greater than packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the "bucket" for the configured peak-data-rate.

**burst-size *bytes***

Default: 3000

Specifies the allowed peak burst size in bytes. *bytes* must be an integer from 0 through 4294967295.

**Important** This parameter should be configured to be greater than the following two values: 1) three times greater than the packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the "bucket" for the configured peak-data-rate.

**committed *bps***

Default: 144000

Specifies the committed data rate (guaranteed-data-rate) in bits per second (bps).

*bps* must be an integer from 0 through 4294967295.

**exceed-action { drop | lower-ip-precedence | allow }**

Default: **lower-ip-precedence**

Specifies the action to take on packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:

**drop**: Drops the packet

**lower-ip-precedence**: Transmits the packet after lowering the ip-precedence

**allow**: Transmits the packet

**peak *bps***

Default: 256000

Specifies the peak data-rate for the subscriber in bits per second (bps).

*bps* must be an integer from 0 through 4294967295.

**violate-action { drop | lower-ip-precedence | allow }**

Default: drop

Specifies the action to take on the packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

**drop**: Drops the packet

**lower-ip-precedence**: Transmits the packet after lowering the IP precedence

**allow**: Transmits the packet

**Usage Guidelines** Use this command to apply the QoS policy to a subscriber session flow for flow-based traffic policing.

**Important** For additional information on the QoS traffic policing, see the *System Administration Guide*.

### Example

The following command sets the committed data rate to *102400* bps with a peak data rate of *128000* bps and a burst size of *2048* bytes. This lowers the IP precedence when the committed-data-rate is exceeded and drops the packets when the peak-data-rate are violated:

```
qos traffic-police commited 102400 peak 128000 burst-size 2048
exceed-action lower-ip-precedence violate-action drop
```

# qos user-datagram dscp-marking

Enables and configures Quality of Service (QoS) policy related to differentiated service code point (DSCP) marking in the user datagrams of subscriber session flows on a per-flow basis.

**Product** ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure > context** *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**qos user-datagram dscp-marking** *dscp_code*
**no qos user-datagram dscp-marking**

***dscp_code***

Specifies the use of the DSCP code value marked in the IP header of packet/flow to determine the QoS for traffic policing. *dscp_code* must be expressed as a hexadecimal number from 0x00 through 0x3F.

**Usage Guidelines**

Use this command to apply the QoS policy to subscriber session flow by DSCP marking in user datagram.

**Example**

The following command sets DSCP marking for user datagram as *0x01* for QoS to subscriber session flow:

**qos user-datagram dscp-marking 0x01**

# sess-tp-trigger

Configures the trigger for traffic policing based on the traffic volume for a subscriber session.

**Product**

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure** > **context** *context_name* > **policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**sess-tp-trigger volume** *volume* **direction { both | downlink | uplink }**
**no sess-tp-trigger**

**no**

Enables or disables the **sess-tp-trigger**

***volume***

Specifies the traffic volume threshold (in bytes) that triggers traffic control. *volume* is an integer from 1 through 4294967295.

**Usage Guidelines**

Use this command to trigger traffic control based on the traffic volume for a subscriber session. This command requires the purchase and installation of a license.

**Example**

```
sess-tp-trigger 500
```

# type

Specifies the type of traffic policy within a specific Policy-Map.

**Product**

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure > context** *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**type { accounting | dynamic { three-gpp2 rev-A profile-id { any | id** *profile_id* **| range** *low_value* **to** *high_value* **} flow-id { any | id** *flow_id* **| range** *low_value* **to** *high_value* **} | pre-provisioned wimax asn-service-profile-id { any | id** *service_id* **} asn-pdfid { any | id** *pdf_id* **} | static | template }**

**accounting**

Specifies the type of traffic policing as accounting for this specific policy map. This configuration is used for enabling/disabling the accounting of different flows matching conditions within this Policy-Map.

**dynamic**

Identifies the type of policy map as dynamic.

**three-gpp2 rev-A**

Configures the dynamic policy map type for CDMA2000-3GPP2 RevA service.

**profile-id { any | id *profile_id* | range *low_hex* to *high_hex* }**

Specifies the profile id matching within this policy map.

**any**: allows any profile identifier matching this policy map.

**id** *profile_id*: allows specific profile identifier matching with in this policy map. *profile_id* must be a hexadecimal number from 0x0 to 0xFFFF.

**range** *low_value* **to** *high_value*: identifies a range in which a profile identifier must fall within to be considered a match. *low_value* and *high_value* must be either a hexadecimal number from 0x0 to 0xFFFF, or an integer from 0 through 65535 characters.

**flow-id { any | id *flow_id* | range *low_hex* to *high_hex* }**

Specifies the flow id matching in this policy map.

**any** allows any flow identifier matching with in this policy map.

**id** *flow_id* allows specific flow identifier matching with in this policy map. *flow_id* must be either a a hexadecimal number from 0x0 to 0xFFFF, or an integer from 0 to 65535.

**range** *low_value* **to** *high_value*: identifies a range in which a flow identifier must fall within to be considered a match. *low_value* and *high_value* must be either a hexadecimal number from 0x0 to 0xFFFF, or an integer 0 to 65535.

**pre-provisioned**

Identifies the type of policy map as pre-provisioned.

**wimax**

Configures WiMAX service policy map in an ASN-GW service.

**asn-service-profile { any | id *service_id* }**

Specifies the ASN Service profile identifier to match with in this policy map.

**any**: Allows any ASN Service Profile Identifier matching within this policy map.

**id** *service_id*: Allows specific Service Profile matching to a specified identifier. *service_id* must be an integer from 1 to 65535 that matches a service ID that was configured in the Subscriber Configuration Mode.

**asn-pdfid { any | id *pdf_id* }**

Specifies the ASN Packet Data Flow Identifier to match with in this policy map.

**any**: Allows any ASN Packet Data Flow Identifier matching within this policy map.

**id** *pdf_id*: Allows specific Packet Data Flow matching to a specified identifier. *pdf_id* must be an integer from 1 to 255 that matches a PDF ID that was configured in the Subscriber Configuration Mode.

**static**

Specifies the type of traffic policing as static for this specific Policy Map. In this type of policy, the traffic flow classification and flow treatment is pre-defined with classification rules through Class-Map configuration.

This is the detailed type of policy map.

**template**

Specifies the type of traffic policy to as a template to all subscribers associated with this policy map.

## Usage Guidelines

Specifies the type of traffic policy within the specific Policy-Map.

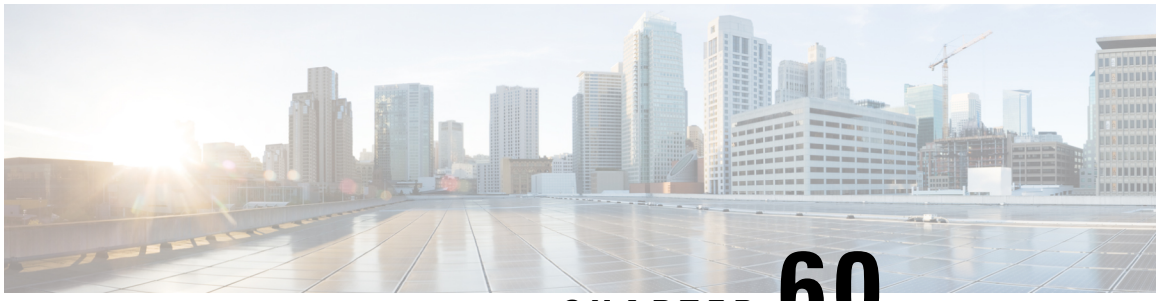
### Example

The following commands configures the traffic policy for this Policy-Map as static:

```
type static
```

The following commands configures the traffic policy for this Policy-Map as pre-provisioned for WiMAX service requiring a match of any service profile and PDF id of *3*:

```
type pre-provisioned wimax asn-service-profile any asn-pdfid id 3
```



CHAPTER 60

# Traffic Policy Group Configuration Mode Commands

Policy-Group is used to form a set of configured Policy-Maps for the Traffic Policy feature. Multiple policies can be applied for a subscriber session flow within a destination context.

**Command Modes**

Exec > Global Configuration > Context Configuration > Traffic Policy Group Configuration

**configure > context** *context_name* **> policy-group name** *group_name*

Entering the above command sequence results in the following prompt:

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

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


- 3gpp2 data-over-signaling, on page 754
- access-control, on page 754
- accounting suppress, on page 755
- accounting trigger, on page 756
- class-map, on page 758
- description, on page 759
- do show, on page 759
- end, on page 760
- exit, on page 760
- flow-tp-trigger, on page 760
- ip header-compression, on page 761
- qos encaps-header, on page 762
- qos traffic-police, on page 763
- qos user-datagram dscp-marking, on page 765
- sess-tp-trigger, on page 766
- type, on page 767

# 3gpp2 data-over-signaling

Configures 3GPP2-related flow treatment policy for the flow-based traffic policing of subscriber sessions.

**Product**

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure > context** *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**3gpp2 data-over-signaling marking [ class-map** *class_name* **]**
**no 3gpp2 data-over-signaling marking**

**no**

Disables configured 3GPP2-related flow treatment policy.

**class-map *class_name***

Associates class map to be used for selective data over signaling (DOS) marking. *class_name* is an alphanumeric string of 1 through 15 characters.

**marking**

Indicates 3GPP2-related traffic flow for data over signaling channel.

**Usage Guidelines**

Use this command to mark traffic flows for 3GPP2-related policy.

**Example**

**3gpp2 data-over-signaling marking**

# access-control

Configures the access control action for traffic flows matching the Class-Map rules.

**Product**

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure > context** *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**access-control { allow | discard }**

**allow**

Allows the packets, if the policy matches with the criteria defined in the Class-Map assigned to the specific traffic policy.

**discard**

Discards the packets, if the policy matches with the criteria defined in the Class-Map assigned to the specific traffic policy.

**Usage Guidelines**

Configures the action or treatment for traffic flows match criteria specified in the assigned Class-Map.

**Example**

The following command allows the packets or traffic flow on matching with criteria specified in assigned Class-Map for specific traffic policy.

**access-control allow**

# accounting suppress

Suppresses accounting action for traffic flows matching the policy map.

**Product**

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure > context** *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**`[ no ] accounting suppress`**

**no**

Removes the suppression of accounting for traffic flow matching this policy map.

**Usage Guidelines**

Use this command to suppress accounting action on traffic flow matching this policy map.

Policy maps configured for accounting suppression are used to implement the QChat Billing Suppression feature that selectively starts and terminates accounting sessions based on the categorization of traffic as being interesting or non-interesting. See the **accounting trigger** command.

**Example**

The following command configures suppression of accounting on traffic flows matching this policy map:

**`accounting suppress`**

# accounting trigger

Configures an accounting trigger policy map to selectively start and terminate accounting sessions based on the categorization of traffic as being interesting or non-interesting. This command supports the QCHAT Billing Suppression feature.

**Product**

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure** > **context** *context_name* > **policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

## Syntax Description

**[ no | default ] accounting trigger { inactivity-timeout | interesting-traffic | intra-service-handoff }**

### default

Sets or restores the default value assigned for specified parameter.

### no

Disables previously configured triggers.

### inactivity-timeout

Generates an accounting Stop message if there has been no data activity on the session for the interim accounting timeout interval.

Default: disabled

### interesting-traffic

Generates an accounting Start message upon arrival of interesting traffic.

Default: disabled

### intra-service-handoff

Generates accounting Start and Stop messages during intra-service handoffs.

Default: enabled

If disabled, the messages are suppressed during the handoffs. The current accounting session continues and no Stop or Start messages are generated during the intra-service handoff.

## Usage Guidelines

Use this command to configure an accounting trigger policy map (ATPM) to selectively start and terminate accounting sessions based on the categorization of traffic as being interesting or non-interesting. This command supports the QChat Billing Suppression feature.

Interesting traffic is identified as traffic that does not match any of the other Accounting Policy Maps (APMs) configured for accounting suppression. See the **accounting suppress** command.

An ATPM is similar to an APM, but without the class map rules. The ATPM is configured as of type accounting using the **type accounting** command.

Optionally, timeout can be triggered when there is no data traffic for the interim accounting timeout interval using the **accounting trigger inactivity-timeout stop** command. On timeout, the accounting session is terminated and an Accounting Stop message is sent. A new accounting session is created if interesting traffic resumes.

In the ATPM, the trigger to start accounting for interesting traffic is configured using the **accounting trigger interesting-traffic** command. Accounting Start is triggered on arrival of interesting traffic, or change in airlink parameters conveyed through active-start airlink record. If an active-start record was included in the initial

connection setup, Accounting Start is not triggered. But if the active-start comes separately and is the first one for the session, it is treated as airlink change and an Accounting Start is sent.

The ATPM should have the lowest precedence among the APMs.

As the airlink events are generated on the ingress side, the ATPM must be included in a policy group that is applied to the ingress direction in the subscriber profile. The configuration is applicable only for standard trigger policy and session based accounting mode.

### Example

The following command sets the trigger to generate accounting start message upon arrival of interesting traffic:

```
accounting trigger interesting-traffic
```

# class-map

Assigns a traffic classification rule (Class-Map) to the policy map.

**Product**

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure > context** *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] class-map** *name*

***no***

Enables or disables **class-map**.

***name***

Specifies the name of the class map assigned for this policy map. The class map should have been preconfigured via the Class Map Configuration Mode.

*name* must be an alphanumeric a string of 1 through 15 characters.

**Usage Guidelines** Use this command to assign a class map to the policy map for traffic policing. The class map is configured in the Class Map Configuration Mode.

### Example

The following command assigns the class map *classification1* to the current policy map:

```
class classification1
```

# description

Allows you to enter descriptive text for this configuration.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
description text
no description
```

#### no

Clears the description for this configuration.

#### *text*

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

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

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

# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# flow-tp-trigger

This command specifies that the traffic volume will be calculated based on the traffic on the flow.

**Product** ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure > context** *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**flow-tp-trigger volume** *traffic_volume_threshold*
**no flow-tp-trigger volume**

***traffic_volume_threshold***

Specifies the volume threshold to trigger traffic policing. *volume* must be an integer from 1 through 4294967295.

**Usage Guidelines**

This command is available if you have purchased and installed the Intelligent Traffic Control License on your system. Use this command to calculate the traffic volume based on the traffic on the flow.

**Example**

**flow-tp-trigger volume 500**

# ip header-compression

Enables the system to mark IP flows for Robust Header Compression (RoHC).

**Product**

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure > context** *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] ip header-compression rohc flow-marking**

**no**

Disables the setting.

**rohc flow-marking**

Marks the IP flow for SO67 and PPP RoHC.

**Usage Guidelines** Use this command to mark IP flows for SO67 and PPP RoHC.

**Example**

```
ip header-compression rohc flow-marking
```

# qos encaps-header

Enables and configures Quality of Service (QoS) policy to use Differentiated Service Code Point (DSCP) marking in IP header fields for the flow-based traffic policing to subscriber session flow.

**Product**

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure > context** *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
qos encaps-header dscp-marking { dscp_code | copy-from-user-datagram [
ignore-pcf-signaled-dscp ] | user-datagram }
no qos encaps-header dscp-marking { dscp_code | copy-from-user-datagram [
ignore-pcf-signaled-dscp ] }
```

**no**

Enables/Disables the **qos encaps-header**.

The value must be expressed as a hexadecimal value from 0x00 through 0x3F.

**dscp-marking *dscp_code***

Uses the DSCP code value marked in the IP header of packet/flow to determine the QoS for traffic policing. *dscp_code* must be expressed as a hexadecimal number from 0x00 through 0x3F.

**copy-from-user-datagram**

Uses the DSCP code value from the user datagram (UDP header) to determine the QoS for traffic policing.

**ignore-pcf-signaled-dscp**

Overrides the highest priority DSCP value signaled by the PCF.

**user-datagram**

Uses the DSCP value copied from the user datagram.

**Usage Guidelines** Use this command to apply the QoS policy based on the DSCP value encapsulated in the IP packet header to police subscriber session traffic flows.



**Important** For more information on the QoS traffic policing, see the *System Administration Guide*.

**Example**

The following command sets QoS policy with DSCP code value to *0x0C* for Class 1, silver (AF12):

```
qos encaps-header dscp-marking 0x0c
```

# qos traffic-police

Enables and configures Quality of Service (QoS) policy for flow-based traffic policing of subscriber session flows on a per-flow basis.

**Product**

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure > context** *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**qos traffic-police committed** *bps* **peak** *bps* **burst-size** *byte* **exceed-action { drop | lower-ip-precedence | allow } violate-action { drop | lower-ip-precedence | allow }**
**no qos traffic-police**

**no**

Enables/Disables the **qos traffic-police**

**Important** This parameter should be configured to be greater than the following two values: 1) three times greater than packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the "bucket" for the configured peak-data-rate.

**burst-size *bytes***

Default: 3000

Specifies the allowed peak burst size in bytes. *bytes* must be an integer from 0 through 4294967295.

**Important** This parameter should be configured to be greater than the following two values: 1) three times greater than the packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the "bucket" for the configured peak-data-rate.

**committed *bps***

Default: 144000

Specifies the committed data rate (guaranteed-data-rate) in bits per second (bps).

*bps* must be an integer from 0 through 4294967295.

**exceed-action { drop | lower-ip-precedence | allow }**

Default: **lower-ip-precedence**

Specifies the action to take on packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:

**drop**: Drops the packet

**lower-ip-precedence**: Transmits the packet after lowering the ip-precedence

**allow**: Transmits the packet

**peak *bps***

Default: 256000

Specifies the peak data-rate for the subscriber in bits per second (bps).

*bps* must be an integer from 0 through 4294967295.

**violate-action { drop | lower-ip-precedence | allow }**

Default: drop

Specifies the action to take on the packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

**drop**: Drops the packet

**lower-ip-precedence**: Transmits the packet after lowering the IP precedence

**allow**: Transmits the packet

**Usage Guidelines** Use this command to apply the QoS policy to a subscriber session flow for flow-based traffic policing.



**Important** For additional information on the QoS traffic policing, see the *System Administration Guide*.

### Example

The following command sets the committed data rate to *102400* bps with a peak data rate of *128000* bps and a burst size of *2048* bytes. This lowers the IP precedence when the committed-data-rate is exceeded and drops the packets when the peak-data-rate are violated:

```
qos traffic-police commited 102400 peak 128000 burst-size 2048
exceed-action lower-ip-precedence violate-action drop
```

# qos user-datagram dscp-marking

Enables and configures Quality of Service (QoS) policy related to differentiated service code point (DSCP) marking in the user datagrams of subscriber session flows on a per-flow basis.

**Product** ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure > context** *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**qos user-datagram dscp-marking** *dscp_code*
**no qos user-datagram dscp-marking**

***dscp_code***

Specifies the use of the DSCP code value marked in the IP header of packet/flow to determine the QoS for traffic policing. *dscp_code* must be expressed as a hexadecimal number from 0x00 through 0x3F.

**Usage Guidelines**

Use this command to apply the QoS policy to subscriber session flow by DSCP marking in user datagram.

**Example**

The following command sets DSCP marking for user datagram as *0x01* for QoS to subscriber session flow:

**qos user-datagram dscp-marking 0x01**

# sess-tp-trigger

Configures the trigger for traffic policing based on the traffic volume for a subscriber session.

**Product**

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure** > **context** *context_name* > **policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**sess-tp-trigger volume** *volume* **direction { both | downlink | uplink }**
**no sess-tp-trigger**

**no**

Enables or disables the **sess-tp-trigger**

***volume***

Specifies the traffic volume threshold (in bytes) that triggers traffic control. *volume* is an integer from 1 through 4294967295.

**Usage Guidelines**

Use this command to trigger traffic control based on the traffic volume for a subscriber session. This command requires the purchase and installation of a license.

**Example**

```
sess-tp-trigger 500
```

# type

Specifies the type of traffic policy within a specific Policy-Map.

