

Command Line Interface Reference, Modes C - D, StarOS Release 21.26

First Published: 2021-12-22

Last Modified: 2022-02-11

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)

© 2021-2022 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

Call Control Profile Configuration Mode 1

a-msisdn 5

access-restriction-data 6

accounting context 9

accounting mode 10

accounting stop-trigger 11

allocate-ptmsi-signature 12

apn-restriction 12

associate 13

attach access-type 16

attach allow 20

attach imei-query-type 21

attach implicit-ulr 23

attach restrict 23

authenticate 26

authenticate activate 31

authenticate all-events 32

authenticate attach 34

authenticate context 36

authenticate detach 37
authenticate on-first-vector 38
authenticate rau 39
authenticate service-request 41
authenticate sms 42
authenticate tau 44
cc 45
check-zone-code 48
ciot-optimisation 48
ciphering-algorithm-gprs 50
csfb 51
dcnr 52
decor 52
description 54
diameter-result-code-mapping 54
direct-tunnel 56
dns-ggsn 57
dns-mrme 58
dns-msc 59
dns-sgsn 60
dns-pgw 61
dns-sgw 62
ecn 63
edrx 64
egtp 65
eir-profile 66
encryption-algorithm-lte 67
encryption-algorithm-umts 68
end 69
epdg-s2b-gtpv2 70
epdg-swm 71
equivalent-plmn 72
esm t3396-timeout 74
exit 75

gbr-bearer-preservation-timer 75
gmm Extended-T3312-timeout 76
gmm information-in-messages 77
gmm rau-accept 79
gmm retrieve-equipment-identity 80
gmm t3346 81
gs-service 82
gtp send 83
gtpp 86
gtpu fast-path 87
guti 88
gw-selection 89
hss 91
ie-override 92
ignore-ul-data-status 94
idle-mode-signaling-reduction 94
ims-apn 95
integrity-algorithm-lte 96
integrity-algorithm-umts 98
lcs-mo 98
lcs-mt 99
lcs-ni 100
local-cause-code-mapping apn-mismatch 100
local-cause-code-mapping apn-not-subscribed 101
local-cause-code-mapping apn-not-supported-in-plmn-rat 102
local-cause-code-mapping auth-failure 104
local-cause-code-mapping congestion 105
local-cause-code-mapping ctxt-xfer-fail-mme 106
local-cause-code-mapping ctxt-xfer-fail-sgsn 108
local-cause-code-mapping gw-unreachable 109
local-cause-code-mapping hss-unavailable 110
local-cause-code-mapping map-cause-code 111
local-cause-code-mapping no-active-bearers 113
local-cause-code-mapping odb packet-services 114

local-cause-code-mapping odb roamer-to-vplmn 115
local-cause-code-mapping path-failure 116
local-cause-code-mapping peer-node-unknown 117
local-cause-code-mapping pgw-selection-failure 118
local-cause-code-mapping restricted-zone-code 119
local-cause-code-mapping sgw-selection-failure 120
local-cause-code-mapping vlr-down 121
local-cause-code-mapping vlr-unreachable 122
location-area-list 123
location-reporting 124
lte-zone-code 125
lte-m-rat 127
map 127
map-service 130
max-bearers-per-subscriber 130
max-pdns-per-subscriber 131
min-unused-auth-vectors 132
mme s6a 133
mme sgd 134
mobility-protocol 135
monitoring-events 135
mps 136
msc-fallback-disable 137
nb-iot 138
network-feature-support-ie 140
network-initiated-pdp-activation 141
n1-mode 5gs-interworking-with-n26 144
override-arp-with-ggsn-arp 145
paging-priority 146
pcscf-restoration 148
pdp-activate access-type 148
pdp-activate allow 150
pdp-activate restrict 151
pdn-type-override 152

peer-mme 153
peer-msc 155
peer-nri-length 156
plmn-protocol 157
prefer subscription-interface 158
psm 159
ptmsi-reallocate 161
ptmsi-signature-reallocate 163
qos 165
rau-inter 168
rau-inter-plmn 172
rau-intra 175
re-authenticate 178
regional-subscription-restriction 179
release-access-bearer 181
reporting-action 183
reuse-authentication-triplets 184
rfsp-override 184
rfsp-override ue-settings 185
routing-area-list 187
s1-reset 188
samog-cdr 189
samog-gtpv1 190
samog-s2a-gtpv2 191
sctp-down 193
secondary-rat 193
serving-plmn 194
serving-plmn-rate-control 195
sgs-cause-code-mapping 196
sgsn-address 198
sgsn-core-nw-interface 200
sgsn-number 202
sgtp-service 203
sgw-retry-max 204

sms-in-mme 205
sms-mo 206
sms-mt 207
srns-inter 208
srns-intra 209
srvcc exclude-stnsr-nanpi 211
srvcc 211
subscriber multi-device 212
subscriber-control-inactivity 213
super-charger 214
tau 215
tcp-maximum-segment-size 216
timeout 217
treat-as-hplmn 218
vplmn-address 219
zone-code 220

CHAPTER 2 Call-Home Configuration Mode 223
activate 223
alert-group 224
contact-email-addr 225
contract-id 226
customer-id 227
end 228
exit 228
mail-server 228
phone-number 229
profile 230
rate-limit 231
sender 231
site-id 232
street-address 233

CHAPTER 3 Call-Home Profile Configuration Mode 235

active 235
destination 236
end 238
exit 238
subscribe-to-alert-group 238

CHAPTER 4 CAMEL Service Configuration Mode Commands 243
associate-sccp-network 243
end 244
exit 244
tcap destination-address 245
timeout 245