**Product**

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

**configure > context** *context_name* **> policy-map name** *map_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**type { accounting | dynamic { three-gpp2 rev-A profile-id { any | id** *profile_id* **| range** *low_value* **to** *high_value* **} flow-id { any | id** *flow_id* **| range** *low_value* **to** *high_value* **} | pre-provisioned wimax asn-service-profile-id { any | id** *service_id* **} asn-pdfid { any | id** *pdf_id* **} | static | template }**

**accounting**

Specifies the type of traffic policing as accounting for this specific policy map. This configuration is used for enabling/disabling the accounting of different flows matching conditions within this Policy-Map.

**dynamic**

Identifies the type of policy map as dynamic.

**three-gpp2 rev-A**

Configures the dynamic policy map type for CDMA2000-3GPP2 RevA service.

**profile-id { any | id *profile_id* | range *low_hex* to *high_hex* }**

Specifies the profile id matching within this policy map.

**any**: allows any profile identifier matching this policy map.

**id** *profile_id*: allows specific profile identifier matching with in this policy map. *profile_id* must be a hexadecimal number from 0x0 to 0xFFFF.

**range** *low_value* **to** *high_value*: identifies a range in which a profile identifier must fall within to be considered a match. *low_value* and *high_value* must be either a hexadecimal number from 0x0 to 0xFFFF, or an integer from 0 through 65535 characters.

**flow-id { any | id *flow_id* | range *low_hex* to *high_hex* }**

Specifies the flow id matching in this policy map.

**any** allows any flow identifier matching with in this policy map.

**id** *flow_id* allows specific flow identifier matching with in this policy map. *flow_id* must be either a a hexadecimal number from 0x0 to 0xFFFF, or an integer from 0 to 65535.

**range** *low_value* **to** *high_value*: identifies a range in which a flow identifier must fall within to be considered a match. *low_value* and *high_value* must be either a hexadecimal number from 0x0 to 0xFFFF, or an integer 0 to 65535.

**pre-provisioned**

Identifies the type of policy map as pre-provisioned.

**wimax**

Configures WiMAX service policy map in an ASN-GW service.

**asn-service-profile { any | id *service_id* }**

Specifies the ASN Service profile identifier to match with in this policy map.

**any**: Allows any ASN Service Profile Identifier matching within this policy map.

**id** *service_id*: Allows specific Service Profile matching to a specified identifier. *service_id* must be an integer from 1 to 65535 that matches a service ID that was configured in the Subscriber Configuration Mode.

**asn-pdfid { any | id *pdf_id* }**

Specifies the ASN Packet Data Flow Identifier to match with in this policy map.

**any**: Allows any ASN Packet Data Flow Identifier matching within this policy map.

**id** *pdf_id*: Allows specific Packet Data Flow matching to a specified identifier. *pdf_id* must be an integer from 1 to 255 that matches a PDF ID that was configured in the Subscriber Configuration Mode.

**static**

Specifies the type of traffic policing as static for this specific Policy Map. In this type of policy, the traffic flow classification and flow treatment is pre-defined with classification rules through Class-Map configuration.

This is the detailed type of policy map.

**template**

Specifies the type of traffic policy to as a template to all subscribers associated with this policy map.

## Usage Guidelines

Specifies the type of traffic policy within the specific Policy-Map.

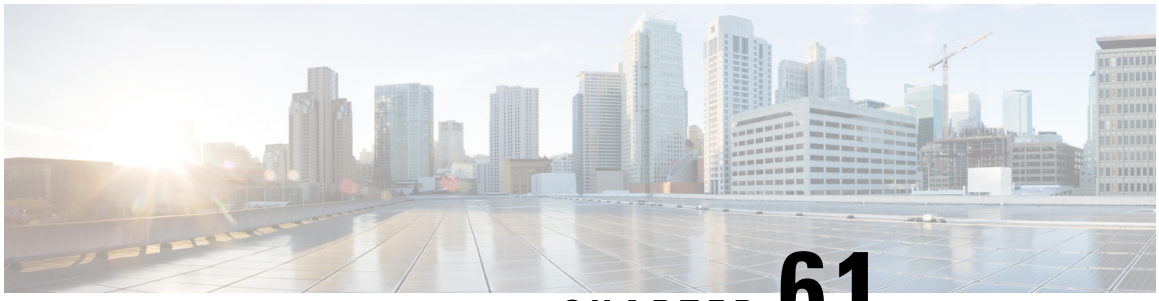
### Example

The following commands configures the traffic policy for this Policy-Map as static:

```
type static
```

The following commands configures the traffic policy for this Policy-Map as pre-provisioned for WiMAX service requiring a match of any service profile and PDF id of *3*:

```
type pre-provisioned wimax asn-service-profile any asn-pdfid id 3
```



CHAPTER 61

# Traffic Steering Configuration Mode Commands

The Traffic Steering Configuration Mode, which works on StarOS, is used to forward user data streams to external appliances or servers through an alternate SGi interface. This mode enhances user experience by performing tasks, such as optimizing traffic streams and segregating traffic.

**Command Modes**

Exec > Global Configuration > Traffic Steering

**configure > traffic-steering**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-traffic-steering)#
```


- appliance-group, on page 771
- do show, on page 772
- end, on page 772
- exit, on page 772
- service-chain, on page 773


# appliance-group

This command allows you to configure appliance group for traffic steering.

**Product**

P-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Traffic Steering

**configure > traffic-steering**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-traffic-steering)#
```

**Syntax Description**

**appliance-group** *appliance_group_name*

***appliance_group_name***

Specifies the name of the appliance group. The name is a string ranging from 1 to 63 characters.

**Usage Guidelines** Use this command to configure an appliance group.

**Example**

The following command sets the appliance group name to *appliance1*:

```
appliance-group appliance1
```

# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
end
```

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **`exit`**

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

# service-chain

This command allows you to configure service chain.

**Product** P-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Traffic Steering

**configure > traffic-steering**

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-traffic-steering)#`

**Syntax Description** **`service-chain`** *`service_chain_name`*

***service_chain_name***

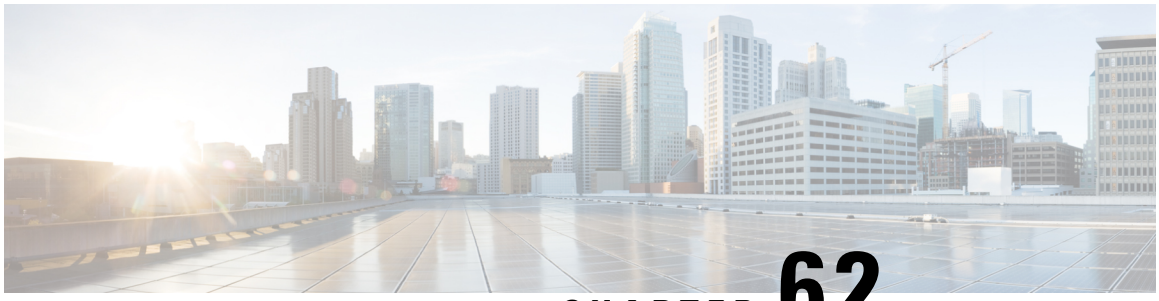
Specifies the name of the service chain. The name is a string ranging from 1 to 63 characters.

**Usage Guidelines** Use this command to configure a service chain.

### Example

The following command sets the service chain to *sch1*:

**`service-chain sch1`**



CHAPTER 62

# Traffic Steering Appliance Group Configuration Mode Commands

The Traffic Steering Appliance Group is used to define the appliances to which the user traffic is forwarded. You can configure an Appliance Group under the Traffic-Steering mode.

**Command Modes**

Exec > Global Configuration > Traffic Steering > Appliance Group

**configure > traffic-steering > appliance-group**

Entering the above command sequence results in the following prompt:

`[local]host_name(config-traffic-steering-app-grp)#`


- do show, on page 775
- end, on page 776
- exit, on page 776
- ip, on page 776
- nsh-format, on page 777


# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

`do show`

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# ip

This command allows you to configure details related to an IP address.

**Product** P-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Traffic Steering > Appliance Group

**configure > traffic-steering > appliance-group**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-traffic-steering-app-grp)#
```

**Syntax Description** **ip address {***ip_address(IPv4/IPv6)* **| preserve-orig-addr }**

**address**

Specifies the IP address; either IPv4 or IPv6.

**preserve-orig-addr**

This keyword when configured uses the same Destination IP as that of original packet.

**Usage Guidelines** Use this command to define the IP address of an external appliance. If you wish to use same IP addresses for both source and destination as that of the original packet, then you need to configure the **preserve-orig-addr**value for IP.



**Note** You can configure either the IP address of the external appliance or preserve same IP addresses for both source and destination. Both the IP configurations do not work at the same time.

**Example**

The following command sets the IP address of an external appliance to *1.1.1.1*:

**ip address 1.1.1.1**

The following command sets the same Destination IP as that of original packet:

**ip address preserve-orig-addr**

# nsh-format

This command allows you to associate NSH format with the appliance group.

**Product** P-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Traffic Steering > Appliance Group

**configure > traffic-steering > appliance-group**

Entering the above command sequence results in the following prompt:

`[local]host_name(config-traffic-steering-app-grp)#`

**Syntax Description** **nsh-format** *nsh_format_name*

***nsh_format_name***

Specifies the NSH format name. The name is a string ranging from 1 to 63 characters.

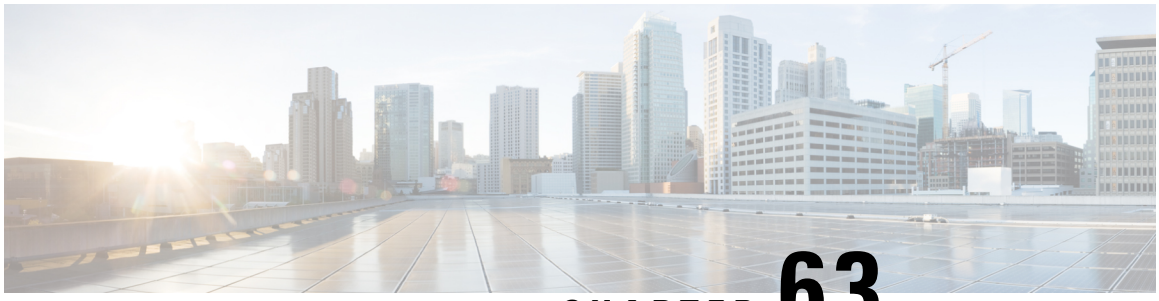
## Usage Guidelines

Use this command to configure NSH format for each appliance. With this configuration, Star-OS communicates with the appliances through NSH protocol.

### Example

The following command configures the NSH format for an appliance to *nsh1*:

```
nsh-format nsh1
```



CHAPTER 63

# Traffic Steering Service Chain Configuration Mode Commands

Traffic Steering uses the concept of service-chaining. Hence, define a Service Chain in the Traffic Steering mode.

**Command Modes**

Exec > Global Configuration > Traffic Steering > Service Chain

Entering the above command sequence results in the following prompt:

`[local]host_name(config-service-chain)#`


- do show, on page 779
- end, on page 780
- exit, on page 780
- load-balancing, on page 780
- sfp, on page 781


## do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# load-balancing

This command allows you to choose an algorithm to balance load among the appliances.

**Product** P-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Traffic Steering > Service Chain

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-service-chain)#
```

**Syntax Description** **load-balancing round-robbin**

**round-robbin**

Specifies the round robin algorithm. By default, round-robbin is used as the load-balancing algorithm.

**Usage Guidelines** Use this command to choose an algorithm to load balance among the appliances.

**Example**

The following command sets the default load balancing algorithm:

**load-balancing round-robbin**

# sfp

This command allows you to configure a Service Function Path (SFP). The SFP is a path that an NSH packet takes in the service-chain.

**Product** P-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Traffic Steering > Service Chain

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-service-chain)#`

**Syntax Description** **sfp direction uplink service-index** *service_index_value* **appliance-group** *appliance_group_name*

**direction**

Moves the packet to the specified direction. The options for directions are listed as follows:

- Uplink—Applies the service function path to an uplink packet.

**service-index**

Specifies the sequence of an appliance in SFP. A maximum of 4 appliances can be configured in an SFP.

For example, **service-index** *1* indicates the first appliance in SFP.

**Usage Guidelines** Use this command to configure the SFP for an NSH packet that it should take in the service-chain. The **sfp direction** field defines the SFP path for uplink or downlink packets. For example, **sfp direction uplink** defines an SFP for uplink user packets.

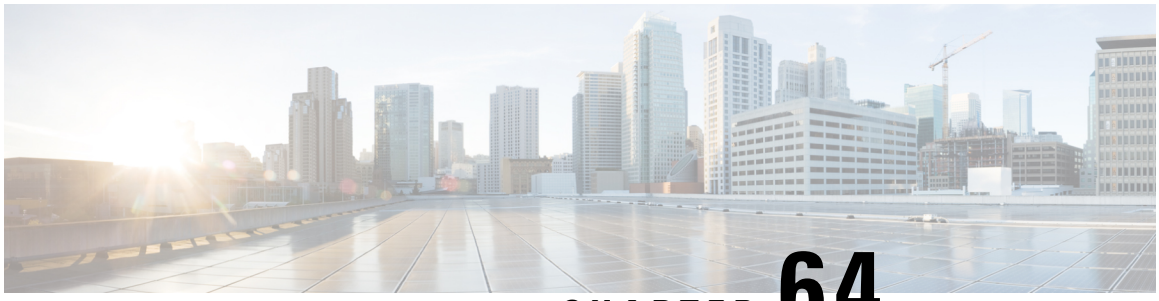
The SFP contains multiple appliances. Details of the sequence of these appliances in SFP is available with StarOS. .

Configure the sequence of appliances by using service-index. For example, **service-index** *1* indicates the first appliance in SFP.

### Example

The following command configures the SFP for a uplink packet in which the appliance group *firewall* is set to *2* as the service index:

```
sfp direction uplink service-index 2 appliance-group firewall
```



CHAPTER 64

# TSI Server Configuration Mode Commands

**Command Modes**

Exec > Global Configuration > Security Configuration > TSI Server Configuration

**configure > security > server talos-intelligence** *server-name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-server-tsi)#`

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


- do show, on page 783
- end, on page 784
- exit, on page 784
- ip, on page 784
- logging, on page 785
- sftp, on page 786
- update-time, on page 787


# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**do show**

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# ip

Configures the IP address and port number used to communicate with the Talos Security Intelligence (TSI) database server (Mediator).

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Security Configuration > TSI Server Configuration

**configure > security > server talos-intelligence** *server-name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-server-tsi)#
```

**Syntax Description**

```
ip address ip_address port port_number
no ip
```

**no ip**

Removes the configured TSI server.

**address *ip_address***

Specifies the IP address of the TSI database server (Mediator) from which security updates are received.

*ip_address* must be specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**port *port_number***

Specifies the port number used to communicate with the TSI server (Mediator).

*port_number* must specified as **5341** for successful communication with the TSI database server..

**Usage Guidelines**

Use this command to configure the IP address and port number for the system to connect to the TSI database server.

**Example**

The following command configures the system to connect to a TSI server with the IP address of 10.1.10.10 on port number 5341:

```
ip address 10.1.10.10 port 5341
```

# logging

Configures the logging level for connection events to the TSI database server events and transactions.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Security Configuration > TSI Server Configuration

**configure > security > server talos-intelligence** *server-name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-server-tsi)#
```

**Syntax Description**

```
logging level { error | warning | unusual | info | debug }
no logging
```

**no logging**

Removes the configured event logging level and returns the system to the default logging level of **error**.

**level { error | warning | unusual | info | debug }**

Specifies the level of information to be logged for TSI database server connectivity events. The following severities are supported:

- **error** – log error events and all events with a higher severity level
- **warning** – log warning events and all events with a higher severity level
- **unusual** – log unusual events and all events with a higher severity level
- **info** – log info events and all events with a higher severity level
- **debug** – log all events.

The default logging level severity is **error**.

**Usage Guidelines** Use this command to set the logging level for events and transactions with the TSI database server.

# sftp

Configures the SFTP port number used to pull database updates from the Talos Security Intelligence (TSI) database server (Mediator).

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Security Configuration > TSI Server Configuration

**configure > security > server talos-intelligence** *server-name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-server-tsi)#
```

**Syntax Description** **[ no ] port** *port_number*

**no**

Removes the configured port number.

***port_number***

Specifies the SFTP port number used to retrieve updates from the TSI database server (Mediator).

*port_number* must specified as **2222** for successful communication with the TSI database server.

**Usage Guidelines** Use this command to configure the SFTP port number for the system to retrieve update files from the TSI database server.

Update files are stored locally in /hd-raid/tsi/update.

# update-time

Configures the time of day when the system shall contact the Talos Security Intelligence (TSI) database server (Mediator) for security updates.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Security Configuration > TSI Server Configuration

**configure > security > server talos-intelligence** *server-name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-server-tsi)#
```

**Syntax Description**

```
update-time hour value minute value
no update-time
```

**no update-time**

Removes the configured time of day when the system retrieves security updates.

**hour *value***

Specifies the hour of the day when the system retrieves security updates.

*value* must be an integer from 0 through 23.

The default is a value of zero for both hour and minute which results in a UTC of midnight.

**minute *value***

Specifies the hour of the day when the system retrieves security updates.

*value* must be an integer from 0 through 59.

The default is a value of zero for both hour and minute which results in a UTC of midnight.

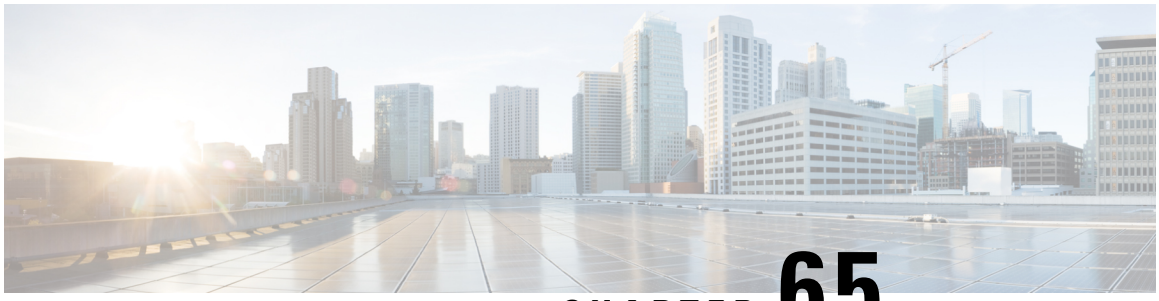
**Usage Guidelines**

Use this command to configure time of day when the system shall connect to the TSI database server to retrieve security updates. The security databases are updated once a day.

**Example**

The following command configures the system to connect to a TSI server at 11:00 PM:

```
update-time hour 23 minute 0
```



CHAPTER 65

# Tunnel Interface Configuration Mode Commands

**Command Modes**

The Tunnel Interface Configuration Mode is used to create and manage the L2TP interface parameters within a specified context.

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

**configure > context** *context_name* **> interface** *interface_name* **tunnel**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-tunnel)#
```

**Important** Available commands or keywords/variables vary based on platform type, product version, and installed license(s).


- description, on page 790
- end, on page 790
- exit, on page 790
- ip address, on page 791
- ip ospf authentication-key, on page 792
- ip ospf authentication-type, on page 792
- ip ospf bfd, on page 793
- ip ospf cost, on page 794
- ip ospf dead-interval, on page 794
- ip ospf hello-interval, on page 795
- ip ospf message-digest-key, on page 796
- ip ospf network, on page 796
- ip ospf priority, on page 797
- ip ospf retransmit-interval, on page 798
- ip ospf transmit-delay, on page 799
- ip vrf, on page 799
- ipv6 address, on page 800
- tunnel-mode, on page 801

# description

Sets the descriptive text for the current interface.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**description** *text*
**no description**

**no**

Clears the description for the interface.

***text***

Specifies the descriptive text as an alphanumeric string of 0 through 79 characters.

**Usage Guidelines**

Set the description to provide useful information on the interface's primary function, services, end users, etc. Any information useful may be provided.

**Example**

**description sampleInterfaceDescriptiveText**

# end

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**end**

**Usage Guidelines**

Use this command to return to the Exec mode.

# exit

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description** `exit`

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

# ip address

Specifies the primary and optional secondary IPv4 addresses and subnets for this interface.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
ip address ip_address { mask | /mask } [ secondary ip_address ] [ srp-activate ]
no ip address ip_address
```

**no**

Removes the IPv4 address from this interface.

***ip_address*{ mask | /*mask* }**

Configures the IPv4 address and mask for the interface. *ip_address* must be entered using IPv4 dotted-decimal notation. IPv4 dotted-decimal or CIDR notation is accepted for the mask.



**Important** For IPv4 addresses, 31-bit subnet masks are supported per RFC 3021.

**secondary *ip_address***

Configures a secondary IPv4 address on the interface.



**Important** You must configure the primary IPv4 address before you will be allowed to configure a secondary address.

**srp-activate**

Activates the IP address for Interchassis Session Recovery (ICSR). Enable this IPv4 address when the Service Redundancy Protocol (SRP) determines that this chassis is ACTIVE. Requires an ICSR license on the chassis to activate.

**Usage Guidelines** The following command specifies the primary IP address and subnets for this interface.

**Example**

The following example configures an IPv4 address for this interface:

```
ip address 192.154.3.5/24
```

# ip ospf authentication-key

Configures the password for authentication with neighboring Open Shortest Path First (OSPF) routers.

**Product**

PDSN

HA

GGSN

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
ip ospf authentication-key [ encrypted ] password auth_key
no ip ospf authentication-key
```

**no**

Deletes the authentication key.

**encrypted**

Use this keyword if you are pasting a previously encrypted authentication key into the CLI command.

**password *auth_key***

Specifies the password to use for authentication as an alphanumeric string of 1 through 16 characters entered in clear text format.

**Usage Guidelines**

Use this command to set the authentication key used when authenticating with neighboring routers.

**Example**

To set the authentication key to 123abc, use the following command;

```
ip ospf authentication-key password 123abc
```

Use the following command to delete the authentication key;

```
no ip ospf authentication-key
```

# ip ospf authentication-type

Configures the OSPF authentication method to be used with OSPF neighbors over the logical interface.

**Product**

PDSN

HA

GGSN

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
ip ospf authentication-type { message-digest | null | text }
no ip ospf authentication-type { message-digest | null | text }
```

**no**

Disable this function.

**message-digest**

Uses the message digest (MD) authentication method.

**null**

Uses no authentication, thus disabling either MD or clear text methods.

**text**

Uses the clear text authentication method.

**Usage Guidelines**

Use this command to set the type of authentication to use when authenticating with neighboring routers.

**Example**

To set the authentication type to use clear text, enter the following command;

```
ip ospf authentication-type text
```

# ip ospf bfd

Enables or disables OSPF Bidirectional Forwarding Detection (BFD) on this interface.

**Product**

PDSN

HA

GGSN

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
ip ospf bfd [ disable ]
no ip ospf cost
```

**no**

Disable this function.

**disable**

Disables OSPF BFD on this interface.

**Usage Guidelines**

Enable or disable OSPF Bidirectional Forwarding Detection (BFD) on this interface.

### Example

Use the following command to enable OSPF BFD;

```
ip ospf bfd
```

# ip ospf cost

Configures the cost associated with sending a packet over the OSPF logical interface.

**Product**

PDSN

HA

GGSN

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
ip ospf cost value
no ip ospf cost
```

**no**

Disable this function.

***value***

Specifies the cost to assign to OSPF packets as an integer from 1 through 65535. Default: 10

**Usage Guidelines**

Use this command to set the cost associated with routes from the interface.

### Example

Use the following command to set the cost to *20*;

```
ip ospf cost 20
```

Use the following command to disable the cost setting;

```
no ip ospf cost
```

# ip ospf dead-interval

Configures the interval that the router should wait, during which time no packets are received and after which the router considers a neighboring router to be off-line.

**Product**

PDSN

HA

GGSN

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**`[ no ] ip ospf dead-interval`** *`seconds`*

**no**

Returns the value to its default of 40 seconds.

***seconds***

Specifies the interval (in seconds) as an integer from 1 through 65535. This number is typical four times the hello-interval. Default: 40

**Usage Guidelines**

Use this command to set the dead intervals for OSPF communications.

**Example**

To set the dead-interval to *100*, use the following command;

```
ip ospf dead-interval 100
```

# ip ospf hello-interval

Configures the interval (in seconds) between sending OSPF hello packets.

**Product**

PDSN

HA

GGSN

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**`ip ospf hello-interval`** *`seconds`*
**`no ip ospf hello-interval`**

**no**

Returns the value to its default of 10 seconds.

***seconds***

Specifies the number of seconds between sending hello packets as an integer from 1 through 65535. Default: 10

**Usage Guidelines**

Specify the interval (in seconds) between sending OSPF hello packets.

**Example**

To set the hello-interval to *25*, use the following command;

```
ip ospf hello-interval 25
```

# ip ospf message-digest-key

Enables or disables the use of MD5-based OSPF authentication.

**Product**

PDSN

HA

GGSN

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**ip ospf message-digest-key** *key_id* **md5 [ encrypted ] password** *authentication_key*
**no ip ospf message-digest-key** *key_id*

**no**

Deletes the key.

**message-digest-key *key_id***

Specifies the key identifier number as an integer from 1 through 255.

**encrypted**

Use this if you are pasting a previously encrypted authentication key into the CLI command.

**password *authentication_key***

Specifies the password to use for authentication as an alphanumeric string of 1 through 16 characters entered in clear text format.

**Usage Guidelines**

Use this command to create an authentication key that uses MD5-based OSPF authentication.

**Example**

To create a key with the ID of *25* and a password of *123abc*, use the following command;

```
ip ospf message-digest-key 25 md5 password 123abc
```

To delete the same key, enter the following command;

```
no ip ospf message-digest-key 25
```

# ip ospf network

Configures the Open Shortest path First (OSPF) network type.

**Product**

PDSN

HA

GGSN

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
ip ospf network { broadcast | non-broadcast | point-to-multipoint |
point-to-point }
no ip ospf network
```

**no**

Disable this function.

**broadcast**

Sets the network type to broadcast.

**non-broadcast**

Sets the network type to non-broadcast multi access (NBMA).

**point-to-multipoint**

Sets the network type to point-to-multipoint.

**point-to-point**

Sets the network type to point-to-point.

**Usage Guidelines**

Use this command to specify the OSPF network type.

**Example**

To set the OSPF network type to *broadcast*, enter the following command;

```
ip ospf network broadcast
```

To disable the OSPF network type, enter the following command;

```
no ip ospf network
```

# ip ospf priority

Designates the OSPF router priority.

**Product**

PDSN

HA

GGSN

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
ip ospf priority value
no ip ospf priority value
```

**no**

Disable this function.

***value***

Sets the priority value as an integer from 0 through 255.

**Usage Guidelines**

Use this command to set the OSPF router priority.

**Example**

To set the priority to *25*, enter the following command:

```
ip ospf priority 25
```

To disable the priority, enter the following command:

```
no ip ospf priority
```

# ip ospf retransmit-interval

Configures the interval in (seconds) between LSA (Link State Advertisement) retransmissions.

**Product**

PDSN

HA

GGSN

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
ip ospf retransmit-interval seconds
no ip ospf retransmit-interval
```

**no**

Returns the value to its default of 5 seconds.

***seconds***

Specifies the number of seconds between LSA (Link State Advertisement) retransmissions as an integer from 1 through 65535. Default: 5

**Usage Guidelines**

Configure the interval in (seconds) between LSA (Link State Advertisement) retransmissions.

**Example**

To set the retransmit-interval to *10*, use the following command;

```
ip ospf retransmit-interval 10
```

# ip ospf transmit-delay

Configures the interval (in seconds) that the router should wait before transmitting an OSPF packet.

**Product**

PDSN

HA

GGSN

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**ip ospf transmit-delay** *seconds*
**no ip ospf transmit-delay**

**no**

Returns the value to its default of 1 second.

***seconds***

Specifies the number of seconds that the router should wait before transmitting a packet as an integer from 1 through 65535. Default: 1

**Usage Guidelines**

Configure the interval (in seconds) that the router should wait before transmitting an OSPF packet.

**Example**

To set the transmit-delay to 5, use the following command;

```
ip ospf transmit-delay 5
```

# ip vrf

Associates this interface with a specific Virtual Routing and Forwarding (VRF) table.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**[ no ] ip vrf forwarding** *vrf_name*

**no**

Removes the specified VRF table from this interface.

***vrf_name***

Specifies the name of an existing VRF table as an alphanumeric string of 1 through 63 characters.

Use the Context Configuration mode **ip vrf forwarding** command to preconfigure the VRF name.

**Usage Guidelines** The following command specifies a ranged IP address for this interface.

**Example**

The following example elasticities this interface with VRF named *vrf_012*:

```
ip vrf forwarding vrf_012
```

# ipv6 address

Specifies an IPv6 address and subnet mask.

**Product** PDSN

HA

**Privilege** Security Administrator, Administrator

**Syntax Description** **[ no ] ipv6 address** *ipv6_address/mask*

**no**

Removes the IPv6 address from this interface.

***ipv6_address/mask***

Specifies an individual host IP address to add to this host pool in IPv6 colon-separated-hexadecimal CIDR notation.



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

**Usage Guidelines** Configures the IPv6 address and subnet mask for a specific interface.

**Example**

The following example configures an IPv6 address for this interface:

```
ipv6 address 2002:0:0:0:0:0:c014:101/128
```

# tunnel-mode

Configures mode (transport protocol) of the tunnel.

**Product**

All products that support IPSec

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
tunnel-mode { gre | ipv6ip }
default tunnel-mode
```

#### default

Sets the default tunnel mode for this interface which is IPv6-to-IPv4 type.

#### gre

Sets the tunnel interface mode to Generic Routing Encapsulation (GRE) type and enters the GRE Tunnel Configuration mode, if required.



**Important** This keyword is only available if an optional GRE Interface Tunneling license is installed to create IP-GRE tunnels.

#### ipv6ip

Sets the tunnel interface mode to IPv6-to-IPv4 type and creates the IPv6-to-IPv4 Tunnel Configuration mode, if required. This is the default mode.

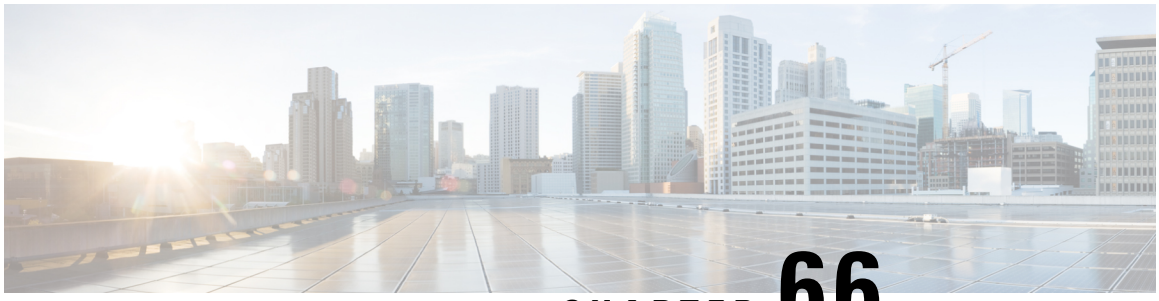
**Usage Guidelines**

Use this command to set the tunnel mode type of GRE or IPv6-to-IPv4 for the tunneling interface. For SaMOG (S2a Mobility Over GTP), use the **tunnel-mode gre** command to configure a GRE tunnel for the IP-over-GRE feature.

#### Example

The following example configures GRE tunnel-mode for this interface:

```
tunnel-mode gre
```



CHAPTER 66

# TWAN Profile Configuration Mode Commands

**Command Modes**

The TWAN Profile Configuration Mode is used to configure the Radius client addresses (WLC) and access-type corresponding to the Radius clients to enable SaMOG to attach a session to a specific WiFi Access Network.

Exec > Global Configuration > Context Configuration > TWAN Profile Configuration

**configure > context** *context_name* **> twan-profile** *twan_profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-twan-profile)#`

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


- access-type, on page 803
- dictionary, on page 805
- do show, on page 805
- end, on page 806
- exit, on page 806
- radius, on page 806
- session-trigger, on page 809
- ue-address, on page 810


# access-type

This command allows you to specify the access-type for the RADIUS client or specify a default access type for all RADIUS clients under a TWAN profile.

**Product** SaMOG

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > TWAN Profile Configuration

**configure > context** *context_name* **> twan-profile** *twan_profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-twan-profile)#
```

## Syntax Description

```
access-type client { ipv4 | ipv6_address[/mask ] } { eogre | ip | pmip }
access-type { eogre | ip [ vrf vrf_name ]| pmip }
no access-type { client { ipv4/ipv6_address[/mask  ] } | eogre | ip [ vrf ]
| pmip }
```

### no

Removes the previously configured access type for the TWAN profile.

### client { *ipv4* | *ipv6_address*[/*mask* ] }

Specifies the IP address of the RADIUS client.

*ipv4* | *ipv6_address* must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. *mask* must be a subnet mask bit of the IP address. The mask bit is a numeric value which corresponds to the number of bits in the subnet mask.

### ip [ vrf *vrf_name* ]

Specifies that all RADIUS clients under this TWAN profile will use the Layer 3 IP (L3IP) access type.

**vrf**: Specifies to use the VRF name to install the IP flow for L3IP subscriber session.

*vrf_name* must be an alphanumeric string between 1 and 63 characters.

### eogre

Specifies that all RADIUS clients under this TWAN profile will use the Ethernet over GRE (EoGRE) access type.

### pmip

Specifies that all RADIUS clients under this TWAN profile will use the Proxy Mobile IP version 6 (PMIPv6) access type.

## Usage Guidelines

Use this command to configure the access type for a specific NAS/WLC IP address or IP address with a subnet mask, or a common access type for the entire TWAN profile.

### Example

The following command sets the default access type for the TWAN profile to EoGRE

```
access-type eogre arg1
```

The following command configures a RADIUS client with IP address *192.168.15.50* with access type as *eogre*, and a client with IP address *192.168.16.50* with access type as *pmip* under the current TWAN profile.

```
access-type client 192.168.15.50 eogre
access-type client 192.168.16.50 pmip
```

# dictionary

Configure the dictionary to be used to forward the permanent identity of the subscriber to the AAA server.

**Product**

SaMOG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > TWAN Profile Configuration

**configure > context** *context_name* **> twan-profile** *twan_profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-twan-profile)#`

**Syntax Description**

**dictionary { custom70 | custom71 }**
**default dictionary**

**default**

Configures the dictionary to its default value.

Default: custom70

**Usage Guidelines**

Use this command to configure the dictionary to forward the permanent identity of the subscriber to the AAA server. The dictionary configuration at the TWAN profile level will be applied to all the RADIUS clients under that TWAN profile.

Configure the custom71 dictionary when Cisco WLC is used with PMIPv6 as the access-type. Configuring the custom71 dictionary enables attributes like the UE's permanent identity (NAI), subscribed APN, network protocol (PMIPv6), and LMA address (CGW service's bind address) to be sent in the Cisco Vendor-specific attributes to WLC. The WLC uses this information to build the PMIPv6 PBU to the SaMOG gateway when the **aaa-override** option is enabled on the Cisco WLC. These attributes are not sent when the custom70 dictionary is configured.

To configure the dictionary to use for individual RADIUS clients, use the **dictionary** keyword in the **radius client** command under the TWAN Profile Configuration Mode.

**Example**

The following command configures the TWAN profile to use custom71 dictionary:

**dictionary custom71**

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege** Security Administrator, Administrator

**Syntax Description** `do show`

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `end`

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `exit`

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

# radius

This command allows you to specify the IP address and shared secret of the RADIUS accounting and authentication client from which RADIUS accounting and authentication requests are received or configure the Radius VRF for an IPoVLAN model.

**Product**

SaMOG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > TWAN Profile Configuration

**configure > context** *context_name* **> twan-profile** *twan_profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-twan-profile)#
```

**Syntax Description**

```
radius { client ipv4 | ipv6_address[/mask ] [ encrypted ] key value [
disconnect-message [ dest-port destination_port_number ] ] [ dictionary {
custom70 | custom71 } ] | ip vrf vrf_name }
no radius { client ipv4/ipv6_address[/mask ] | ip vrf vrf_name }
radius cisco-mpc-protocol-interface { none | eogre | pmipv6 | suppress }
[ no ] radius cisco-mpc-protocol-interface
```

**no**

Removes the previously configured RADIUS client address or IP VRF under this TWAN profile.

**client { *ipv4* | *ipv6_address*[/*mask* ] }**

Specifies the IP address of the RADIUS client (WLC).

*ipv4* | *ipv6_address* must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. *mask* must be a subnet mask bit of the IP address. The mask bit is a numeric value which corresponds to the number of bits in the subnet mask.



**Important** A maximum of 16 RADIUS clients can be configured under one TWAN profile.

**[ encrypted ] key *value***

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

The key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 288 characters with encryption enabled.

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

**disconnect-message**

Specifies to send RADIUS disconnect message to the configured RADIUS accounting client in call failure scenarios.

**dest-port *destination_port_number***

Specifies the port number to which the disconnect message must be sent.

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

**dictionary { custom70 | custom71 }**

Specifies to forward the permanent identity of the subcriber to the AAA server using the custom70 or custom71 dictionary.

Configure the custom71 dictionary when Cisco WLC is used with PMIPv6 as the access-type. Configuring the custom71 dictionary enables attributes like the UE's permanent identity (NAI), subscribed APN, network protocol (PMIPv6), and LMA address (CGW service's bind address) to be sent in the Cisco Vendor-specific attributes to WLC. The WLC uses this information to build the PMIPv6 PBU to the SaMOG gateway when the **aaa-override** option is enabled on the Cisco WLC. These attributes are not sent when the custom70 dictionary is configured.

To configure the dictionary to use for all RADIUS clients belonging to a specific TWAN profile, use the **dictionary** command under the TWAN Profile Configuration Mode.

Default: custom70

**ip vrf *vrf_name***

Associates the specific TWAN profile with a Virtual Routing and Forwarding (VRF) Context instance for RADIUS communication.

*vrf_name* must be an alphanumeric string from 1 through 63 characters.

**cisco-mpc-protocol-interface**

Configures cisco-mpc-protocol-interface AVP for access-type eogre-pmip.

**none**

Configures cisco-mpc-protocol-interface AVP as none. It is neither eogre nor pmipv6.

**eogre**

Configures cisco-mpc-protocol-interface AVP as eogre.

**pmipv6**

Configures cisco-mpc-protocol-interface AVP as pmipv6

**suppress**

Suppresses cisco-mpc-protocol-interface AVP and it is not sent in the Access-Accept message.

**no**

Removes configuration for cisco-mpc-protocol-interface AVP.

## Usage Guidelines

Use this command to specify the IP address and shared secret of the RADIUS accounting and authentication client from which RADIUS accounting and authentication requests are received or configure the VRF for RADIUS communication.

### Example

The following example configures a RADIUS client with an IP address of *193.14.23.1* and an encrypted key of value *enc32*

```
radius client 193.14.23.1 encrypted key enc32
```

# session-trigger

This command specifies the protocol type that will trigger session creation on the SaMOG Gateway.

**Product**

SaMOG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > TWAN Profile Configuration

**configure > context** *context_name* **> twan-profile** *twan_profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-twan-profile)#
```

**Syntax Description**

```
session-trigger { dhcp [ location { circuit-id | remote-id } ] | radius
[ acct ] | pmip }
default session-trigger
no session-trigger dhcp location
```

#### default

Resets the configuration to its default value.

Default: RADIUS (authentication)-based session trigger.

#### no

If previously configured, removes the DHCP configuration.

#### dhcp [ location { circuit-id | remote-id } ]

Specifies the session trigger protocol as DHCP, and the sub-option to choose the UE location from the DHCP-Relay-Agent-Info option (DHCP option 82).

At least one TWAN profile must have a DHCP session trigger enabled. If multiple TWAN profiles have DHCP session trigger enabled, the first configured TWAN profile with DHCP session trigger is used.

#### radius [ acct ]

Specifies the session trigger protocol as RADIUS messages. The default configuration is RADIUS (authentication)-based session trigger.