CHAPTER 5 Card Configuration Mode Commands 249
end 249
exit 249
link-aggregation 250
mode 251
shutdown 252

CHAPTER 6 CBS Service Configuration Mode Commands 255
bind 255
cbc-address-validation 256
cbc-server 257
end 258
exit 258
sabp timer 258
sabp-class2-aggregation 259
tcp-keepalive 259
tcp-mode 260

CHAPTER 7 Cell Trace Module Configuration Mode Commands 263
cell-trace 263
do show 265

end 266
exit 266
file 266

CHAPTER 8 Certificate Policy Configuration Mode Commands 269
do show 269
end 270
exit 270
id 270

CHAPTER 9 CGW Service Configuration Mode Commands 273
associate 273
bind 275
enable-bra-failure-handling 277
end 277
exit 277
gre sequence-numbers 278
reg-lifetime 278
revocation 279
session-delete-delay 280
timestamp-option-validation 281
timestamp-replay-protection 281

CHAPTER 10 Cipher Suite Configuration Mode Commands 283
encryption 283
end 284
exit 284
hmac 285
key-exchange 285

CHAPTER 11 Class-Map Configuration Mode Commands 287
end 287
exit 288
match any 288

match dst-ip-address 289
match dst-port-range 289
match ip-tos 290
match ipsec-spi 291
match packet-size 292
match protocol 293
match src-ip-address 294
match src-port-range 295

CHAPTER 12 Congestion Action Profile Configuration Mode Commands 297
ddn 297
drop 298
end 300
exclude-emergency-events 301
exclude-voice-events 301
exit 302
none 302
reject 304
report-overload 306

CHAPTER 13 Connected Apps Configuration Mode Commands 309
activate 309
ca-certificate-name 310
end 311
exit 311
ha-chassis-mode 311
ha-network-mode 312
rri-mode 313
sess-ip-address 314
sess-name 314
sess-passwd 315
sess-userid 316

CHAPTER 14 Content Filtering Policy Configuration Mode Commands 317

analyze 317
discarded-flow-content-id 322
end 323
exit 323
failure-action 323
timeout action 325

CHAPTER 15 Content Filtering Server Group Configuration Mode Commands 327
connection retry-timeout 327
deny-response code 328
dictionary 329
end 331
exit 331
failure-action 331
header extension options 334
icap server 334
origin address 336
response-timeout 337
timeout action 338
url-extraction 338

CHAPTER 16 Context Configuration Mode Commands A-D 341
aaa accounting 342
aaa authentication 344
aaa constructed-nai 345
aaa filter-id rulebase mapping 347
aaa group 348
aaa nai-policy 349
aaa tacacs+ 350
access-list undefined 351
administrator 351
apgroupname-list 355
apn 356
asn-qos-descriptor 357

asn-service-profile 359
asngw-service 360
asnpc-service 361
associate 362
bfd-protocol 363
bgp extended-asn-cap 364
bmsc-profile 364
busyout ip 365
busyout ipv6 367
cae-group 370
camel-service 371
cbs-service 372
cipher-suite 373
class-map 374
closedrp-rp handoff 375
config-administrator 376
content-filtering 379
credit-control-service 380
crypto dns-nameresolver 381
crypto group 382
crypto ipsec transform-set 383
crypto map 385
crypto template 386
crypto vendor-policy 388
css server 389
cups chunk-threshold-timer 389
cups enabled 389
cups max-user-planes 390
cups min-chunks-threshold-per-pool 390
cups-redundancy-protocol 391
description 392
dhcp-client-profile 392
dhcp-server-profile 393
dhcp-service 394

dhcpv6-service 396
diameter accounting 397
diameter authentication 400
diameter authentication failure-handling 402
diameter dictionary 404
diameter endpoint 404
diameter-hdd-module 406
diameter sctp 407
diameter origin 408
dns-client 408
domain 409

CHAPTER 17 Context Configuration Mode Commands E-H 411
eap-profile 412
edr-module active-charging-service 413
egtp-service 414
end 416
epdg-service 416
event-report-conn 417
event-notif-endpoint 418
exit 419
external-inline-server 420
fa-service 420
firewall max-associations 421
fng-service 421
ggsn-service 422
gprs-service 423
gs-service 425
gtpc high-throughput-sub 426
gtpc overload-protection egress 427
gtpc overload-protection ingress 428
gtpc peer-salvation 432
gtpc-system-param-poll interval 434
gtpp algorithm 435

gtpp attribute 436
gtpp charging-agent 447
gtpp data-record-format-version 448
gtpp data-request sequence-numbers 449
gtpp dead-server suppress-cdrs 450
gtpp deadtime 451
gtpp detect-dead-server 452
gtpp dictionary 453
gtpp duplicate-hold-time 456
gtpp echo-interval 457
gtpp egcdr 458
gtpp error-response 462
gtpp group 462
gtpp max-cdrs 464
sgtpp max-pdu-size 465
gtpp max-retries 466
gtpp node-id 467
gtpp redirection-allowed 468
gtpp redirection-disallowed 469
gtpp server 469
gtpp source-port-validation 471
gtpp storage-server 472
gtpp storage-server local file 473
gtpp storage-server max-retries 477
gtpp storage-server mode 477
gtpp storage-server timeout 479
gtpp suppress-cdrs zero-volume 479
gtpp suppress-cdrs zero-volume-and-duration 481
gtpp timeout 482
gtpp trigger 482
gtpp transport-layer 483
gtpu-service 484
gtpu peer statistics threshold 485
ha-service 486