**acct**: Specifies to trigger session on receiving RADIUS accounting messages.

**pmip**

Specifies the session trigger protocol as PMIP. SaMOG can create sessions based on the PMIPv6 (PBU) messages from the Access Point (AP).

**Usage Guidelines**

Use this command to specify the protocol type that will trigger session creation on the SaMOG Gateway.

**Important** If this TWAN profile is configured with a DHCP session trigger, the access type must be EoGRE.

**Example**

The following command sets the session trigger to DHCP:

```
session-trigger dhcp location circuit-id
```

The following command sets the session trigger to PMIP:

```
session-trigger pmip
```

# ue-address

This command allows you to specify how the UE address allocation should be handled.

**Product**

SaMOG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > TWAN Profile Configuration

**configure** > **context** *context_name* > **twan-profile** *twan_profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-twan-profile)#
```

**Syntax Description**

```
ue-address { dhcp | twan }
no ue-address
```

**no**

If previously configured, disables the UE allocation configuration.

**dhcp**

Specifies that the UE address will be assigned at SaMOG by P-GW or GGSN, and sent to the UE using DHCP.

**twan**

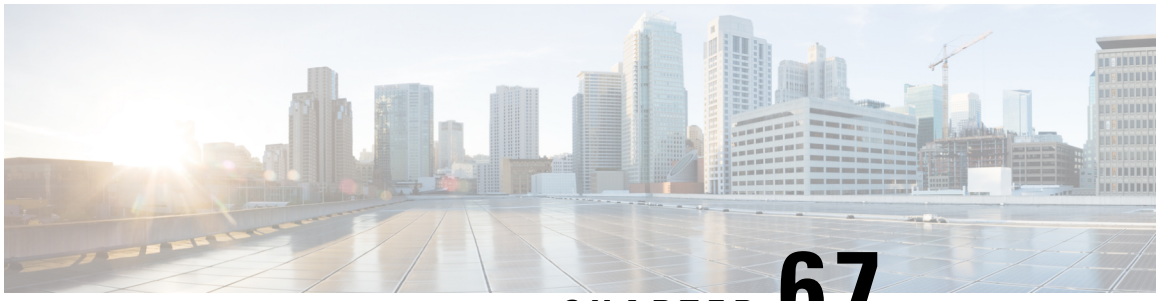
Specifies that the UE address will be assigned at TWAN also. SaMOG receives the TWAN UE address through the Accounting Start Framed-IP-Address message, and NAT is performed between the two UE addresses.

## Usage Guidelines

Use this command to specify how the UE address allocation should be handled. This configuration can be used to detect whether a DHCP request is expected or if the configuration setup is an IP@WLAN (no DHCP required) model.

**Important** If the configured access-type is PMIP or EoGRE, the ue address configuration is ignored.

If the configured access-type is IP, and no ue address is configured, the call setup will fail.



CHAPTER 67

# UDR Format Configuration Mode Commands

The UDR Format Configuration Mode enables configuring User Detail Record (UDR) formats.

**Command Modes**

Exec > ACS Configuration > UDR Format Configuration

**active-charging service** *service_name* > **udr-format** *format_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-udr)#
```

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


- attribute, on page 813
- do show, on page 818
- end, on page 819
- event-label, on page 819
- exit, on page 820
- rule-variable, on page 820


# attribute

This command allows you to specify the fields and their order in UDRs.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > UDR Format Configuration

**active-charging service** *service_name* > **udr-format** *format_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-udr)#
```

## Syntax Description

```
attribute attribute { [ format { MM/DD/YY-HH:MM:SS | MM/DD/YYYY-HH:MM:SS |
 YYYY/MM/DD-HH:MM:SS | YYYYMMDDHHMMSS | seconds } [ localtime ] | [ {
bytes | pkts } { downlink | uplink } ] ] priority priority }
no attribute attribute [ priority priority ]
```

### no

If added previously, removes the specified attribute from the UDR format.

### attribute *attribute*

Specifies the attribute.

*attribute* must be one of the following:

| Attribute | Description |
|---|---|
| **diameter-session-id** | This attribute reports Diameter session identifier.<br>**Important**<br>This attribute is customer specific, and is only available in 8.3 and later r |
| **failure-handling-mode** | This attribute reports failure handling mode in case the Online Charging S abnormal. |
| **nemo-prefix-list** | This attribute reports the VRF names associated with the base session of N MR Prefixes.<br>**Important**<br>This attribute is customer specific, and is available only with NEMO lice |
| **num-nemo-prefix** | This attribute reports the number of NEMO MR Prefixes.<br>**Important**<br>This attribute is customer specific, and is available only with NEMO lice |
| **radius-called-station-id** | This attribute reports the Called Station ID of the mobile handling the flo |
| **radius-calling-station-id** | This attribute reports the Calling Station ID of the mobile handling the fl |
| **radius-fa-nas-identifier** | This attribute reports the RADIUS NAS identifier of Foreign Agent (FA) |
| **radius-fa-nas-ip-address** | This attribute reports the RADIUS IP address of Foreign Agent (FA). |
| **radius-nas-identifier** | This attribute reports the RADIUS NAS identifier. |
| **radius-nas-ip-address** | This attribute reports the RADIUS NAS IP address.<br>Note that this attribute is interchangeable with **sn-st16-ip-addr** for the us |
| **radius-user-name** | This attribute reports the user name associated with the flow. |
| **sn-3gpp2-bsid** | This option has been deprecated.<br>To configure this attribute see the **rule-variable** command. |

| Attribute | Description |
|---|---|
| **sn-3gpp2-carrier-id** | This option has been deprecated.<br>To configure this attribute see the **rule-variable** command. |
| **sn-3gpp2-esn** | This option has been deprecated.<br>To configure this attribute see the **rule-variable** command. |
| **sn-3gpp2-meid** | This option has been deprecated.<br>To configure this attribute see the **rule-variable** command. |
| **sn-3gpp2-service-option** | This option has been deprecated.<br>To configure this attribute see the **rule-variable** command. |
| **sn-acct-beginning-session** | This attribute reports the Session Beginning information.<br>**Important**<br>This attribute is customer specific, and is only available in 8.3 and lat |
| **sn-acct-session-continue** | This attribute reports the Session Continue information.<br>**Important**<br>This attribute is customer specific, and is only available in 8.3 and lat |
| **sn-acct-session-id** | This attribute reports the Accounting Session identifier. |
| **sn-acct-session-time** | This attribute reports the duration from acct-status-type:start to acct-s<br>**Important**<br>This attribute is customer specific, and is only available in 8.3 and lat |
| **sn-acct-status-type** | This attribute reports the Accounting Status identifier.<br>**Important**<br>This attribute is customer specific, and is only available in 8.3 and lat |
| **sn-charging-type** | This attribute reports the charging type: offline or online.<br>**Important**<br>This attribute is customer specific, and is only available in 8.3 and lat |

| Attribute | Description |
|---|---|
| **sn-closure-reason** | This attribute reports the reason for termination of the flow/UDR:<br>• 0 = CALL_TERMINATION — normal, such as subscriber session e<br>• 1 = PDSN_HO — handoff control processing specified<br>• 2 = TIME_LIMIT<br>• 3 = VOLUME_LIMIT<br>• 4 = MGMT_INTERVENTION<br>• 5 = ACCT_SESS_START<br>• 6 = CCRU_RESPONSE<br>• 7 = OFFLINE_CHARGING — for UDRs generated when offline ch received from DCCA |
| **sn-content-id** | This attribute reports the unique identifier for the content-id. |
| **sn-content-label** | This attribute reports the identifier for text label for content-id. |
| **sn-content-vol** | This attribute reports the identifier for content volume. |
| **sn-correlation-id** | This attribute reports the RADIUS correlation identifier. |
| **sn-duration** | This attribute reports the time difference between the first and last packet flow accounted in the UDR record.<br>For example, the time difference between the first ICMP echo request an echo response before the record gets written for the content-id. |
| **sn-end-time [ format** *format***]** | This attribute reports the timestamp for last packet of flow in UTC. |
| **sn-fa-correlation-id** | This attribute reports the RADIUS Correlation Identifier of the Foreign A |
| **sn-fa-ip-address** | This attribute reports IP address of the FA. |
| **sn-filler-blank** | This attribute inserts a blank filler field, generates an empty UDR field. |
| **sn-filler-zero** | This attribute inserts a "0" in the UDR field. |
| **sn-format-name** | This attribute reports name of the UDR format used. |
| **sn-group-id** | This attribute reports the sequence group identifier for the records. |
| **sn-ha-ip-address** | This attribute reports IP address of the Home Agent (HA).<br>**Important**<br>This attribute is customer specific, and is only available in 8.3 and later r |
| **sn-local-seq-no** | This attribute reports unique local sequence number of UDR identifier per A and linearly increasing in UDR file. |

| Attribute | Description |
|---|---|
| **sn-ocs-ip-address** | This attribute reports IP address of the Online Charging Server.<br>**Important**<br>This attribute is customer specific, and is only available in 8.3 and lat |
| **sn-rulebase** | This attribute reports name of the ACS rulebase used. |
| **sn-sequence-no** | This attribute reports unique sequence number (per **sn-sequence-grou**<br>**radius-nas-ip-address**) of UDR identifier and linearly increasing in U |
| **sn-served-bsa-addr** | This attribute reports address of Base Station Area being served. |
| **sn-service-name** | This attribute reports name of the ACS service. |
| **sn-st16-ip-addr** | This option has been deprecated.<br>This attribute reports IP address of the chassis handling this flow.<br>This attribute is interchangeable with **radius-nas-ip-address** for othe |
| **sn-start-time [ format** *format* **]** | This attribute reports timestamp for first packet of flow in UTC. |
| **sn-stream-number** | This attribute reports unique UDR billing record identifier.<br>**Important**<br>This attribute is customer specific, and is only available in 8.3 and lat |
| **sn-subscriber-id** | This attribute reports subscriber ID. |
| **sn-subscriber-ipv4-address** | This attribute reports the IPv4 address of the subscriber. |
| **sn-subscriber-ipv6-address** | This attribute reports the IPv6 address of the subscriber. |
| **sn-subscriber-nat-flow-ip** | This attribute reports NAT IP address(es) of NAT-enabled subscriber. |
| **sn-timestamp** | This attribute reports timestamp when the UDR is actually generated.<br>**Important**<br>This attribute is customer specific, and is only available in 8.3 and lat |
| **sn-vrf-name** | This attribute indicates the VRF name associated with the base sessio<br>**Important**<br>This is a customer-specific attribute. |

**format{ MM/DD/YY-HH:MM:SS | MM/DD/YYYY-HH:MM:SS | YYYY/MM/DD-HH:MM:SS | YYYYMMDDHHMMSS | seconds }**

Specifies the timestamp format.

**localtime**

Specifies the local time. By default, timestamps are displayed in Coordinated Universal Time (UTC).

**{ bytes | pkts }{ downlink | uplink }**

Specifies bytes/packets sent/received from/by mobile.

**priority *priority***

Specifies the position priority of the field within the UDR. Lower numbered priorities (across all attribute, event-label, and rule-variable) occur first.

*priority* must be an integer from 1 through 65535. Up to 50 position priorities (across all attribute, event-label, and rule-variable) can be configured.

**Usage Guidelines**

Use this command to set the attributes and priority for UDR file format.

A particular field in UDR format can be entered multiple times at different priorities. While removing the UDR field using the **no attribute** command, you can either remove all occurrences of a particular field by specifying the field name or remove a single occurrence by additionally specifying the optional **priority** keyword.

Consider the following scenario. If the volume/time threshold interval is large enough (or disabled). At time t=0, 10 ICMP packets are sent, which takes 9 seconds. There is nothing for the next 100 seconds, and then again 10 ICMP packets are sent which takes 10 seconds, and then again nothing for next the 60 seconds and then the session is terminated.

In this scenario:

- sn-start-time should be t = 0.
- sn-end-time should be t = 0+9+100+10 (sn-end-time would be the last ICMP packet sent).
- sn-duration should be sn-end-time minus sn-start-time, i.e. 0+9+100+10 – 0 = 119 seconds (since the ICMP flow would exist between the two intervals of sending ICMP packets, the sn-start-time would be that of the first packet of the flow and sn-end-time of the last packet (20th packet). Hence, sn-duration would take into account all the seconds between the first and last packet of the flow).

**Example**

The following is an example of this command:

```
attribute radius-user-name priority 12
```

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# event-label

This command allows you to specify an optional event label/identifier to be used as an attribute in the UDRs.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > ACS Configuration > UDR Format Configuration

**active-charging service** *service_name* **> udr-format** *format_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-udr)#
```

**Syntax Description**

**event-label** *event_label* **priority** *priority*
**no event-label**

**no**

If previously configured, removes the event label configuration.

***event_label***

Specifies the event label/identifier to be used as UDR attribute.

*event_label* must be an alphanumeric string of 1 through 63 characters.

**priority *priority***

Specifies the Comma Separated Value (CSV) position of the attribute (label/identifier) in the UDR.

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

**Usage Guidelines** Use this command to configure an optional event label/identifier as an attribute in the UDR and its position in the UDR.

**Example**

The following is an example of this command:

```
event-label radius_csv1 priority 23
```

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
exit
```

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

# rule-variable

This command allows you to specify fields and their order in UDRs.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > ACS Configuration > UDR Format Configuration

**active-charging service** *service_name* **> udr-format** *format_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-udr)#
```

**Syntax Description**

```
rule-variable rule_variable priority priority
no rule-variable rule_variable [ priority priority ]
```

**no**

If previously configured, removes the specified rule variable configuration.

**rule-variable *rule_variable***

Specifies the rule variable for the UDR format.

*rule_variable* must be one of the following options:

- **bearer 3gpp2**: Bearer-related configuration:
  - **always-on**
  - **bsid**
  - **carrier-id**
  - **esn**
  - **ip-qos**
  - **ip-technology**
  - **meid**
  - **release-indicator**
  - **serv-MDN**
  - **service-option**
  - **session-begin**
  - **session-continue**



**Important** For more information on protocol-based rules see the *ACS Ruledef Configuration Mode Commands* chapter.

**priority *priority***

Specifies the CSV position of the field (protocol rule) in the UDR.

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

## Usage Guidelines

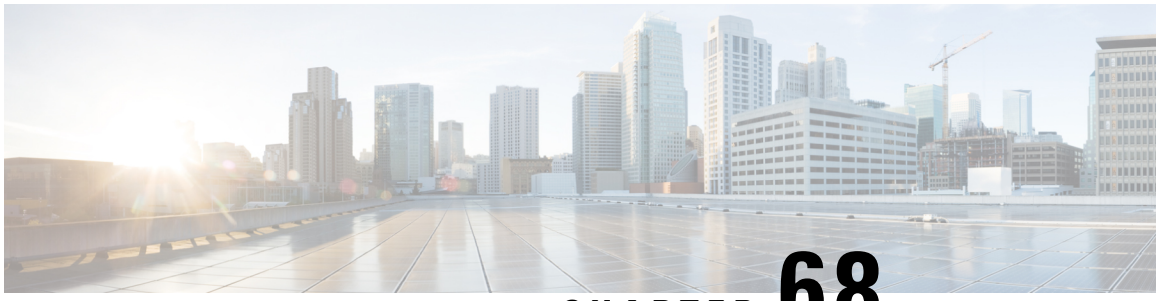
Use this command to specify what field appears in which order in the UDR.

A particular field in UDR format can be entered multiple times at different priorities. While removing the UDR field using the **no rule-variable** command, you can either remove all occurrences of a particular field by specifying the field name, or remove a single occurrence by additionally specifying the optional priority keyword.

### Example

The following is an example of this command:

```
rule-variable bearer 3gpp2 bsid priority 36
```



CHAPTER 68

# UDR Module Configuration Mode Commands

The UDR Module Configuration Mode allows you to configure Usage Data Record (UDR) file transfer parameters.

**Command Modes**

Exec > Global Configuration > Context Configuration > UDR Module Configuration

**configure > context** *context_name* **> udr-module active-charging-service**

Entering the above command sequence results in the following prompt:

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

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


- cdr, on page 823
- do show, on page 828
- end, on page 828
- exit, on page 829
- file, on page 829


# cdr

This command allows you to configure EDR/UDR file transfer parameters.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > UDR Module Configuration

**configure > context** *context_name* **> udr-module active-charging-service**

Entering the above command sequence results in the following prompt:

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

## Syntax Description

**cdr { purge { storage-limit** *storage_limit* **| time-limit** *time_limit* **} [ max-files** *max_records_to_purge* **] | push-interval** *push_interval* **| push-trigger space-usage-percent** *trigger_percentage* **| remove-file-after-transfer | transfer-mode { pull [ module-only ] | push primary { encrypted-url** *encrypted_url* **| url** *url* **} [ [ max-files** *max_records* **] [ max-tasks** *task_num* **] [ module-only ] [ secondary { encrypted-secondary-url** *encrypted_secondary_url* **| secondary-url** *secondary_url* **} ] [ source-address** *ip_address* **] [ via local-context ] + ] | use-harddisk }**
**default cdr [ purge | push-interval | push-trigger space-usage-percent | remove-file-after-transfer | transfer-mode [ pull [ module-only] | push primary via ] | use-harddisk ] +**
**no cdr [ purge | remove-file-after-transfer | use-harddisk ] +** | [**cdr push-count** *push_count* **default cdr push-count**]

### default

Configures the default setting for the specified keyword(s):

- **purge**: Disabled
- **push-interval**: 300 seconds
- **push-trigger**: 80 percent
- **remove-file-after-transfer**: Disabled
- **transfer mode**: Pull
- **push via**: line cardMIO is used for push
- **use-harddisk**: Disabled

**Important** The **use-harddisk** keyword is only available on ASR 5000 chassis.

### no

If previously configured, disables the specified configuration:

- **purge**: Disables purging of records.
- **remove-file-after-transfer**: Retains a copy of the file even after it has been pushed or pulled to another server.
- **use-harddisk**: Disables data storage on the SMC hard disk.

**Important** The **use-harddisk** keyword is available only on the ASR 5000 chassis.

- **push-count** *push_count*: Specifies the number of EDR/CDR/UDR files transferred in each EDR/UDR push SFTP session. Default value is "1". *push_count* is configured as an integer value between 1 and 32, inclusive.

**purge { storage-limit *storage_limit* | time-limit *time_limit* } [ max-files *max_records_to_purge* ]**

Specifies to purge/delete the UDR records based on "time" or "volume" limit.

When the configured threshold limit is reached on the hard disk drive, the records that are created dynamically in the */mnt/hd-raid/data/records/* directory are automatically deleted. Files that are manually created should be deleted manually.

- **storage-limit** *storage_limit*: Specifies to start deleting files when the specified megabytes of space is used for storage.

  *storage_limit* specifies the volume limit for the record files, in megabytes, and must be an integer from 10 through 143360.

- **time-limit** *time_limit*: Specifies to start deleting files older than the specified time limit.

  *time_limit* specifies the time limit for the record files, and must be an integer from 600 through 2592000.

- **max-files** *max_records_to_purge*: Specifies the maximum number of records to purge.

  *max_records_to_purge* can be 0, or an integer from 1000 through 10000. If the value is set to 0, during each cycle, the records will be deleted until the purge condition is satisfied. If the value is set between 1000 and 10000, during each cycle, the records will be deleted until either the purge condition is satisfied or the number of records deleted equals the configured **max-files** value.

  Default: 0

**push-interval *value***

Specifies the transfer interval (in seconds) to push UDR/EDR files to an external file server.

*value* must be an integer from 60 through 3600.

Default: 300

**push-trigger space-usage-percent *trigger_percentage***

Specifies the UDR/EDR disk space utilization percentage, upon reaching which an automatic push is triggered and files are transferred to the configured external server.

*trigger_percentage* specifies the UDR/EDR disk utilization percentage for triggering push, and must be an integer from 10 through 80.

Default: 80%

**remove-file-after-transfer**

Specifies that the system must delete UDR/EDR files after they are transferred to the external file server.

Default: Disabled

**transfer-mode { pull [ module-only ] | push primary { encrypted-url *encrypted_url* | url *url* } [ [ max-files *max_records* ] [ max-tasks *task_num* ] [ module-only ] [ secondary { encrypted-secondary-url *encrypted_secondary_url* | secondary-url *secondary_url* } ] [ source-address *ip_address* ] [ via local-context ] + ]**

Specifies the UDR/EDR file transfer mode.

- **pull**: Specifies that the external storage is to pull the UDR files.

- **push**: Specifies that the system is to push UDR files to the configured external storage.
- **max-files** *max_records*: Specifies the maximum number of files sent per iteration based on configured file size.

  Default: 4000
- **max-tasks** *task_num*: Specifies the maximum number of tasks (child processes) that will be spawned to push the files to the remote server. The *task_num* must be an integer from 4 through 8.

  Default: 4

**Important** Note that increasing the number of child processes will improve the record transfer rate. However, spawning more child will consume additional resource. So, this option needs to be used with proper resource analysis.

- **module-only**: Specifies that the transfer-mode is only applicable to the UDR module; if not configured it is applicable to both EDR and UDR modules. This enables support for individual record transfer-mode configuration for each module.
- **primary encrypted-url** *encrypted_url*: Specifies the primary location in encrypted format to which the system pushes the UDR files.

  *encrypted_url* must be the primary location name in an encrypted format, and must be an alphanumeric string of 1 through 1024 characters.
- **primary url** *url*: Specifies the primary location to which the system pushes the UDR files.

  *url* must be the primary location, and must be an alphanumeric string of 1 through 1024 characters in the format: *//user:password@host:[port]/directory*.
- **secondary encrypted-secondary-url** *encrypted_secondary_url*: Specifies the secondary location in encrypted format to which the system pushes the UDR files when the primary location is unreachable or fails.

  *encrypted_secondary_url* must be the location in an encrypted format, and must be an alphanumeric string of 1 through 1024 characters.
- **secondary secondary-url** *secondary_url*: Specifies the secondary location to which the system pushes the UDR files when the primary location is unreachable or fails.

  *secondary_url* must be the secondary location, and must be an alphanumeric string of 1 through 1024 characters in the format: *//user:password@host:[port]/directory*.
- **source-address** *ip_address*: Configures the source IP address to be used to establish the connection for the SFTP/SSH file-transfer operation.
- **via local-context**: Selects the LC/SPIO for transfer of UDRs. The system pushes the UDR files via SPIO in the local context.
- **via local-context**: Selects the MIO for transfer of UDRs. The system pushes the UDR files via the MIO in the local context.

**use-harddisk**

**Important** The **use-harddisk** keyword is available only on the ASR 5000 chassis.

Specifies that on an ASR 5000 chassis, the hard disk on the SMC will be used to store UDR/EDR files. When configured to use the hard disk for UDR/EDR storage, UDR/EDR files are transferred from packet processing cards to the hard disk on the SMC.

Specifies that on an ASR 5500 chassis, the hard disk array on the FSCs will be used to store UDR/EDR files. On configuring to use the array for UDR/EDR storage, UDR/EDR files are transferred from DPCs to the array.

Default: Disabled

**+**

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

**push-count *push_count***

Specifies the number of EDR/CDR/UDR files transferred in each EDR/UDR push SFTP session. Default value is "1". push_count is configured as an integer value between 1 and 32,inclusive.

**Note** When push_count is set to “1”, file transfer operation is functionally identical to legacy behavior.

## Usage Guidelines

Use this command to configure how UDRs are moved and stored.

On the ST16 chassis, run this command only from the context where the UDR/EDR module is configured. Running this command in any other context will fail and deliver an error message.

On the ASR 5000ASR 5500 chassis, run this command only from the local context. Running in any other context would fail and deliver an error message.

If PUSH transfer mode is configured, the external storage server URL to which the UDR files need to be transferred to must be specified. The configuration allows a primary and a secondary server to be configured. Configuring the secondary server is optional. Whenever a file transfer to the primary server fails for four consecutive times, the files will be transferred to the secondary server. The transfer will switch back to the original primary server when:

- Four consecutive transfer failures to the secondary server occur
- After switching from the primary server, 30 minutes elapses

When changing the transfer-mode from pull to push, disable the PULL from external storage and then change the transfer mode to push. Make sure that the push server URL configured is accessible from the local context. Also, make sure that the base directory that is mentioned contains udr directory created within it.

When changing the transfer-mode from push to pull, after changing, enable PULL on the external storage. Any of the ongoing PUSH activity will continue till all the scheduled file transfers are completed. If there is no PUSH activity going on at the time of this configuration change, all the PUSH related configuration is nullified immediately.

The **cdr use-harddisk** command is available only on the ASR 5000ASR 5500 chassis. This command can be run only in a context where CDRMOD is running. Configuring in any other context will result in failure with the message *"Failure: Please Check if CDRMOD is running in this context or not."*

The **cdr use-harddisk** command can be configured either in the UDR or EDR module, but will be applicable to both record types. Configuring in one of the modules will prevent the configuration to be applied in the other module. Any change to this configuration must be done in the module in which it was configured, the change will be applied to both record types.

The VPNMgr can send a maximum of 4000 files to the remote server per iteration. However if the individual file size is big (say when compression is not enabled), then while transferring 4000 files SFTP operation takes a lot of time. To prevent this, the **cdr transfer-mode push** command can be configured with the keyword **max-files**, which allows operators to configure the maximum number of files sent per iteration based on configured file size.

### Example

The following command configures the system to retain a copy of the data file after it has been transferred to the storage location:

```
no cdr remove-file-after-transfer
```

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# file

This command allows you to configure UDR file parameters.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > UDR Module Configuration

**configure > context** *context_name* **> udr-module active-charging-service**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
file [ charging-service-name { include | omit } ] [ compression { gzip |
 none } ] [ current-prefix string ] [ delete-timeout seconds ] [ directory
directory_name ] [ exclude-checksum-record ] [ field-separator { hyphen |
omit | underscore } ] [ file-sequence-number rulebase-seq-num ] [ headers
 ] [ name file_name ] [ reset-indicator ] [ rotation [ num-records number |
 time seconds | volume bytes ] ] [ sequence-number { length length | omit |
padded | padded-six-length | unpadded } ] [ storage-limit limit ] [
time-stamp { expanded-format | rotated-format | unix-format } ] [
trailing-text string ] [ trap-on-file-delete ] [ udr-seq-num ] [
xor-final-record ] +
default file [ charging-service-name ] [ compression ] [ current-prefix
] [ delete-timeout ] [ directory ] [ field-separator ] [
file-sequence-number ] [ headers ] [ name ] [ reset-indicator ] [ rotation
```

```
{ num-records | time | volume } ] [ sequence-number ] [ storage-limit ]
[ time-stamp ] [ trailing-text ] [ udr-seq-num ]
```

**default**

Configures the default setting for the specified keyword(s). Using the **default file** command will reset some but not all keyword parameters to their default values. To ensure that the default is reset for a specific parameter, include the corresponding keyword in the command.

**charging-service-name { include | omit }**

Specifies to include/exclude name of the charging service in the file name.

- **include**: Includes name of the charging service in the UDR file name.
- **omit**: Excludes name of the charging service in the UDR file name.

Default: **include**

**compression { gzip | none }**

Configures gzip compression of the UDR file.

- **gzip**: Enables GNU zip compression of the UDR file at approximately 10:1 ratio.
- **none**: Disables Gzip compression.

Default: **none**

**current-prefix *string***

Specifies a string to add to the beginning of the UDR file that is currently being used to store UDR records.

*string* must be an alphanumeric string of 1 through 31 characters.

Default: curr

**delete-timeout *seconds***

Specifies a timeout period (in seconds) when completed UDR files are deleted. By default, files are never deleted.

*seconds* must be an integer from 3600 through 31536000.

Default: Disabled

**directory *directory_name***

Specifies a subdirectory in the default directory in which to store UDR files.

*directory_name* must be an alphanumeric string of 1 through 191 characters.

Default: /records/udr

**exclude-checksum-record**

When entered, this keyword excludes the final record containing #CHECKSUM followed by the 32-bit Cyclic Redundancy Check (CRC) of all preceding records from the UDR file.

Default: Disabled, inserts checksum record into the UDR file header.

**field-separator { hyphen | omit | underscore }**

Specifies the field separators to be used between two fields of a UDR file name.

- **hyphen**: Specifies to use '-' (hyphen) as the field separator.
- **omit**: Excludes the field separator.
- **underscore**: Specifies to use '_' (underscore) as the field separator.

Default: **underscore**

**file-sequence-number rulebase-seq-num**

Generates unique file sequence numbers for different rulebase-format-name combinations.

**headers**

Includes a file header summarizing the record layout.

**name *file_name***

Default: udr

Specifies a string to use as the base file name for UDR files.

*file_name* must be an alphanumeric string of 1 through 31 characters. The file name format is as follows:

*base_rulebase_format_sequencenum_timestamp*

- *base*: Specifies type of record in file or contains the operator-specified string. Default: udr
- *rulebase*: Specifies the name of the ACS rulebase. UDRs from different rulebases go into different UDR files.
- *format*: Specifies the name of the UDR format if **single-udr-format** is specified, else the format field (and the trailing underscore) is omitted from the file name.
- *sequencenum*: This is a 5-digit sequence number to detect the missing file sequence. It is unique among all UDR files on the system.
- *timestamp*: Contains a timestamp based on file creation time in UTC formatted as: MMDDYYYYHHMMSS.

UDR files that have not been closed have a string added to the beginning of their file names.

File name for a UDR file in CSV format that contains information for a rulebase named *rulebase1* and a UDR schema named *udr_schema1* appears as follows:

*udr_rulebase1_udr_schema1_00005_01302006143409*

If file name is not configured, the system creates files for EDRs/UDRs/FDRs (xDRs) using the following name template with limits to 256 characters:

*basename_ChargSvcName_ timestamp_SeqNumResetIndicator_FileSeqNumber*

- *basename*: A global-based configurable text string that is unique per system that uniquely identifies the global location of the system running ACS.

- *ChargSvcName*: A system context-based configurable text string that uniquely identifies a specific context-based charging service.
- *timestamp*: Date and time at the instance of file creation. Date and time in the format: "MMDDYYYYHHmmSS", where HH is a 24-hour value from 00-23.
- *SeqNumResetIndicator*: A one-byte counter used to discern the potential for duplicated FileSeqNumber with a range of 0 through 255, which is incremented by a value of 1 for the following conditions:
  - Failure of an ACS software process on an individual packet processing card
  - Failure of the system such that a second system takes over (for example, a standby or backup chassis put in place according to Inter-chassis Session Recovery)
  - File Sequence Number (FileSeqNumber) rollover from 999999999 to 0
- *FileSeqNumber*: unique file sequence number for the file is a 9-digit integer from 000000000 through 999999999. It is unique on each chassis.

File name for a closed xDR file in CSV format that contains information for ACS *xyz_city1* and charging service name *preapaid2* with timestamp *12311969190000*, and file sequence number counter reset indicator to *002* for file sequence number *034939002* appears as follows:

*xyz_city1_preapaid2_12311969190000_002_034939002*

File name for a running xDR file in CSV format that contains information for the same parameters for file sequence number *034939003* prefixed with *curr_* and appears as follows:

*curr_xyz_city1_preapaid2_12311969190000_002_034939002*



**Important** When the "rulebase name" and "edr-format-name" options are enabled through this **file** command, if the "field-separator" value is "underscore" (default value) then, in the filename, the fields Rulebase name and EDR format name will be separated by "hyphen". If the "field-separator" value is "hyphen" then, in the filename, the fields Rulebase name and EDR format name will be separated by "underscore". This will ensure that the number of the fields in the filename is not increased and does not affect the backend billing system.

### reset-indicator

Specifies to include the reset indicator counter value, from 0 to 255, in the UDR file name and is incremented (by one) whenever any of the following conditions occur:

- An ACSMgr/SessMgr process fails.
- An Inter-chassis Session Recovery (ICSR) peer chassis has transitioned from standby to active.
- The sequence number in sequence-number keyword has rolled over to zero.

### rotation { num-records *records* | time *seconds* | volume *bytes* }

Specifies when to close a UDR file and create a new one.

- **num-records** *records*: Specifies the number of records that should be added to the file. When the number of records in the file reaches this specified value, the file is complete.

  *records* must be an integer from 100 through 10240.

Default: 1024

- **time** *seconds*: Specifies the period of time to wait before closing the UDR file and creating a new one.

  *seconds* must be an integer from 30 through 86400.

  Default: 3600 seconds

- **volume** *bytes*: Specifies the maximum size of the UDR file before closing it and creating a new one.

  *bytes* must be an integer from 51200 through 62914560.

  Default: 102400 bytes

  Note that higher settings may provide the best compression ratio when the **compression** keyword is set to *gzip*.

**sequence-number { length *length* | omit | padded | padded-six-length | unpadded }**

Specifies including or excluding the sequence number in the file name.

- **length** *length*: Includes the sequence number with the specified length.

  *length* must be the length of the file sequence number with preceding zeroes in the file name, and must be an integer from 1 through 9.



**Important** The **length** configuration is applicable in both UDR and EDR modules. When applied in both modules without the **file udr-seq-num** configuration, the minimum among the two values will come into effect for both modules. With the **file udr-seq-num** config, each module will use its own value of length.

- **omit**: Excludes the sequence number from the file name.
- **padded**: Includes the padded sequence number with preceding zeros in the file name. This is the default setting.
- **padded-six-length**: Includes the padded sequence number with six preceding zeros in the file name.
- **unpadded**: Includes the unpadded sequence number in the file name.

Default: **padded**

**storage-limit *limit***

Specifies deleting files when the specified amount of space, in bytes, is used up for UDR/EDR file storage on packet processing card RAM.

On an ST16 chassis, *limit* must be an integer from 10485760 through 268435456.

On ASR 5500 chassis, *limit* must be an integer from 10485760 through 536870912.

Default: 33554432



**Important** On the ST16 chassis, the total storage limit is 268435456 bytes (256 MB). This limit is for both UDR and EDR files combined.



**Important** On the ASR 5500 chassis, the total storage limit is 536870912 bytes (512 MB). This limit is for both UDR and EDR files combined.

**time-stamp { expanded-format | rotated-format | unix-format }**

Specifies the timestamp of when the file was created be included in the file name.

- **expanded-format**: Specifies the UTC MMDDYYYYHHMMSS format.
- **rotated-format**: Specifies the YYYYMMDDHHMMSS format.
- **unix-format**: Specifies the UNIX format of *x.y*, where *x* is the number of seconds since 1/1/1970 and *y* is the fractional portion of the current second that has elapsed.

**trailing-text *string***

Specifies the inclusion of arbitrary text string in the file name.

*string* must be an alphanumeric string of 1 through 30 characters.

**trap-on-file-delete**

Instructs the system to send an SNMP notification (starCDRFileRemoved) when an UDR/EDR file is deleted due to lack of space.

Default: Disabled

**udr-seq-num**

Specifies that the file sequence numbers that are part of the UDR file names be independently generated. If disabled, a single set of sequence numbers are shared by both UDR and EDR files.

Default: Disabled

**xor-final-record**

Specifies inserting an XOR checksum (in place of the CRC checksum) into the UDR file header if the **exclude-checksum-record** keyword is left at its default setting.

Default: Disabled

**+**

More than one of the previous keywords can be entered within a single command.

## Usage Guidelines

Use this command to configure UDR file characteristics.

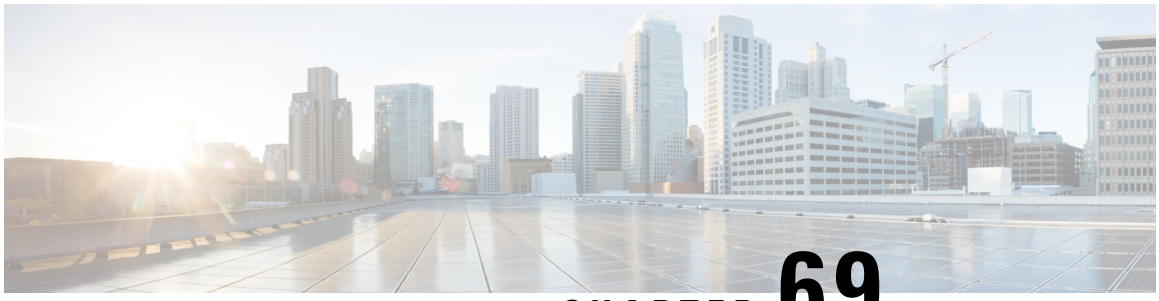
### Example

The following command sets the prefix of the current active UDR file to *current*:

```
file current-prefix current
```

The following command sets the base file name to *UDRfile*:

```
file name UDRfile
```



CHAPTER 69

# UIDH Server Configuration Mode Commands

The UIDH Server Configuration Mode commands are used to configure the parameters when a connection is established with the UIDH Server.

**Command Modes**

Exec > Global Configuration > Context Configuration > UIDH Server Configuration Mode Configuration

**configure > context** *context_name* **> uidh-server** *uidh_server_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(uidh-server)#`


- end, on page 837
- exit, on page 837
- refresh-interval, on page 838
- remote-address, on page 839
- response-timeout, on page 840


## end

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**end**

**Usage Guidelines**

Use this command to return to the Exec mode.

## exit

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description** **exit**

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

# refresh-interval

This command allows you to configure the refresh interval for a UIDH key.

**Product** P-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > UIDH Server Configuration Mode Configuration

**configure > context** *context_name* **> uidh-server** *uidh_server_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(uidh-server)#`

**Syntax Description**

**refresh-interval** *refresh_interval_time*
**default refresh-interval**
**no refresh-interval**

**no**

Deletes the refresh interval parameter from the UIDH server configuration.

**default**

Configures the default interval value in the UIDH server configuration.

***refresh_interval_time***

The refresh interval time is configured in hours and is an integer ranging from 8 to 168 hours. The default interval value is 8 hours.

**Usage Guidelines** Use this command to configure the refresh interval in the UIDH sever configuration.

When a session is attached to P-GW, the P-GW queries the UIDH server. If there is no response from the UIDH server, the UIDH service is not enabled for this session. If there is a Whitelisted subscriber, the UIDH server sends the UIDH string to P-GW. The P-GW queries the UIDH string after the refresh interval.

- On querying, if P-GW does not receive a response, it uses the existing key and sends another request after the refresh interval.
- If P-GW receives a response with an empty string – subscriber moving from OPT-IN to OPT-OUT, it does not perform a key refresh and UIDH insertion is disabled until the subscriber re-attaches.
- Any status change of a subscriber from OPT-OUT to OPT-IN is applied only on subscriber attach. However, the status changes from OPT-IN to OPT-OUT is applied only after refresh interval.

- When a subscriber moves to the OPT-OUT status, it is indicated with the following response: 200 OK Blank Response. This indicates that the request has been processed successfully at the UIDH server and that the subscriber has opted out.

In case of UIDH service failure, either because of a failure in service or because of failure in connection to the UIDH server, the P-GW continues to process the session without inserting the UIDH hash value.

### Example

The following command sets the refresh interval in the UIDH server as 6 hours::

```
refresh-interval 6
```

# remote-address

This command allows you to configure the remote address of the UIDH server.

**Product**

P-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > UIDH Server Configuration Mode Configuration

**configure > context** *context_name* **> uidh-server** *uidh_server_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(uidh-server)#
```

**Syntax Description**

**remote-address** *uidh_address* **port** *uidh_port_number* **local-address** *local_address*
**no remote-address**

#### no

Deletes the remote address configuration from the UIDH Server.

#### port

Configures the remote port address to connect to the UIDH server. The port address is an integer ranging from 1 to 65535.

#### local-address

Configures a local IP address (IPv4/IPv6) to be used to connect to a UIDH server.

**Usage Guidelines**

Use this command to configure the remote address of the UIDH server.

### Example

The following command sets the remote address as 209.165.200.225, port number as 600 and local address as 209.165.200.226:

```
remote-address 209.165.200.225 port 600 local-address 209.165.200.226
```

# response-timeout

This command allows you to configure the response timeout for UIDH requests.