hexdump-module 487
hnbgw-service 488
hsgw-service 489
hss-peer-service 490

CHAPTER 18 Context Configuration Mode Commands I-M 493
ignore ssh-ip 495
ikev1 disable-initial-contact 495
ikev1 disable-phase1-rekey 496
ikev1 keepalive dpd 497
ikev1 policy 498
ikev2-ikesa 499
ims-auth-service 502
ims-sh-service 503
inspector 504
interface 508
ip access-group 510
ip access-list 511
ip arp 512
ip as-path access-list 513
ip community-list 514
ip dns-proxy source-address 515
ip domain-lookup 516
ip domain-name 517
ip extcommunity-list 518
ip forward 519
ip guarantee 520
ip identification packet-size-threshold 521
ip igmp profile 521
ip localhost 522
ip name-servers 523
ip pool 524
ip prefix-list 539
ip prefix-list sequence-number 540

ip route 541
ip routing maximum-paths 544
ip routing overlap-pool 545
ip rri 546
ip rri-route 547
ip sri-route 548
ip vrf 549
ip vrf-list 550
ipms 551
ipne-service 552
ipsec replay 553
ipsec transform-set 554
ipsg-service 555
ipv6 access-group 557
ipv6 access-list 557
ipv6 dns-proxy 558
ipv6 neighbor 559
ipv6 pool 560
ipv6 prefix-list 564
ipv6 prefix-list sequence-number 566
ipv6 route 566
ipv6 route-access-list 569
ipv6 rri 570
ipv6 rri-route 571
ipv6 sri-route 572
isakmp disable-phase1-rekey 573
isakmp keepalive 573
isakmp policy 573
iups-service 573
l2tp peer-dead-time 574
lac-service 575
lawful-intercept 576
lawful-intercept dictionary 576
limit ipsecmgr ikev1 max 576

lma-service 577
lns-service 579
location-service 580
logging 581
mag-service 584
map-service 585
max-sessions 586
mipv6ha-service 587
mme-embms-service 588
mme-service 590
mobile-access-gateway 592
mobile-ip fa 593
mobile-ip ha assignment-table 594
mobile-ip ha newcall 595
mobile-ip ha reconnect 597
monitor-protocols 598
mpls bgp forwarding 598
mpls exp 599
mpls ip 600
mseg-service 600
multicast-proxy 601

CHAPTER 19 **Context Configuration Mode Commands N-R** 603
nw-reachability server 605
network-requested-pdp-context activate 606
network-requested-pdp-context gsn-map 608
network-requested-pdp-context hold-down-time 609
network-requested-pdp-context interval 610
network-requested-pdp-context sgsn-cache-time 610
operator 611
optimize pdsn inter-service-handoff 615
password 615
pcc-af-service 618
pcc-policy-service 620

pcc-service 621
pcc-sp-endpoint 623
pdg-service 624
pdif-service 625
pdsn-service 626
pdsnclosedrp-service 627
pgw-service 628
policy 629
policy-group 630
policy-map 631
ppp 632
ppp magic-number 637
ppp statistics 638
proxy-dns intercept-list 639
rac-profile 640
radius accounting 640
radius accounting algorithm 643
radius accounting apn-to-be-included 644
radius accounting billing-version 645
radius accounting gtp trigger-policy 646
radius accounting ha policy 647
radius accounting interim volume 648
radius accounting ip remote-address 649
radius accounting keepalive 650
radius accounting rp 651
radius accounting server 654
radius algorithm 658
radius allow 659
radius attribute 660
radius authenticate null-username 662
radius authenticate apn-to-be-included 663
radius authenticator-validation 663
radius change-authorize-nas-ip 664
radius charging 667

radius charging accounting algorithm 668
radius charging accounting server 669
radius charging algorithm 671
radius charging server 672
radius deadtime 674
radius detect-dead-server 675
radius dictionary 677
radius group 678
radius ip vrf 678
radius keepalive 679
radius max-outstanding 681
radius max-retries 682
radius max-transmissions 683
radius mediation-device 684
radius probe-interval 684
radius probe-max-retries 685
radius probe-message 686
radius probe-timeout 686
radius server 687
radius strip-domain 690
radius timeout 690
radius trigger 691
realtime-trace-module 692
remote-server-list 693
route-access-list extended 694
route-access-list named 695
route-access-list standard 697
route-map 698
router 699

CHAPTER 20 Context Configuration Mode Commands S-Z 701
s102-service 702
saegw-service 703
sbc-service 704

server 705
service-redundancy-protocol 707
session-event-module 707
sgsn-service 708
sgs-service 709
sgtp-service 710
sgw-service 711
sls-service 712
smsc-service 713
ssh 715
ssl 716
subscriber 717
sx-service 718
tac-profile 719
threshold available-ip-pool-group 719
threshold ha-service init-rrq-rcvd-rate 721
threshold ip-pool-free 722
threshold ip-pool-hold 723
threshold ip-pool-release 724
threshold ip-pool-used 726
threshold ip-pool-usable 727
threshold ip-pool-usable-final 728
threshold monitoring 729
threshold pdsn-service init-rrq-rcvd-rate 730
twan-profile 731
udr-module active-charging-service 732
udr-module charging-service 733
uidh-server 733
user-plane-service 734
uut-profile name 734
wsg-service 735