**Product**

P-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > UIDH Server Configuration Mode Configuration

**configure > context** *context_name* **> uidh-server** *uidh_server_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(uidh-server)#
```

**Syntax Description**

**response-timeout** *timeout_value*
**default refresh-interval**
**no remote-address**

**no**

Deletes the response timeout configuration for UIDH requests.

**default**

Configures the default response timeout value for UIDH requests.

***response_timeout***

The timeout value is configured in seconds and is an integer ranging from 1 to 10. The default timeout value is 2 seconds.

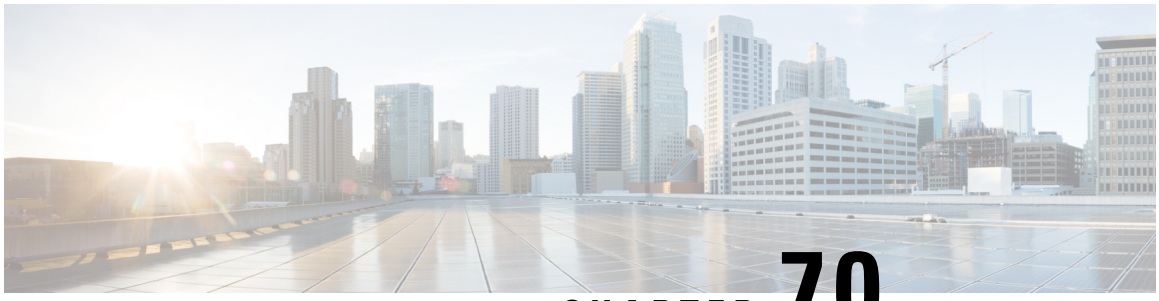
**Usage Guidelines**

Use this command to configure the response timeout value for UIDH requests.

**Example**

The following command sets the response timeout value as 10 seconds in the UIDH requests:

```
response-timeout 10
```



CHAPTER 70

# Unnumbered Interface Configuration Mode Commands

**Command Modes**

The Unnumbered Interface Configuration Mode creates an unnumbered IP interface within a specified context. An unnumbered interface enables IP processing without assigning an explicit IP address to the interface. In StarOS this type of interface supports an untagged BFD port. The only parameter for this type of interface is a text description.

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

**configure > context** *context_name* **> interface** *interface_name* **unnumbered**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-unnumbered)#
```

**Important** Available commands or keywords/variables vary based on platform type, product version, and installed license(s).


- description, on page 841
- end, on page 842
- exit, on page 842


# description

Sets the descriptive text for the current interface.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**description** *text*
**no description**

**no**

Clears the description for the interface.

***text***

Specifies the descriptive text as an alphanumeric string of 0 through 79 characters.

**Usage Guidelines** Set the description to provide useful information on the interface's primary function, services, end users, etc. Any information useful may be provided.

**Example**

```
description sampleInterfaceDescriptiveText
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
end
```

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

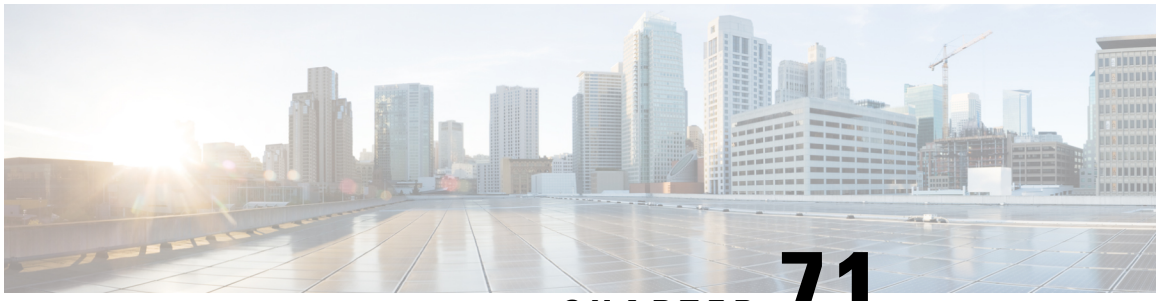
**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
exit
```

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



CHAPTER 71

# UPF Load Control Profile Configuration Mode Commands

Load control profile configuration commands enable the UPF to send its load information to a peer node to adaptively balance the session load across UPFs. The load information reflects the operating status of the resources of the UPF.

**Command Modes**

Exec > Global Configuration >UPF Load Control Profile Configuration

**configure > upf-load-control-profile** *profile_name*

Entering the above command results in the following prompt:

```
[local]UPlane (config-upf-load-control-profile)#
```

**Important** Available commands or keywords/variables vary based on platform type, product version, and installed license(s).


- inclusion-frequency, on page 843
- end, on page 844


# inclusion-frequency

Configures parameters to determine the inclusion frequency of the Load Control Information IE for a UPF Control Profile configuration.

**Product**

UPF

**Privilege**

Administrator, Security Administrator

**Command Modes**

Exec > Global Configuration >UPF Load Control Profile Configuration

**configure > upf-load-control-profile** *profile_name*

Entering this command results in the following prompt:

```
[local]UPlane (config-upf-load-control-profile)#
```

**Syntax Description** **inclusion-frequency { advertisement-interval** *interval_in_seconds* **| change-factor** *change_factor* **}**

**inclusion-frequency**

Specifies that parameters to determine the inclusion frequency of the Load Control Information IE for a UPF Load Control Profile is configured. This parameter specifies how often the operator wants to send this information to the peers.

**advertisement-interval *interval_in_seconds***

Configures the advertisement-interval for Load Control in seconds. Specifies the frequency at which the load control information should be sent to the peers.

*interval_in_seconds* must be an integer 0–3600.

Default: 300

**change-factor *change_factor***

Specifies the percentage change from the previous LCI factor, at which the LCI IE is sent out.

*change_factor* must be an integer 1–20.

Default: 5%

**Usage Guidelines** Use this command to specify parameters to determine the inclusion frequency of the Load control information IE for a UPF Load Control Profile configuration.

**Example**

```
[local]UPlane(config-upf-load-control-profile)# inclusion-frequency advertisement-interval
 300
[local]UPlane(config-upf-load-control-profile)# inclusion-frequency change-factor 5
```

# end

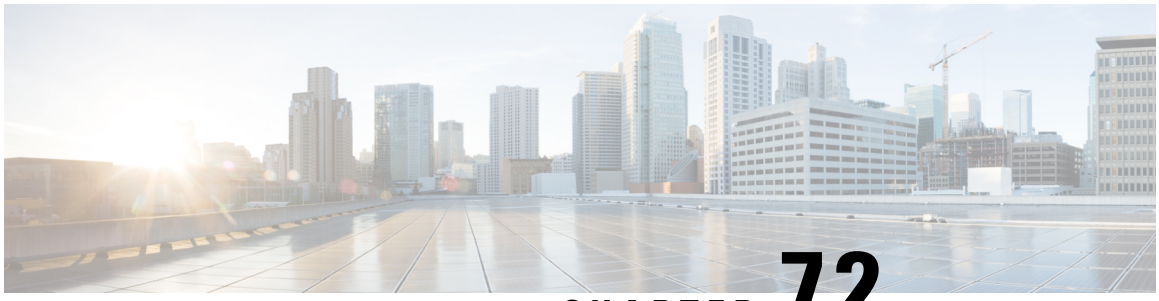
Exits the current configuration mode and returns to the Global Configuration mode.

**Product** UPF

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Global Configuration mode.



CHAPTER 72

# UPF Overload Control Profile Configuration Mode Commands

Overload control profile configuration commands enable the UPF to send its overload information to a peer node to adaptively balance the session load across UPFs. The overload information reflects the operating status of the resources of the UPF.

**Command Modes**

Exec > Global Configuration >UPF Overload Control Profile Configuration

**configure > upf-overload-control-profile** *profile_name*

Entering the above command results in the following prompt:

```
[local]UPF (config-ovrloadcontrolprof)#
```

**Important** Available commands or keywords/variables vary based on platform type, product version, and installed license(s).


- overload-threshold, on page 845
- inclusion-frequency, on page 847
- validity-period, on page 848
- end, on page 848


# overload-threshold

Configure lower and upper limits of the overload threshold parameters (System level and VPP CPU) under the UPF Overload Control Profile.

**Product**

UPF

**Privilege**

Administrator, Security Administrator

**Command Modes**

Exec > Global Configuration > UPF Overload Control Profile Configuration

**configure > upf-overload-control-profile** *profile_name*

Entering the above command results in the following prompt:

```
[local]UPlane (config-upf-overload-control-profile)#
```

## Syntax Description

**overload-threshold { system { cpu | memory | session-count } lower-limit** *lower_limit* **upper-limit** *upper_limit* **} | vpp-cpu lower-limit** *lower_limit* **upper-limit** *upper_limit*

### overload-threshold

Configure lower and upper limits of the overload threshold parameters (System level and VPP CPU) under the Overload Control Profile.

### system { cpu | memory | session-count }

Configures the overload system thresholds for CPU, Memory, and Session Count.

### vpp-cpu

Configures overload system thresholds for VPP CPU.

### lower-limit *lower_limit*

Configures the lower limit threshold for system and VPP CPU loads.

### upper-limit *upper_limit*

Configures the upper limit threshold for system and VPP CPU loads. Following are the defined thresholds for lower and upper limits:

| Overload Control Parameters | Lower Limit (Overload Control State) | Upper Limit (Self-Protection State) |
|---|---|---|
| System CPU | 80 | 90 |
| System Memory | 70 | 80 |
| System Session Count | 80 | 90 |
| VPP CPU | 50 | 80 |

**Note** The VPP CPU usage typically remains high, ranging between 90% and 100%. To standardize this metric, the reported value from Resource Manager is scaled to a percentage range of 1%– 100%. For instance, a reported VPP CPU usage of 97% is interpreted as 70%. Thus, the configurable threshold for VPP CPU is defined within the 1% to 100% range.

## Usage Guidelines

Use this command to configure the threshold values for System and VPP CPU loads under overload system thresholds.

### Example

```
[local]UPlane(config-upf-overload-control-profile)# overload-threshold system cpu lower
limit 80
```

```
upper-limit 90
[local]UPlane(config-upf-overload-control-profile)# overload-threshold system memory lower
 limit 70
upper-limit 80
[local]UPlane(config-upf-overload-control-profile)# overload-threshold system session-count
 lower
limit 80 upper-limit 90
[local]UPlane(config-upf-overload-control-profile)# overload-threshold vpp-cpu lower limit
 95
upper-limit 98
```

# inclusion-frequency

Configures parameters to determine the inclusion frequency of the Load Control Information IE for a UPF Overload Control Profile configuration.

**Product**

UPF

**Privilege**

Administrator, Security Administrator

**Command Modes**

Exec > Global Configuration > UPF Overload Control Profile Configuration

**configure > upf-overload-control-profile** *profile_name*

Entering this command results in the following prompt:

```
[local]UPlane (config-upf-overload-control-profile)#
```

**Syntax Description**

**inclusion-frequency { advertisement-interval** *interval_in_seconds* **| change-factor** *change_factor* **}**

**inclusion-frequency**

Specifies that parameters to determine the inclusion frequency of the Overload Control Information IE for a UPF Overload Control Profile is configured. This parameter specifies the frequency at which the operator wants to send this information to the peers.

**advertisement-interval *interval_in_seconds***

Configures the advertisement-interval for Overload Control in seconds. It must be an integer 0–3600.

The default value is 300.

**change-factor *change_factor***

Configures the change factor for the Overload Control profile configuration. This information is only sent to the peers when the load factor changes by the factor configured.

The value must be an integer 1–20.

The default value is 5%.

**Usage Guidelines**

Use this command to specify parameters to determine the inclusion frequency of the Load control information IE for a UPF Overload Control Profile configuration.

### Example

```
[local]UPlane(config-upf-overload-control-profile)# inclusion-frequency advertisement-interval
 300
[local]UPlane(config-upf-overload-control-profile)# inclusion-frequency change-factor 5
[local]UPlane(config-upf-overload-control-profile)# validity-period 300
```

# validity-period

Configures the time, in seconds, that specifies how long the overload control information is valid.

**Product** UPF

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > UPF Overload Control Profile Configuration

**configure > upf-overload-control-profile** *profile_name*

Entering this command sequence results in the following prompt:

```
[local]UPlane (config-upf-overload-control-profile)#
```

**Syntax Description**

**validity-period** *seconds*
**default validity-period**

#### validity-period *seconds*

Specifies the length of time during which the overload condition specified by the OCI IE is to be considered as valid, unless overridden by subsequent new overload control information.

The default value is 300.

### Example

```
validity-period 700
```

# end

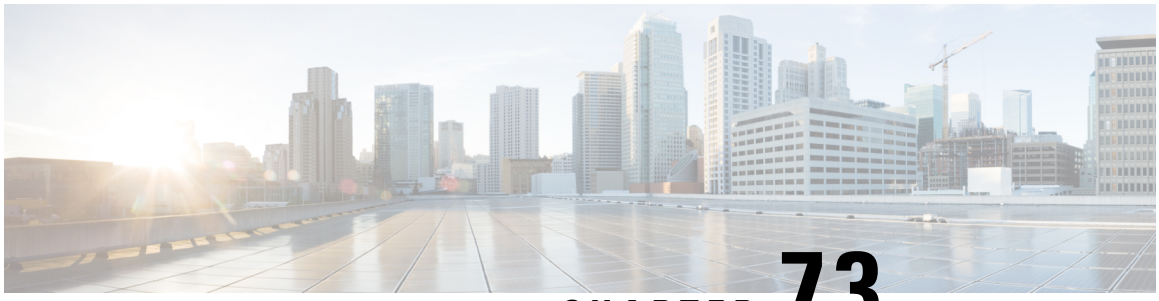
Exits the current configuration mode and returns to the Global Configuration mode.

**Product** UPF

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Global Configuration mode.



CHAPTER 73

# User Plane Group Configuration Mode Commands

**Command Modes**

The User Plane Group Configuration Mode is used for the configuration of Sx peer node IP address. This mode is entered from the Context Configuration Mode.

Exec > Global Configuration > Context Configuration > User Plane Group Configuration

**configure > context** *context_name* **> user-plane-group** *up_group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-user-plane-group)#
```

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

**Important** For information on common commands available in this configuration mode, refer to the *Common Commands* chapter.


- peer-node-id, on page 849


# peer-node-id

Configure the Sx peer node IP address.

**Product**

CUPS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > User Plane Group Configuration

**configure > context** *context_name* **> user-plane-group** *up_group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-user-plane-group)#
```

## Syntax Description

**[ no ] peer-node-id { ipv4-address** *IPv4_address* **| ipv6-address** *IPv6_address* **}**
**monitor-group-name** *monitor-group-name*

**ipv4-address *IPv4_address***

Specify the IPv4 address of the Sx interface on an active UP that is part of the UP group.

You can configure multiple peer-nodes within the group. Note that the Sx interface is a different interface from the one that is used to monitor the BFD.

**ipv6-address *IPv6_address***

Specify the IPv6 address of the Sx interface on an active UP that is part of the UP group.

You can configure multiple peer-nodes within the group. Note that the Sx interface is a different interface from the one that is used to monitor the BFD.

**monitor-group-name *monitor-group-name***

Specify the name of a pre-configured protocol monitoring group the UP is associated with. *monitor-group-name* is an alphanumeric string of 1 through 63 characters.

**Note** The monitor group name must be unique for each peer node IP.

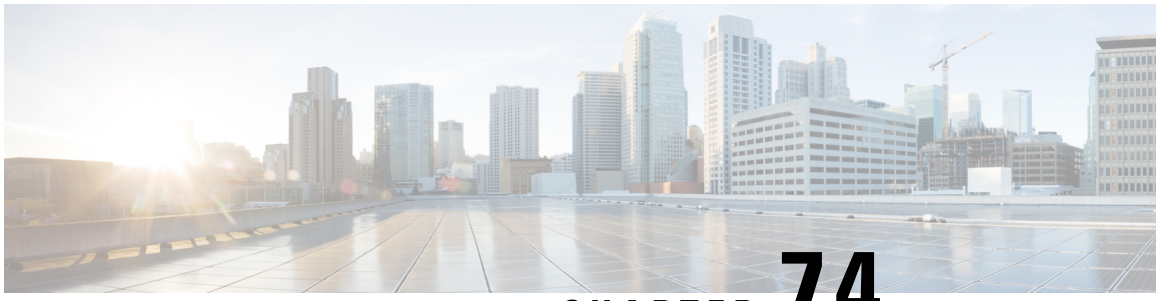
## Usage Guidelines

Use this command to configure the peer node IPs and the monitor group name. That is, this command allows the user to update the specified peer with the configured monitor group name value.

Once a peer has been configured with this parameter, the configurations cannot be modified. You must first delete the peer and then re-configure it.

If you attempt to update the existing configuration with the monitor group name value, it throws an error.

**Note** The value of the monitor group name must be unique to each peer.



CHAPTER 74

# User Plane Profile Configuration Mode

The User Plane Profile Configuration Mode allows you to configure User-Plane profile attributes.

**Important** This command is available in this release only for testing purposes. For more information, contact your Cisco Account representative.

**Command Modes**

Exec > Global Configuration > User-Plane Profile Configuration

**configure > user-plane-profile** *profile_id*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-user-plane-profile)#`

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


- do show, on page 851
- end, on page 852
- endpoint, on page 852
- exit, on page 853


# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character | is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

**`end`**

**Usage Guidelines** Use this command to return to the Exec mode.

# endpoint



**Important** This command is available in this release only for testing purposes. For more information, contact your Cisco Account representative.

Use this command to configure User Plane endpoint IP address attribute.

**Product** SAEGW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > User-Plane Profile Configuration

**configure** > **user-plane-profile** *profile_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-user-plane-profile)#
```

**Syntax Description**

**`endpoint { `** *`ipv4_address`* **` | `** *`ipv6_address`* **` }`**
**`no endpoint`**

**no**

If previously configured, removes the configured endpoint address.

**endpoint { *ipv4_address* | *ipv6_address* }**

Configures User Plane endpoint IPv4 or IPv6 address.

**Usage Guidelines**

Any change in **endpoint {** *ipv4_address* | *ipv6_address* **}** CLI configuration will not impact any existing PDN session. New configuration is applicable only for new incoming PDN sessions.

**Example**

The following command configures User Plane endpoint with IP address *1.1.1.1*:

```
endpoint 1.1.1.1
```

# exit

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

**Product**

All

**Privilege**

Security Administrator, Administrator

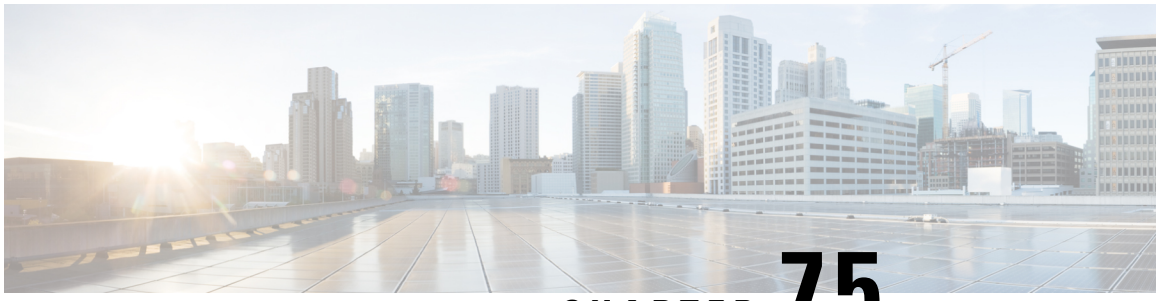
**Syntax Description**

```
exit
```

**Usage Guidelines**

Use this command to return to the parent configuration mode.

exit



CHAPTER 75

# User Plane Service Configuration Mode Commands

The User Plane Service Configuration Mode is used to create and manage the User Plane services on this system. The User Plane service acts as SGW-U service or PGW-U service based on Sx session established from Control plane. A single User-Plane-Service can serve SGW-U type sessions and/or PGW-U type sessions. You can also define two or more separate User-Plane-Services for each node type SGW-U and PGW-U respectively.

User Plane Service is associated with Sx Service for Control Plane interface and GTPU-Service for receiving GTPU packets. For this release, each User-Plane-Service is associated with only single Sx Service to interface with Control plane.

**Command Modes**

Exec > Global Configuration > Context Configuration >User Plane Service Configuration

**configure > context** *context_name* **> user-plane-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name( config-user-plane-service )#
```

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


- associate, on page 855
- associate ise-server-profile name, on page 857
- end, on page 857
- exit, on page 858


# associate

Associates or disassociates a user-plane service with GTPU. By default, this CLI command is disabled.

**Product**

CUPS

**Privilege**

Administrator

## Command Modes

Exec > Global Configuration > Context Configuration > User Plane Service Configuration

**configure > context** *context_name* **> user-plane-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-user-plane-service)#
```

## Syntax Description

```
[ no ] associate gtpu-service service_name  { pgw-ingress | sgw-ingress |
sgw-egress | sx-service | cp-tunnel | upf-ingress | interface-type [ n9
|s5u | s8u | n3 ] }
associate { upf-load-control-profile profile_name |
upf-overload-control-profile profile_name }
```

### upf-load-control-profile *profile_name*

Specify the UPF load control profile name to associate.

### upf-overload-control-profile *profile_name*

Specify the UPF overload control profile name to associate.

### gtpu-service *service_name*

Associate GTPU service with user-plane service.

*service_name* specifies the name for a pre-configured GTPU service to be associated with the user-plane service.

### pgw-ingress

Configure the interface type as PGW ingress.

### sgw-ingress

Configure the interface type as SGW ingress.

### sgw-egress

Configure the interface type as SGW egress.

### sx-service

Configure the interface type as Sx service.

### cp-tunnel

Configure the interface type as cp-tunnel (tunnel towards Control Plane function).

### upf-ingress

Configure the interface type as UPF ingress.

### interface-type [ n9 |s5u | s8u | n3 ]

Configure the desired GTP-U ingress interface type.

**Usage Guidelines** Use this command to associate a pre-configured GTPU service the user-plane service.

### Example

The following command associates a pre-configured GTPU service called *gtp1*, with **pgw-ingress** interface to the user-plane service:

```
associate gtpu-service gtp1 pgw-ingress
```

# associate ise-server-profile name

Associates the required ISE profile within the UPF service.

**Product** UPF

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > User Plane Service Configuration

**configure > context** *context_name* **> user-plane-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-user-plane-service)#
```

**Syntax Description** **associate ise-server-profile name** *profile_name*

**associate ise-server-profile name *profile_name***

Associates an ISE profile within the UPF service.

**Usage Guidelines** Use this command to associate an ISE profile within the user-plane service.

### Example

The following command associates the ISE server profile *ise_1* with the user- plane service.

```
associate ise-server-profile name ise_1
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

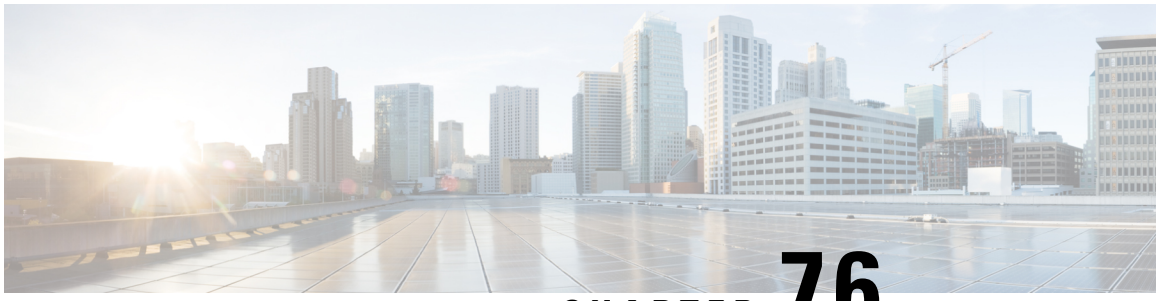
Exits the current mode and returns to the parent configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `exit`

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



CHAPTER 76

# UUT Profile Configuration Mode Commands

The UE Usage Type (UUT) Profile Configuration Mode is used to configure UUT profiles on a per-context basis. UUT profile name is used in APN configuration to associate virtual APN

**Command Modes**

Exec > Global Configuration > Context Configuration > UUT Profile Configuration

**configure > context** *context_name* **> uut-profile name** *profile_name*

`[context_name]host_name(config-uut-profile)#`

**Important** Available commands or keywords/variables vary based on platform type, product version, and installed license(s).


- do show, on page 859
- end, on page 860
- exit, on page 860
- uut, on page 860


# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**do show**

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# uut

Configures UE Usage Type (UUT) profile with discrete values and range.

**Product** CUPS

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > UUT Profile Configuration

**configure > context** *context_name* **> uut-profile name** *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-uut-profile)#
```

## Syntax Description

**[ no ] uut { range** *start_range* **to** *end_range* **|** *value* **}**

**no**

Including **no** with the command disables the specified configuration.

**range *start_range* to *end_range***

Specifies the UUT start and end range of discrete integer value ranging from 1 to 65535.

***value***

The number of discrete UUT values supported per CLI command is 16.

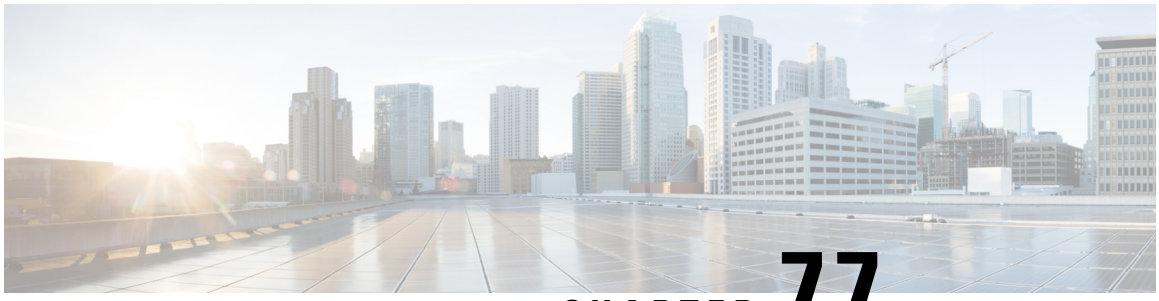
## Usage Guidelines

Use this command to configure UUT profiles per context.

### Example

The following command configures UUT range of 10 to 20:

```
uut range 10 to 20
```



CHAPTER 77

# Video Group Configuration Mode

The Video Group Configuration Mode is used to add CAEs to a CAE group and configure the CAEs for load balancing and health-check monitoring. The CAE (Content Adaptation Engine) is an optional component of the Mobile Videoscape. For additional information, refer to the *Mobile Video Gateway Administration Guide*.

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

**Command Modes** Exec > Global Configuration > Context Configuration > Video Group Configuration

**configure > context** *context_name* **> cae-group** *group_name*

Entering the above command sequence results in the following prompt:

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

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


- do show, on page 863
- end, on page 864
- exit, on page 864
- keepalive-server, on page 864
- local-address, on page 866
- server, on page 867


# do show

Executes all **show** commands while in Configuration mode.

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `do show`

**Usage Guidelines** Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `end`

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `exit`

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

# keepalive-server

Specifies keep-alive messaging information for Content Adaptation Engine (CAE) health-check monitoring, which is part of CAE load balancing on the Mobile Video Gateway. Note that this command and its options configure settings that apply to all CAEs in the CAE group, not to an individual CAE.

**Product** MVG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Video Group Configuration

**configure > context** *context_name* **> cae-group** *group_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ default ] keepalive-server deadtime** *seconds* **interval** *seconds* **num-retry** *num-retries* **port** *port_number* **timeout** *seconds* **[ -noconfirm ]**

**default keepalive-server**

Sets the CAE keep-alive settings to their default values.

**keepalive-server deadtime *seconds* interval *seconds* num-retry *num-retries* port *port_number* timeout *seconds* [ -noconfirm ]**

Specifies keep-alive messaging information for CAE health-check monitoring.

**deadtime *seconds***

Specifies the periodic retry interval (in seconds) after a CAE is detected down. *seconds* is an integer from 1 through 1800. The default value is 120 seconds.

**interval *seconds***

Specifies the interval (in seconds) for how often the Mobile Video Gateway sends a keep-alive message to the CAEs. *seconds* is an integer from 0 through 120. The default value is 10 seconds. A value of 0 turns off keep-alive detection and marks the state of all CAEs to Up.

**num-retry *num_retries***

Specifies the number of keepalive retries after a CAE does not respond. *num_retries* is an integer from 1 through 20. The default value is 3 retries.

**port *port_number***

Specifies the TCP port number for health-check monitoring, which is an integer from 1 through 65535. The default value is 5100.

**timeout *seconds***

Specifies the keep-alive timeout (in seconds) which is an integer from 1 through 30. The default value is 3 seconds.

**-noconfirm**

Specifies that the command must execute without prompting for confirmation.

**Usage Guidelines**

Use this command to specify keep-alive messaging information for CAE health-check monitoring, which is part of CAE load balancing on the Mobile Video Gateway.

### Example

The following command specifies keep-alive messaging information for the CAEs in the CAE group:

```
keepalive-server deadtime 120 interval 10 num-retry 3 port 5100 timeout
3
```

# local-address

Specifies the local IPv4 address on the Mobile Video Gateway for the keepalive TCP connection used for Content Adaptation Engine (CAE) load balancing.

**Product**

MVG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Video Group Configuration

**configure** > **context** *context_name* > **cae-group** *group_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**[ no ] local-address** *IPv4_address* **[ -noconfirm ]**

#### no local-address *IPv4_address*

Deletes the local IPv4 address if previously specified.

#### local-address *IPv4_address*

Specifies the local IPv4 address on the Mobile Video Gateway for the keep-live TCP connection used for CAE load balancing. *IPv4_address* must be in dotted decimal notation.

#### -noconfirm

Specifies that the command must execute without prompting for confirmation.

**Usage Guidelines**

Use this command to specify the local IPv4 address on the Mobile Video Gateway, in dotted-decimal notation.

### Example

The following command specifies the local IPv4 address on the Mobile Video Gateway:

```
local-address 209.165.200.228
```

# server

Adds a CAE (Content Adaptation Engine) and its IPv4 address and port number to the associated CAE group. The Mobile Video Gateway uses this information for CAE load balancing. The Mobile Video Gateway has a system limit of 64 CAEs.

**Product**

MVG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Video Group Configuration

**configure > context** *context_name* **> cae-group** *group_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**`[ no ] server` *`cae_name`* `address` *`IPv4_address`* `port` *`port_number`* `[ -noconfirm ]`**

**no server *cae_name***

Deletes the CAE from the CAE group if previously configured.

**server *cae_name* address *IPv4_address* port *port_number***

Adds a CAE and its IPv4 address and port number to the associated CAE group. *cae_name* is an alphanumeric string of 1 through 15 characters. *IPv4_address* must be in dotted-decimal notation. *port_number* is an integer from 1 through 65535. The default value is 80.

**-noconfirm**

Specifies that the command must execute without prompting for confirmation.

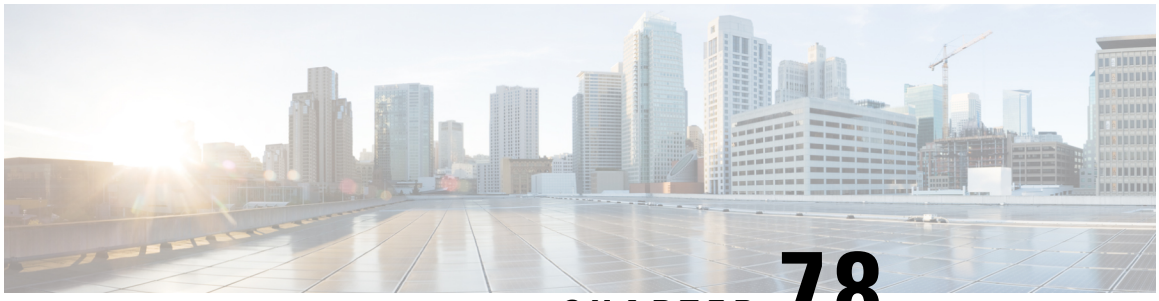
**Usage Guidelines**

Use this command to add a CAE and its IPv4 address and port number to the associated CAE group.

**Example**

The following command adds a CAE named *cae_1* and its IPv4 address and port number to the associated CAE group:

```
server cae_1 address 209.165.200.228 port 80
```



CHAPTER 78

# VLAN Configuration Mode Commands

The VLAN Configuration Mode is used to create and manage Virtual LANs and their bindings with contexts.

**Command Modes**

Exec > Global Configuration > Port Configuration > VLAN Configuration

**configure > port ethernet** *slot_number/port_number* **> vlan** *vlan_tag_id*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-port-slot_number/port_number-vlan-vlan-id)#`

**Important** Availabe commands or keywords/variables vary based on platform type, product version, and installed license(s).


- bind interface, on page 869
- do show, on page 870
- end, on page 871
- exit, on page 871
- ingress-mode, on page 871
- priority, on page 872
- shutdown, on page 873
- vlan-map , on page 874


# bind interface

Associates a VLAN interface with a context.

**Product**

HA

HSGW

PDSN

P-GW

SAEGW

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Port Configuration > VLAN Configuration

**configure > port ethernet** *slot_number/port_number* **> vlan** *vlan_tag_id*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-port-`*`slot_number/port_number`*`-vlan-vlan-`*`id`*`)#`

**Syntax Description**

**`[ no ] bind interface`** *`interface_name context_name`*

**no**

Disasscoiates the VLAN interface from the context.

***interface_name context_name***

Specifies the name of the virtual interface and the context to which it will be bound.

*interface_name* must be an alphanumeric string of 1 through 79 characters.

*context_name* must refer to a previously configured context expressed as an alphanumeric string of 1 through 79 characters.

**Usage Guidelines**

Bind a VLAN interface to a context to suport VLAN service.

**Example**

```
bind interface sampleVirtual sampleContext
no bind interface sampleVirtual sampleContext
```

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**`do show`**

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# ingress-mode

Enables or disables port ingress (incoming) mode for this VLAN ID on this port.

**Product** HA

HSGW

PDSN

P-GW

SAEGW

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Port Configuration > VLAN Configuration

**configure > port ethernet** *slot_number/port_number* **> vlan** *vlan_tag_id*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-port-`*`slot_number/port_number`*`-vlan-vlan-`*`id`*`)#`

**Syntax Description**

**`[ no ] ingress-mode`**

**no**

Disables the port ingress mode.

**Usage Guidelines**

Use this command to enable or disable the VLAN ingress mode for this port.

**Example**

**`ingress-mode`**

# priority

Sets the 802.1p VLAN priority bit.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Port Configuration > VLAN Configuration

**configure > port ethernet** *slot_number/port_number* **> vlan** *vlan_tag_id*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-port-`*`slot_number/port_number`*`-vlan-vlan-`*`id`*`)#`

**Syntax Description**

**`priority`** *`value`*
**`no priority`**

**no**

Disables the setting of the 802.1p priority bit.

***value***

Sets the value of the 802.1p priority bit as an integer from 0 through 7, with 7 being the highest priority.

**Usage Guidelines**

Set a value for the VLAN priority bit.

### Example

To set a VLAN priority bit value, use the following command:

```
priority 3
```

To disable the use of a VLAN priority bit, use the following command:

```
no priority
```

# shutdown

Disables or enables traffic over this VLAN.

**Product**

HA

HSGW

PDSN

P-GW

SAEGW

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Port Configuration > VLAN Configuration

**configure > port ethernet** *slot_number/port_number* **> vlan** *vlan_tag_id*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-port-`*`slot_number/port_number`*`-vlan-vlan-`*`id`*`)#`

**Syntax Description**

**`[ no ] shutdown`**

**no**

Enables the VLAN. When omitted the VLAN is shutdown.

**Usage Guidelines**

Shut down a VLAN.

To bring a VLAN into service, execute this command using the **no** keyword.

### Example

To disable a VLAN from sending or receiving network traffic use the following command:

```
shutdown
```

To enable a VLAN use the following command:

```
no shutdown
```

# vlan-map

Associates an IP interface having a VLAN ID with a context.

**Product**

HA

HSGW

PDSN

P-GW

SAEGW

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Port Configuration > VLAN Configuration

**configure > port ethernet** *slot_number/port_number* **> vlan** *vlan_tag_id*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-port-`*`slot_number/port_number`*`-vlan-vlan-`*`id`*`)#`

**Syntax Description**

**`vlan-map interface`** *`if_name context_name`*

**interface *if_name context_name***

Associates the specified VLAN interface with a context.

*if_name* is an exisitng interface name specified as an alphanumeric string of 1 through 79 characters.

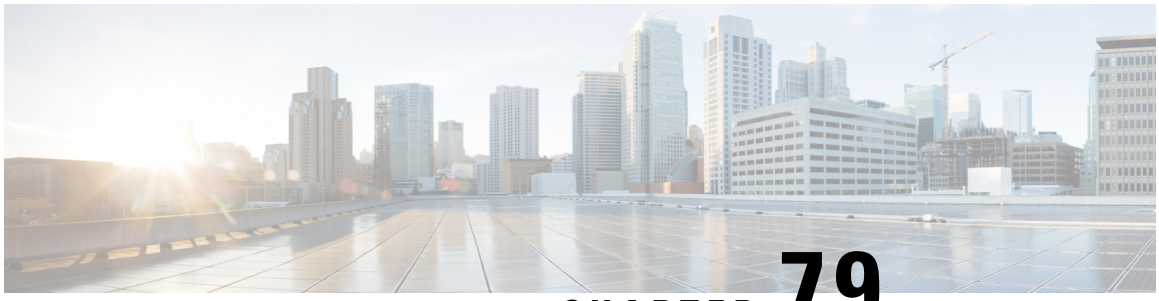
*context_name* is an exisitng context name specified as an alphanumeric string of 1 through 79 characters.

**Usage Guidelines**

Use **vlan-map** to associate multiple VLAN interfaces with a single context. This feature is used in conjunction with nexthop forwarding and overlapping IP pools.

**Example**

```
vlan-map interface vlan234 ingress
```



CHAPTER 79

# WSG Lookup Priority List Configuration Mode Commands

**Command Modes**

The Wireless Security Gateway Lookup Priority List Configuration Mode is used to set the priority of subnet components for site-to-site tunnels. This is a Security Gateway (SecGW) feature [VPC-VSM only].

Exec > Global Configuration > WSG-Lookup Priority List Configuration

**configure > wsg-lookup**

Entering the above command sequence results in the following prompt:

```
host_name(config-wsg-lookup)#
```

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


- do show, on page 875
- end, on page 876
- exit, on page 876
- priority, on page 876


# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# priority

Sets the priority level for a WSG subnet combination (source and destination netmasks). It also disables an existing priority for a specified subnet combination. (VPC-VSM only).

**Product** SecGW

**Privilege** Security Administrator

**Command Modes** Exec > Global Configuration > WSG-Lookup Priority List Configuration

**configure > wsg-lookup**

Entering the above command sequence results in the following prompt:

## Syntax Description

**[ no ] priority** *priority_level* **source-netmask** *subnet_size* **destination netmask** *subnet_size*

### no

Disables the priority for the specified subnet combination.

### priority *priority_level*

Specifies the priority level for the subnet combination as an integer from 1 through 6.

### source-netmask *subnet_size*

Specifies the subnet size for the source netmask as an integer from 1 through 128.

### destination netmask *subnet_size*

Specifies the subnet size for the destination netmask as an integer from 1 through 128.

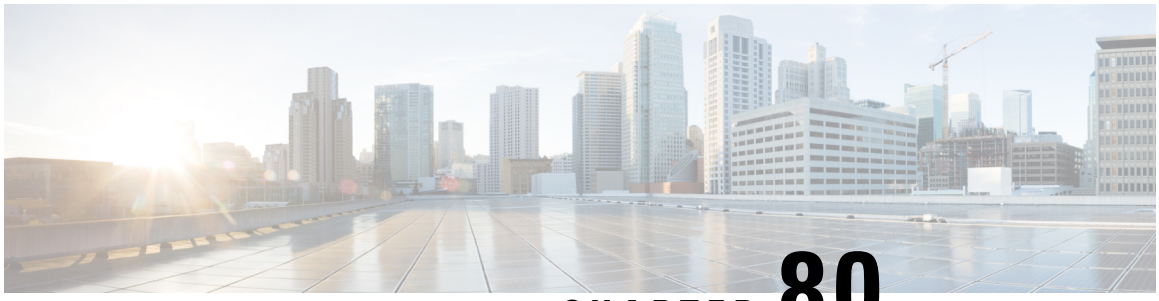
## Usage Guidelines

Use this command to set the priority level for a WSG subnet combination (source and destination netmasks). It can also be used to disable an existing priority for a specified subnet combination.

### Example

The following command sets a priority of 2 for a subnet combination with a /32 subnet size.