CHAPTER 21 **Credit Control Configuration Mode Commands** 737
apn-name-to-be-included 738

app-level-retransmission 739
associate 740
charging-rulebase-name 741
debit-failure-handling 742
diameter dictionary 743
diameter disable-final-reporting-in-ccru 744
diameter dynamic-rules request-quota 745
diameter enable-quota-retry 746
diameter exclude-mscc-in-ccr-terminate 747
diameter fui-redirected-flow 747
diameter gsu-with-only-infinite-quota 748
diameter hdd 749
diameter ignore-returned-rulebase-id 750
diameter ignore-service-id 751
diameter mscc-final-unit-action terminate 752
diameter mscc-per-ccr-update 753
diameter msg-type 754
diameter origin host 756
diameter origin endpoint 756
diameter peer-select 757
diameter pending-timeout 760
diameter reauth-blockedlisted-content 761
diameter redirect-url-token 763
diameter redirect-validity-timer 765
diameter result-code 766
diameter send-ccri 767
diameter service-context-id 768
diameter session failover 769
diameter suppress-avp 770
diameter suppress-ccru zero-gsu-with-validity-timer 771
diameter update-dictionary-avps 772
end 773
event-based-session 773
exit 774

failure-handling 775
gy-rf-trigger-type 778
imsi-imeisv-encode-format 779
mode 780
offline-session re-enable 781
pending-traffic-treatment 782
quota 784
quota request-trigger 785
quota time-threshold 786
quota units-threshold 786
quota volume-threshold 787
radius usage-reporting-algorithm 788
redirect-indicator-received 789
redirect-require-user-agent 790
servers-unreachable 791
subscription-id service-type 797
timestamp-rounding 798
trigger type 799
usage-reporting 800

CHAPTER 22 **Credit Control Service Configuration Mode Commands** 803
diameter dictionary 803
diameter endpoint 804
end 805
exit 805
failure-handling 805
request timeout 806

CHAPTER 23 **CRP Configuration Mode Commands** 809
CRP Configuration Mode Commands 809
node-type 810
monitor bgp context 810
end 811

CHAPTER 24 Crypto Group Configuration Mode Commands 813
end 813
exit 814
match address 814
match ip pool 815
switchover 817

CHAPTER 25 Crypto Map IPSec Dynamic Configuration Mode Commands 819
end 819
exit 820
set 820

CHAPTER 26 Crypto IPSec Configuration Mode Commands 825
end 825
exit 826
replay window-size 826
transform-set 827

CHAPTER 27 Crypto Map IPSec Manual Configuration Mode Commands 829
end 830
exit 830
match address 830
set control-dont-fragment 832
set ip mtu 833
set ipv6 mtu 834
set peer 835
set session-key 836
set transform-set 839

CHAPTER 28 Crypto Map IKEv2-IPv4 Configuration Mode Commands 841
allow-cert-enc cert-hash-url 842
authentication 842

blockedlist 844
ca-certificate list 845
ca-crl list 846
certificate 847
control-dont-fragment 848
end 849
exit 849
ikev2-ikesa 850
keepalive 852
match 853
natt 855
ocsp 856
payload 857
peer 858
remote-secret-list 859
permitlist 860

CHAPTER 29 Crypto Map IPSec IKEv1 Configuration Mode Commands 863
end 863
exit 864
ipsec-on-demux 864
match address 865
match crypto group 866
match ip pool 868
set 869

CHAPTER 30 Crypto Map IKEv2-IPv4 Payload Configuration Mode Commands 875
end 875
exit 876
ipsec 876
lifetime 877
rekey 878

CHAPTER 31 Crypto Map IKEv2-IPv6 Configuration Mode Commands 881

allow-cert-enc cert-hash-url 882
authentication 882
blockedlist 884
ca-certificate list 884
ca-crl list 885
certificate 887
control-dont-fragment 888
end 889
exit 889
ikev2-ikesa 890
keepalive 892
match 893
ocsp 895
payload 896
peer 897
remote-secret-list 898
permitlist 899

CHAPTER 32 Crypto Map IKEv2-IPv6 Payload Configuration Mode Commands 901
end 901
exit 902
ipsec 902
lifetime 903
rekey 905

CHAPTER 33 Crypto Template Configuration Mode Commands 907
allow-cert-enc cert-hash-url 908
allow-custom-fqdn-idr 909
authentication 909
blockedlist 911
ca-certificate list 912
ca-crl list 913
certificate 913
configuration-payload 914

control-dont-fragment 915
dns-handling 916
dos cookie-challenge notify-payload 917
ecn 918
end 919
exit 919
identity local 919
ikev2-ikesa 920
ikev2-ikesa ddos 924
ikev2-ikesa dscp 926
ip 927
ipv6 928
keepalive 929
max-childsa 930
nai 931
natt 932
notify-payload 933
ocsp 934
payload 935
peer network 936
remote-secret-list 937
server certificate 938
timeout 938
vendor-policy 939
permitlist 940

CHAPTER 34 Crypto Template IKEv2-Dynamic Payload Configuration Mode Commands 943
end 943
exit 944
ignore-rekeying-requests 944
ip-address-allocation 945
ipsec transform-set 946
lifetime 946
maximum-child-sa 947

rekey 948
tsi 949
tsr 950

CHAPTER 35 Crypto Template IKEv2-Vendor Configuration Mode Commands 953
configuration-payload 953
do show 954
end 955
exit 955
ikev2-ikesa 955
keepalive 957
payload 958

CHAPTER 36 Crypto Template IKEv2-Vendor Payload Configuration Mode Commands 961
do show 961
end 962
exit 962
ignore-rekeying-requests 962
ipsec 963
lifetime 964
rekey 965

CHAPTER 37 Crypto IPSec Transform Set Configuration Mode Commands 967
end 967
exit 968
mode 968