```
priority 2 source-netmask 32 destination netmask 32
```



CHAPTER 80

# WSG Service Configuration Mode Commands

## Command Modes

The Wireless Security Gateway Configuration Mode is used to define the operating parameters for IPSec-based access control and handling of Encapsulating Security Payload (ESP) packets.

Exec > Global Configuration > Context Configuration > WSG-Service Configuration

**configure > context** *context_name* **> wsg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-wsg-service)#
```

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

**Important** Any changes made to a WSG service require that the service be restarted to apply any changed parameters. You restart the service by unbinding and binding the IP address to the service context.


- associate subscriber-map, on page 880
- bind address, on page 880
- deployment-mode, on page 881
- dhcp, on page 882
- dns-server, on page 883
- do show, on page 884
- duplicate-session-detection, on page 884
- end, on page 885
- exit, on page 885
- initiator-mode-duration, on page 885
- ip, on page 886
- ipv6, on page 887
- peer-list, on page 888
- pre_fragment mtu, on page 889
- responder-mode-duration, on page 890
- Server dhcp, on page 891

# associate subscriber-map

Binds the WSG service to the specified IPv4 or IPv6 address and crypto template (VPC only).

**Product**

SecGW (WSG)

**Privilege**

Security Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > WSG-Service Configuration

**configure > context** *context_name* **> wsg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-wsg-service)#
```

**Syntax Description**

**associate subscriber-map** *subscriber_map_name*

***subscriber_map_name***

Specifies the name of an subscriber map as an alphanumeric string of 0 through 127 characters.

**Usage Guidelines**

Associates the WSG service to Subscriber Map.

**Example**

The following command associates SecGW to subscriber map1.

**associate subscriber-map** *subscriber_map1*

# bind address

Binds the WSG service to the specified IPv4 or IPv6 address and crypto template (VPC only).

**Product**

SecGW (WSG)

**Privilege**

Security Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > WSG-Service Configuration

**configure > context** *context_name* **> wsg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-wsg-service)#
```

**Syntax Description**

**bind address** *IPv4 / IPv6* **crypto-template** *template_name* | **Secure-tunnel** [ **Max-sessions** *sessions* ]
**no bind address**

**no**

Unbinds the WSG service from the IP address.

***IPv4 / IPv6***

IPV4 ##.##.##.## or IPV6 ####:####:####:####:####:####:####:#### (IPV6 also supports :: notation).

***template_name***

Specifies the name of an existing crypto template as an alphanumeric string of 0 through 127 characters.

**Usage Guidelines**

Bind the WSG service to an IPv4 or IPv6 address.

**Example**

The following command binds the WSG service to 10.1.1.1.

```
bind address 10.1.1.1 crypto template tplt01
```

# deployment-mode

Specifies the deployment mode for the WSG service (VPC only).

**Product**

SecGW (WSG)

**Privilege**

Security Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > WSG-Service Configuration

**configure > context** *context_name* **> wsg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-wsg-service)#
```

**Syntax Description**

```
deployment-mode { remote-access | site-to-site }
no deployment-mode
```

**no**

Deletes deployment mode from the configuration.

**{ remote-access | site-to-site }**

Specifies the deployment mode as either:

- **remote-access** – support direct user communication with this WSG
- **site-to-site** – support bidirectional communication with two or more WSGs

**Usage Guidelines**

Specify remote access or site-to-site communication as the deployment mode for this WSG.

### Example

This command deploys this WSG for remote access:

```
deployment-mode remote-access
```

# dhcp

Specifies the DHCPv4 context and service name to be used when the IP address allocation method is set **dhcp-proxy** (VPC only).

**Product**

SecGW (WSG)

**Privilege**

Security Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > WSG-Service Configuration

**configure** > **context** *context_name* > **wsg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-wsg-service)#
```

**Syntax Description**

```
dhcp { context-name context_name | service-name service_name }
no dhcp { context-name | service-name }
```

#### no

Deletes the specified parameter.

#### context-name *context_name*

Specifies the context in which the DHCPv4 service is configured as an alphanumeric string of 1 through 79 characters.

#### service-name *service_name*

Specifies which DHCPv4 service to use for the **dhcp-proxy** as an alphanumeric string of one through 63 characters. Only one DHCPv4 service can be configured as the **dhcp-proxy**.

**Usage Guidelines**

Specifies the DHCPv4 context and service name to be used when the IP address allocation method is set to **dhcp-proxy**. The specified DHCPv4 service is designated via the **ip address alloc-method dhcp-proxy** command.

The WSG service must be restarted to apply the parameters. You restart the service by doing an unbind and bind.

### Example

The following command sequence enables a DHCPv4 service as an allocation method for IP addresses:

```
dhcp context-name wsg01
dhcp service-name dhcp1
```

# dns-server

Enables the WSG service (SecGW) to send the IP Address of the DNS server to the peer. A new request will overwrite the existing entries.

**Product**

SecGW (WSG service)

**Privilege**

Security Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > WSG-Service Configuration

**configure > context** *context_name* **> wsg-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-wsg-service)#`

**Syntax Description**

```
dns-server primary ip_address [ secondary ip_address ]
no dns-server primary ip_address
```

**no**

Disables sending the primary IP address of the DNS server.

**primary *ip_address***

Specifies the IP Address, in IPv4 dotted-decimal or IPv6 colon-separated hexadecimal notation, of the primary DNS server to be sent to the peer.

**secondary *ip_address***

Specifies the IP Address, in IPv4 dotted-decimal or IPv6 colon-separated hexadecimal notation, of the secondary DNS server to be sent to the peer.

**Usage Guidelines**

Use this command to configure an IPv4 or IPv6 address of a DNS server. The same CLI can be configured twice with different IP address type. However, both primary and secondary IP address should be of the same type (IPv4 or IPv6) for a CLI.

A new request will overwrite the existing entries of the same IP address type.

**Example**

The following command enables the WSG service to send the IPv4 address of the primary DNS server to the peer:

```
dns-server primary 10.1.1.1 secondary 10.1.1.2
```

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
do show
```

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution**

There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# duplicate-session-detection

Enables or disables allowing only one IKE-SA per remote IKE-ID. A new request will overwrite the existing tunnel.

**Product**

SecGW (WSG service)

**Privilege**

Security Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > WSG-Service Configuration

**configure > context** *context_name* **> wsg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-wsg-service)#
```

**Syntax Description**

```
duplicate-session-detection
no duplicate-session-detection
```

**no**

Disables duplicate session detection and allows multiple IKE-SAs per remote IKE-ID. This is the default behavior.

**Usage Guidelines**

Enables or disables allowing only one IKE-SA per remote IKE-ID. A new request will overwrite the existing tunnel. For a complete description of this feature, refer to the *IPSec Reference*.

**Example**

The following command enables duplicate session detection:

**duplicate-session-detection**

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **end**

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

# initiator-mode-duration

Specifies the interval during which the WSG service (SecGW) will try to initiate a call with an IKE peer. A peer list must be configured in this WSG service for this command to be available (VPC only).

**Product** SecGW (WSG)

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > WSG-Service Configuration

**configure > context** *context_name* **> wsg-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-wsg-service)#`

**Syntax Description**

**initiator-mode-duration** *seconds*
**default initiator-mode-duration**

**default**

Sets the initiator mode duration to 10 seconds.

***seconds***

Specifies the duration interval in seconds as an integer from 5 through 250.

**Usage Guidelines**

Use this command to specify the interval during which the WSG service (SecGW) will try to initiate an IKE call when a peer list is activated (default is 10 seconds).

This command is only available when a peer-list has been configured for the WSG service.

See the *IPSec Reference* for additional information on configuring an SecGW as an IKE initiator.

**Example**

The following command sets the initiator mode duration to 15 seconds:

**initiator-mode-duration 15**

# ip

Specifies the IPv4 access group and address allocation method for this WSG service (VPC only).

**Product**

SecGW (WSG)

**Privilege**

Security Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > WSG-Service Configuration

**configure** > **context** *context_name* > **wsg-service** *service_name*

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(config-wsg-service)#

**Syntax Description**

**ip { access-group** *group_name* **| address { alloc-method { dhcp-proxy | local } | pool name** *pool_name* **}**
**no ip access-group** *group_name*
**no ip address alloc-method** *pool_name*
**no ip address pool name** *pool_name*

**no**

Deletes the specified parameter.

**access-group *group_name***

Specifies an existing IPv4 ACL access group as an alphanumeric string of 1 through 47 characters. For additional information, see *ACL Configuration Mode Commands*.

**address alloc-method { dhcp-proxy | local }**

Specifies the method to be used when allocating IPv4 addresses:

- **dhcp-proxy** – allocates via a DHCP server
- **local** – allocates from a local pool (default)

**pool name *pool_name***

Specifies an existing IPv4 access pool as an alphanumeric string of 1 through 31 characters. Up to 16 named IPv4 pools can be configured. For additional information, see *APN Configuration Mode Commands*.

**Usage Guidelines**

Use this command to specify the IPv4 access group and IPv4 address allocation method for this WSG service.

This command and its keywords are subject to the following limitations:

- The WSG service configuration takes precedence over the equivalent configuration in Subscriber mode or the template payload.
- The WSG service must be restarted to apply the parameters. You restart the service by doing an unbind and bind.
- Up to 16 named IPv4 pools can be configured. The list is sorted, and the addresses are allocated from the first pool in the list with available addresses.
- One IPv4 ACL can be configured.
- The IPv4 pools will only be used for IPv4 calls.

**Example**

This command specifies the IPv4 address pool named *pool401*:

```
ip address pool name pool401
```

This command specifies the use of a previously configure DHCPv4 service to allocate IPv4 addresses:

```
ip address alloc-method dhcp-proxy
```

# ipv6

Specifies the IPv6 access group and prefix pool for this WSG service (VPC only).

**Product**

SecGW (WSG)

**Privilege**

Security Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > WSG-Service Configuration

**configure** > **context** *context_name* > **wsg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-wsg-service)#
```

**Syntax Description**

```
ipv6 { access-group group_name | address prefix-pool pool_name }
no ipv6 access-group group_name
no ipv6 address prefix-pool
```

**no**

Deletes the specified parameter.

**access-group *group_name***

Specifies an existing IPv6 ACL access group as an alphanumeric string of 1 through 47 characters. For additional information, see *IPv6 ACL Configuration Mode Commands*.

**address prefix-pool *pool_name***

Specifies an existing IPv6 prefix pool as an alphanumeric string of 1 through 31 characters. For additional information, see *Subscriber Configuration Mode Commands*.

**Usage Guidelines**

Specify the IPv6 access group and prefix pool for this WSG service.

This command and its keywords are subject to the following limitations:

- The WSG service configuration takes precedence over the equivalent configuration in Subscriber mode or the template payload.
- The WSG service must be restarted to apply the parameters. You restart the service by doing an unbind and bind.
- One named IPv6 pool can be configured.
- One named IPv6 ACL can be configured.
- The IPv6 pools will only be used for IPv6 calls.

**Example**

This command specifies the IPv6 prefix pool named pool601:

```
ipv6 prefix-pool name pool601
```

# peer-list

Configures an SecGW to initiate an IKEv2 session setup request when the peer does not initiate a setup request within a specified time interval. This command is only available for a WSG service configured for site-to-site (S2S) deployment mode (VPC only).

**Product**

SecGW (WSG)

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > WSG-Service Configuration

**configure > context** *context_name* **> wsg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-wsg-service)#
```

**Syntax Description**

**peer-list** *peer_list_name*
**no peer-list**

**no**

Disables the current peer list and SecGW as an IKE initiator functionality.

***peer_list_name***

Specifies the name of an existing peer list as an alphanumeric string of 1 through 79 characters. The crypto peer list must have been previously created using the Global Configuration mode **crypto peer-list** command.

**Usage Guidelines**

Enables the use of a peer list so that the SecGW can act as an initiator of an IKEv2 call session. The WSG service deployment mode must be configured as site-to-site for the **peer-list** command to execute.

The following limitations apply when the SecGW as initiator feature is enabled:

- The SecGW will only support up to 1,000 peers. This restriction is applied when configuring a crypto peer list.
- SecGW will not support the modification of an IPv4/IPv6 peer list on the fly (call sessions in progress). The modification will be allowed only after all the calls are removed.

When a peer list has been configured in the WSG service, the initiator and responder mode timer intervals each default to 10 seconds. The SecGW will wait for 10 seconds in the responder mode for a peer session initiation request before switching to the initiator mode and waiting 10 seconds for a peer response.

You can change the default settings for the initiator and/or responder mode intervals using the WSG Service mode **initiator-mode-duration** and **responder-mode-duration** commands.

See the *IPSec Reference* for additional information on configuring an SecGW as an IKE initiator.

**Example**

The following command enables the user of a peer list named *peer1*.

```
peer-list peer1
```

# pre_fragment mtu

Specifies the Maximum Transmission Unit (MTU) size which when exceeded initiates pre-tunnel (before encryption) fragmentation of IPSec Encapsulated Security Payload (ESP) packets within this WSG service (VPC only).

**Product**

SecGW (WSG)

**Privilege**

Security Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > WSG-Service Configuration

**configure > context** *context_name* **> wsg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-wsg-service)#
```

**Syntax Description**

```
pre_fragment mtu size
no pre_fragment size
default pre_fragment size
```

**no**

Disables this function.

**default**

Sets the MTU size to the default value of 1400 bytes.

**mtu *size***

Specifies the MTU size in bytes as an integer from 576 through 2048. Default = 1400

**Usage Guidelines**

Specify the MTU size which when exceeded initiates pre-tunnel fragmentation of IPSec ESP packets within this WSG service.

Pre-Tunnel-Fragmentation improves packet processing performance as compared to post-tunnel-fragmentation.

If a clear IPv4 packet is longer than the predefined MTU size, it will be fragmented before the packet is encrypted and transmitted to internet.

If a clear IPv6 packet is longer than the predefined MTU size, it is dropped and an ICMP packet with the maximum length is sent back to the source. The source will then fragment the IPv6 packet and retransmit.

**Example**

The following command sets MTU size to 2048 bytes.

```
pre_fragment mtu 2048
```

# responder-mode-duration

Specifies the interval during which the WSG service (SecGW) will wait for a response from an IKE peer before switching to initiator mode. A peer list must be configured in this WSG service for this command to be available (VPC only).

**Product**

SecGW (WSG)

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > WSG-Service Configuration

**configure > context** *context_name* **> wsg-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-wsg-service)#`

**Syntax Description**

**responder-mode-duration** *seconds*
**default responder-mode-duration**

**default**

Sets the responder mode duration to 10 seconds.

***seconds***

Specifies the duration interval in seconds as an integer from 5 through 250.

**Usage Guidelines**

Use this command to specify the interval during which the WSG service (SecGW) will wait or a response from an IKE peer before switching to initiator mode (default is 10 seconds).

This command is only available when a peer-list has been configured for the WSG service.

See the *IPSec Reference* for additional information on configuring an SecGW as an IKE initiator.

**Example**

The following command sets the responder mode duration to 15 seconds:

**responder-mode-duration 15**

# Server dhcp

Specifies the dhcp server addresses to be sent to the peer in authentication response.

**Product**

SecGW (WSG)

**Privilege**

Security Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > WSG-Service Configuration

**configure > context** *context_name* **> wsg-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-wsg-service)#`

**Syntax Description**

**server dhcp { ipv4** *ipv4_address* **[ IP-ADDRESS | IP-ADDRESS ] | ipv6** *ipv6_address* **[ IPv6-ADDRESS | IPv6-ADDRESS ] }**
**no server dhcp { ipv4 [ ipv6 ] | ipv6 [ ipv4 ] }**

**no**

Deletes the specified parameter.

***ipv4_address***

Specifies the ipv4 address of the dhcp-server to be sent to the peer. The IPV4 address should be in the format ##.##.##.## which is the first ipv4 dhcp-server's address.

***IP-ADDRESS***

Specifies ipv4 address of the dhcp-server to be sent to the peer.

***ipv6_address***

Specifies the ipv6 address of the dhcp-server to be sent to the peer. The IPV6 address should be in the format ####:####:####:####:####:####:####:#### (IPv6 also supports :: notation).

***IPv6-ADDRESS***

Specifies ipv6 address of the dhcp-server to be sent to the peer.

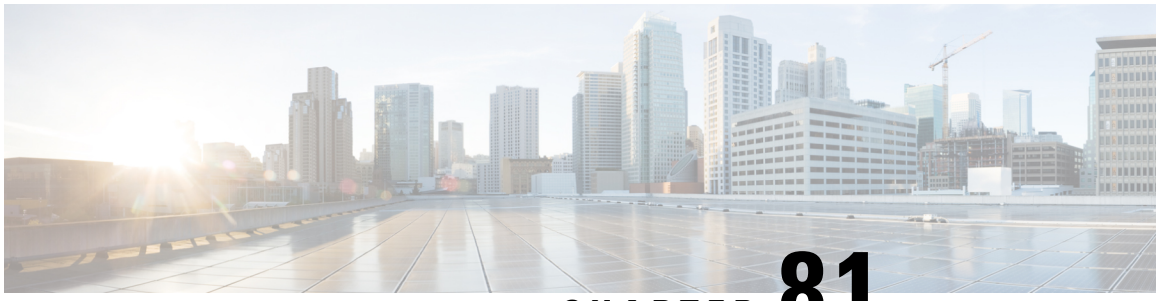
## Usage Guidelines

This command specifies the dhcp server addresses to be sent to the peer in authentication response

### Example

The following command specifies the dhcp server ipv4 addresses to be sent to the peer in authentication response:

```
server dhcp ipv4 209.165.200.242
```



CHAPTER 81

# X2-GW Service Configuration Mode Commands

**Important** In Release 20, 21.0 and 21.1, HeNBGW is not supported. Commands in this configuration mode must not be used in these releases. For more information, contact your Cisco account representative.

The X2 Gateway Service Configuration Mode is associated with HeNBGW-access-service.

**Command Modes** Exec > Global Configuration > Context Configuration > X2 GW Service Configuration

**configure > context** *context_name* **> x2gw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-x2gw-service)#
```

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


- bind, on page 893
- do show, on page 894
- end, on page 895
- exit, on page 895
- x2-c, on page 895


# bind

This command binds X2GW service to IP address of interface.

**Product** HeNB-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > Global Configuration > Context Configuration > X2 GW Service Configuration

**configure > context** *context_name* **> x2gw-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-x2gw-service)#
```

**Syntax Description**

**bind x2-c ipv4-address** *IPv4_address*
**no bind x2-c**

**no**

Removes the X2GW service to IP address of interface.

**x2-c**

Configure the X2-C parameters.

**ipv4-address *IPv4_address***

Configure the X2-C IPV4 address.

*IPv4_address* is an ip_address that must be entered in IPv4 dotted-decimal notation.

**Usage Guidelines**

Use this command to bind/associate X2GW service to IP address of interface

**Example**

Following command binds X2GW service to IP address of interface.

```
bind x2-c ipv4-address 209.165.200.230
```

# do show

Executes all **show** commands while in Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**do show**

**Usage Guidelines**

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.



**Caution** There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

# end

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
end
```

**Usage Guidelines** Use this command to return to the Exec mode.

# exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
exit
```

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

# x2-c

This command configures the X2-C parameters.

**Product** HeNB-GW

**Privilege** Security Administrator, Administrator

**Syntax Description**

```
x2-c sctp port value
default x2-c sctp port
```

**default**

Sets/Restores the default value assigned for X2-C parameters. The defalt value of SCTP port is 36422.

**sctp**

Configure the X2-C sctp parameters.

**port*value***

Designates SCTP port.

*value* is an integer ranging from 1 to 65535.

**Usage Guidelines** Use this to configure the X2-C parameters.

### Example

Following command configures the parameter X2-C sctp port to 345 .

```
x2-c sctp port 345
```