CHAPTER 38 Crypto Vendor Policy Configuration Mode Commands 971
do show 971
end 972
exit 972
precedence 972

CHAPTER 39 CSS Delivery Sequence Configuration Mode Commands 975
end 975
exit 975
recovery 976
server-interface 976

CHAPTER 40 DDN APN Profile Configuration Mode Commands 977
end 977
exit 977
isr-sequential-paging 978
qci 978

CHAPTER 41 Decor Profile Configuration Mode Commands 981
dcn-id 981
description 982
dns 983
do show 983
end 984
exit 984
mmegi 984
plmn-id 985
served-dcn 986
ue-usage-types 987

CHAPTER 42 DHCP Client Profile Configuration Mode Commands 989
client-identifier 989
dhcpv6-client-unicast 990
disable 991
enable 992
end 993
exit 993
request 993

CHAPTER 43 DHCP Server Profile Configuration Mode Commands 995

dhcpv6-server-preference 995

disable 996

enable 997

end 998

exit 998

process 999

CHAPTER 44 DHCP Service Configuration Mode Commands 1001

allow 1002

bind 1003

default 1005

dhcp chaddr-validate 1006

dhcp client-identifier 1007

dhcp deadtime 1009

dhcp detect-dead-server 1010

dhcp ip vrf 1011

dhcp server 1012

dhcp server selection-algorithm 1014

end 1015

exit 1015

lease-duration 1015

lease-time 1016

max-retransmissions 1017

retransmission-timeout 1018

T1-threshold 1019

T2-threshold 1019

CHAPTER 45 DHCPv6 Client Configuration Mode Commands 1021

end 1021

exit 1022

max-retransmissions 1022

server-dead-time 1023

server-ipv6-address 1024
server-resurrect-time 1025

CHAPTER 46 DHCPv6 Server Configuration Mode Commands 1027
end 1027
exit 1028
ipv6 1028
preferred-lifetime 1029
prefix-delegation 1029
rebind-time 1030
renew-time 1031
valid-lifetime 1032

CHAPTER 47 DHCPv6 Service Configuration Mode Commands 1035
bind 1035
deadtime 1036
detect-dead-server 1037
dhcpv6-client 1038
dhcpv6-server 1039
end 1040
exit 1040
server 1040

CHAPTER 48 Diameter Endpoint Configuration Mode Commands 1043
app-level-retransmission 1044
associate 1045
cea-timeout 1046
connection retry-timeout 1047
connection timeout 1048
description 1049
destination-host-avp 1049
device-watchdog-request 1051
dpa-timeout 1052
dscp 1052

dynamic-peer-discovery 1053
dynamic-peer-failure-retry-count 1054
dynamic-peer-realm 1055
dynamic-route 1056
end 1057
exit 1057
load-balancing-algorithm 1057
max-outstanding 1058
origin address 1059
origin host 1059
origin realm 1061
osid-change 1062
peer 1063
peer-backoff-timer 1066
reconnect-timeout 1067
response-timeout 1068
rlf-template 1069
route-entry 1071
route-failure 1072
server-mode 1074
session-id include imsi 1075
use-proxy 1076
vsa-support 1077
watchdog-timeout 1078

CHAPTER 49 Diameter HDD Module Configuration Mode Commands 1081
diameter-event 1081
end 1086
exit 1086
file 1086

CHAPTER 50 Diameter Failure Handling Template Configuration Mode Commands 1091
end 1091
exit 1092

msg-type 1092

CHAPTER 51 Diameter Host Select Configuration Mode Commands 1097

end 1097

exit 1098

host-select row-precedence 1098

host-select table 1101

CHAPTER 52 DNS Client Configuration Mode Commands 1105

bind 1105

cache algorithm 1106

cache size 1107

cache ttl 1108

case-sensitive 1109

description 1110

end 1110

exit 1110

randomize-answers 1111

resolver 1111

round-robin answers 1112

CHAPTER 53 DSCP Template Configuration Mode Commands 1115

control-packet 1115

end 1117

exit 1117

data-packet 1118



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. 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. 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. 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.
Caution	Alerts you of potential damage to a program, device, or system.

Notice Type	Description
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: `Login:`
Text represented as **commands**	This typeface represents commands that you enter, for example: **show ip access-list** 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: **show card** *slot_number* *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: 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. Required keyword options and variables are surrounded by grouped braces { }. For example: **sctp-max-data-chunks { limit** *max_chunks* **| mtu-limit }** If a keyword or variable is not enclosed in braces or brackets, it is mandatory. For example: **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. These options can be used in conjunction with required or optional keywords or variables. For example: **action activate-flow-detection { intitiation | termination }** or **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:

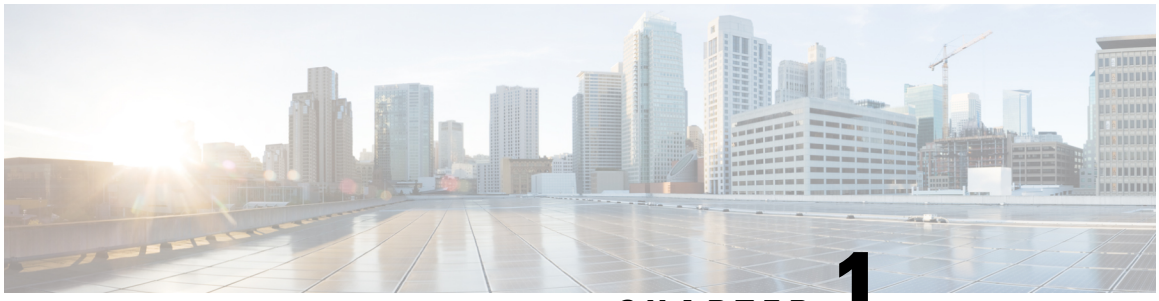
- *AAA Interface Administration and Reference*
- *GTPP Interface Administration and Reference*
- *IPSec Reference*
- Platform-specific System Administration Guides
- Product-specific Administration Guides
- *Release Change Reference*
- *SNMP MIB Reference*
- *Statistics and Counters Reference*
- *Statistics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

Call Control Profile Configuration Mode

The MME and SGSN each support a maximum of 1,000 call control profiles; only one profile can be associated with an operator policy.

By configuring a call control profile, the operator fine tunes any desired restrictions or limitations needed to control call handling per subscriber or for a group of callers across IMSI (International Mobile Subscriber Identity) ranges.

Command Modes

Call Control Profile configuration mode defines call-handling rules which can be combined with other profiles – such as an APN profile (see the *APN Profile Configuration Mode Commands* chapter) – when using the Operator Policy feature. The call control profile is a key element in the Operator Policy feature and the profile is not valid until it is associated with an operator policy (see the **associate** command in the *Operator Policy Configuration Mode Commands* chapter).

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```



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

- a-msisdn, on page 5
- access-restriction-data, on page 6
- accounting context, on page 9
- accounting mode, on page 10
- accounting stop-trigger, on page 11
- allocate-ptmsi-signature, on page 12
- apn-restriction, on page 12
- associate, on page 13
- attach access-type, on page 16
- attach allow, on page 20
- attach imei-query-type, on page 21
- attach implicit-ulr, on page 23
- attach restrict, on page 23

- authenticate, on page 26
- authenticate activate, on page 31
- authenticate all-events, on page 32
- authenticate attach, on page 34
- authenticate context, on page 36
- authenticate detach , on page 37
- authenticate on-first-vector, on page 38
- authenticate rau, on page 39
- authenticate service-request, on page 41
- authenticate sms, on page 42
- authenticate tau , on page 44
- cc, on page 45
- check-zone-code, on page 48
- ciot-optimisation, on page 48
- ciphering-algorithm-gprs, on page 50
- csfb, on page 51
- dcnr, on page 52
- decor, on page 52
- description, on page 54
- diameter-result-code-mapping, on page 54
- direct-tunnel, on page 56
- dns-ggsn, on page 57
- dns-mrme, on page 58
- dns-msc, on page 59
- dns-sgsn, on page 60
- dns-pgw, on page 61
- dns-sgw, on page 62
- ecn, on page 63
- edrx, on page 64
- egtp, on page 65
- eir-profile, on page 66
- encryption-algorithm-lte, on page 67
- encryption-algorithm-umts, on page 68
- end, on page 69
- epdg-s2b-gtpv2, on page 70
- epdg-swm, on page 71
- equivalent-plmn, on page 72
- esm t3396-timeout, on page 74
- exit, on page 75
- gbr-bearer-preservation-timer, on page 75
- gmm Extended-T3312-timeout, on page 76
- gmm information-in-messages, on page 77
- gmm rau-accept, on page 79
- gmm retrieve-equipment-identity, on page 80
- gmm t3346, on page 81
- gs-service, on page 82

- gtp send, on page 83
- gtpp, on page 86
- gtpu fast-path, on page 87
- guti, on page 88
- gw-selection, on page 89
- hss, on page 91
- ie-override, on page 92
- ignore-ul-data-status, on page 94
- idle-mode-signaling-reduction, on page 94
- ims-apn, on page 95
- integrity-algorithm-lte, on page 96
- integrity-algorithm-umts, on page 98
- lcs-mo, on page 98
- lcs-mt, on page 99
- lcs-ni, on page 100
- local-cause-code-mapping apn-mismatch, on page 100
- local-cause-code-mapping apn-not-subscribed, on page 101
- local-cause-code-mapping apn-not-supported-in-plmn-rat, on page 102
- local-cause-code-mapping auth-failure, on page 104
- local-cause-code-mapping congestion, on page 105
- local-cause-code-mapping ctxt-xfer-fail-mme, on page 106
- local-cause-code-mapping ctxt-xfer-fail-sgsn, on page 108
- local-cause-code-mapping gw-unreachable, on page 109
- local-cause-code-mapping hss-unavailable, on page 110
- local-cause-code-mapping map-cause-code, on page 111
- local-cause-code-mapping no-active-bearers, on page 113
- local-cause-code-mapping odb packet-services, on page 114
- local-cause-code-mapping odb roamer-to-vplmn, on page 115
- local-cause-code-mapping path-failure, on page 116
- local-cause-code-mapping peer-node-unknown, on page 117
- local-cause-code-mapping pgw-selection-failure, on page 118
- local-cause-code-mapping restricted-zone-code, on page 119
- local-cause-code-mapping sgw-selection-failure, on page 120
- local-cause-code-mapping vlr-down, on page 121
- local-cause-code-mapping vlr-unreachable, on page 122
- location-area-list, on page 123
- location-reporting, on page 124
- lte-zone-code, on page 125
- lte-m-rat, on page 127
- map, on page 127
- map-service, on page 130
- max-bearers-per-subscriber, on page 130
- max-pdns-per-subscriber, on page 131
- min-unused-auth-vectors , on page 132
- mme s6a, on page 133
- mme sgd, on page 134

- mobility-protocol, on page 135
- monitoring-events, on page 135
- mps, on page 136
- **msc-fallback-disable** , on page 137
- nb-iot, on page 138
- network-feature-support-ie, on page 140
- network-initiated-pdp-activation, on page 141
- n1-mode 5gs-interworking-with-n26, on page 144
- override-arp-with-ggsn-arp, on page 145
- paging-priority, on page 146
- pcscf-restoration, on page 148
- pdp-activate access-type, on page 148
- pdp-activate allow, on page 150
- pdp-activate restrict, on page 151
- pdn-type-override, on page 152
- peer-mme, on page 153
- peer-msc, on page 155
- peer-nri-length, on page 156
- plmn-protocol, on page 157
- prefer subscription-interface, on page 158
- psm, on page 159
- ptmsi-reallocate, on page 161
- ptmsi-signature-reallocate, on page 163
- qos, on page 165
- rau-inter, on page 168
- rau-inter-plmn, on page 172
- rau-intra, on page 175
- re-authenticate, on page 178
- regional-subscription-restriction, on page 179
- release-access-bearer, on page 181
- reporting-action, on page 183
- reuse-authentication-triplets, on page 184
- rfsp-override, on page 184
- rfsp-override ue-settings, on page 185
- routing-area-list, on page 187
- s1-reset, on page 188
- samog-cdr, on page 189
- samog-gtpv1, on page 190
- samog-s2a-gtpv2, on page 191
- sctp-down, on page 193
- secondary-rat, on page 193
- serving-plmn, on page 194
- serving-plmn-rate-control, on page 195
- sgs-cause-code-mapping, on page 196
- sgsn-address, on page 198
- sgsn-core-nw-interface, on page 200

- sgsn-number, on page 202
- sgtp-service, on page 203
- sgw-retry-max, on page 204
- sms-in-mme, on page 205
- sms-mo, on page 206
- sms-mt, on page 207
- srns-inter, on page 208
- srns-intra, on page 209
- srvcc exclude-stnsr-nanpi, on page 211
- srvcc, on page 211
- subscriber multi-device, on page 212
- subscriber-control-inactivity , on page 213
- super-charger, on page 214
- tau, on page 215
- tcp-maximum-segment-size, on page 216
- timeout, on page 217
- treat-as-hplmn, on page 218
- vplmn-address, on page 219
- zone-code, on page 220

a-msisdn

Enables the MME to advertise support for Additional Mobile Station ISDN number (A-MSISDN) functionality to the HSS.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

`[ remove ] a-msisdn`

remove

Disables support for A-MSISDN functionality on the MME. Disabled is the default behavior.

Usage Guidelines

This command enables the MME to notify the HSS of support for Additional-MSISDN for the PLMN associated with this call-control profile in Update Location Request (ULR) messages. Complete the MME configuration to fully support A-MSISDN functionality by instructing the MME to support the AVPs as defined in 3GPP 29.274 Release 11. This is done by using the **3gpp-r11** keyword with the **diameter update-dictionary-avps** command in the HSS Peer Service configuration mode.

With A-MSISDN functionality configured, the MME informs the HSS of A-MSISDN support so the MME sends Feature-List AVP, with an A-MSISDN flag set and the MSISDN, in Update Location Request (ULR) messages over the S6a interface to the HSS at the time a UE Attaches.

If the the MSISDN (A-MSISDN) is available in the subscription data, the HSS sends the provisioned Additional-MSISDN together with the MSISDN in the Update Location Answer (ULA)or the Insert-Subscriber-Data-Request (ISDR). The MME uses the received A-MSISDN as a Correlation-MSISDN (C-MSISDN) in "SRVCC PS to CS Request" and/or in "Forward Relocation Request" messages.

Example

After the **a-msisdn** command has been used to enable support, disable A-MSISDN support with the following command:

```
remove a-msisdn
```

access-restriction-data

Enables the operator to assign a failure code to be included in reject messages if the attach rejection is due to access restriction data (ARD) checking in the incoming subscriber data (ISD) messages. The operator can also disable the ARD checking behavior.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
access-restriction-data { eutran-not-allowed | failure-code cause_code |
no-check | target-access-restriction }
remove access-restriction-data { failure-code | eutran-not-allowed |
no-check | target-access-restriction }
```

remove

Removes the failure code setting or eutran-not-allowed override setting.

eutran-not-allowed

Overrides the eutran-not-allowed flag received in ISD/ULA messages from the HLR/HSS received during the Attach process. The overridden value will be sent to the RNC during PDP context activation (in RAB Assignment Request messages) so that the RNC subsequently avoids performing a handover to E-UTRAN. Configuration of the **eutran-not-allowed** parameter is valid only if SRNS relocation first has been configured in *Call Control Profile Configuration Mode* via the **srns-inter** and/or **srns-intra** commands. The call-control-profile then must be associated with an operator policy in *Operator Policy Configuration Mode*

using the **associate** command. Once the operator policy is associated with the call-control-profile, inclusion of the E-UTRAN Service Handover Information Element in RAB Assignment Request and Relocation Request RANAP messages must be enabled. This is done by executing the **ranap eutran-service-handover-ie** command in *RNC Configuration Mode*.

failure-code *cause_code*

cause_code: Enter an integer from 2 through 111; default code is 13 (roaming not allowed in this location area [LA]).

Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 -MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented

- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

no-check

Including this keyword with the command disables the ARD checking behavior.

target-access-restriction

Including this keyword with the command enables the target access restriction functionality. This functionality works a bit differently for the MME and SGSN:

- MME - No Rejection: if "target-access-restriction" is *not enabled*, then the source-MME *will not* reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.
- MME - Rejection: if "target-access-restriction" is *enabled*, then the source-MME *will* reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.
- SGSN - No Rejection: if "target-access-restriction" is *enabled*, and if "access-restriction-data no-check" is *enabled*, then the source-SGSN *will not* reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.
- SGSN - Rejection: if "target-access-restriction" is *enabled*, and if "access-restriction-data no-check" is *not enabled*, then the source-SGSN will ignore the "target-access-restriction enabled" configuration and the source-SGSN *will* reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

Usage Guidelines

The only feature available to the MME for access-restriction-data is the target access restriction; all others are exclusive to the SGSN.

By default, the SGSN checks access restriction data (ARD) within incoming insert subscriber data (ISD) messages. This enables operator to selectively restrict subscribers in either 3G (UTRAN) or 2G (GERAN). The SGSN ARD checking behavior occurs during the attach procedure and if a reject occurs, the SGSN sends the subscriber an Attach Reject message with a configurable failure cause code.

With the target access restriction feature enabled, including the **no-check** keyword with the command instructs the source-SGSN not to reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

With the target access restriction feature enabled, including the **remove** command filter with the **no-check** keyword instructs the SGSN to reject the outbound RAU Reject based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

Example

For this call control profile, the following command disables the ARD checking function:

```
access-restriction-data no-check
```

accounting context

Defines the name of the accounting context and optionally associates a GTPP group with this call control profile.

Product

ePDG

S-GW

SAEGW

SGSN

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

accounting context *ctxt_name* **[aaa-group** *grp_name* **] [gtpp group** *grp_name* **]**
remove accounting context [aaa-group | gtpp]

remove

Removes the accounting configuration from this profile's configuration.

ctxt_name

Specifies the accounting context as an alphanumeric string of 1 through 79 characters.

aaa-group ***grp_name***

Configures AAA Group for MRME.

*grp_name*is a string of 1 to 63 characters (any combination of letters and digits) to identify the aaa-group created with the **aaa-group** command in the Context configuration mode.

gtpp group ***grp_name***

Identifies the GTPP group, where the GTPP related parameters have been configured in the GTPP Group Configuration mode, to associate with this call control profile.

*grp_name*is a string of 1 to 63 characters (any combination of letters and digits) to identify the GTPP group created with the **gtpp group** command in the Context configuration mode.

Usage Guidelines

This command can be used to associate a predefined GTPP server group - including all its associated configuration - with a specific call control profile. The GTPP group would have been defined with the **gtpp group** command (see the *Context Configuration Mode Commands* chapter).

If the GTPP group is not specified, then a default GTPP group in the accounting context will be used.

If this command is not specified, use the name of the accounting context configured in the SGSN service configuration mode (for 3G) or the GPRS service configuration mode (for 2G), either will automatically use a "default" GTPP group generated in that accounting context.

If the accounting context is specified in the GPRS service or SGSN service and in a call control profile, the priority is given to the accounting context of the call control profile.

Example

For this call control profile, the following command identifies an accounting context called *acctng1* and associates a GTPP server group named *roamers* with defined charging gateway accounting functionality.

```
accounting context acctng1 gtpp group roamers
```

accounting mode

Configures the mode to be used for accounting – GTPP (default), RADIUS/Diameter or None.

Product

ePDG

S-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
accounting mode { gtpp | none | radius-diameter }
remove accounting mode
```

remove

Removes the accounting mode.

gtpp

Specifies that GTPP accounting is performed. This is the default method.

none

Specifies that no accounting will be performed for the call control profile.

radius-diameter

Specifies that RADIUS/Diameter will be performed for the call control profile.

Usage Guidelines Use this command to specify the accounting mode for a call control profile. For additional information on accounting mode and its relationship to operator policy, refer to the *System Administration Guide*.

Example

The following command specifies that RADIUS/Diameter accounting will be used for the call control profile:

```
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 > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

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

Accounting stop CDR triggered once Delete Session/Delete Bearer Response is received at S-GW.

Usage Guidelines Use this command to specify the trigger point for accounting stop CDR for a call control profile.

Example

The following command specifies that accounting stop trigger would be at response of session deletion:

```
accounting stop-trigger custom
```

allocate-ptmsi-signature

Enables or disables the allocation of a P-TMSI (Packet Temporary Mobile Subscriber Identity) signature.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ no | default ] allocate-ptmsi-signature`

no

Disables the allocation of the P-TMSI signature.

default

Resets the configuration value to the default, which is to allocate the P-TMSI signature.

Usage Guidelines

Use this command to enable or disable the allocation of the P-TMSI signature.

Example

`allocate-ptmsi-signature`

apn-restriction

Enables the APN restriction feature and configures the instruction for the SGSN on the action to take when an APN restriction value is received from the GGSN during an Update PDP Context procedure.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`apn-restriction update-policy deactivate` *`restriction`*
`default apn-restriction`

default

Creates a default APN restriction configuration.

update-policy deactivate *restriction*

Specifies one of the two restriction types to define the appropriate action if the APN restriction value received conflicts with the stored value:

- **least-restrictive** set the least restrictive value applicable when there are no already active PDP context(s).
- **most-restrictive** sets the most stringent restriction required by any already active PDP context(s).

Usage Guidelines

When this feature is enabled, the SGSN will send the maximum APN restriction value in every CPC Request message sent to the GGSN. The SGSN expects to receive an APN restriction value in each PDP Context received from the GGSN. The SGSN stores and compares received APN restriction values to check for conflicts. In the case of a conflict, the SGSN rejects the PDP Context with appropriate messages and error codes to the MS.

If an APN restriction value is not assigned by the GGSN, the SGSN assumes the value of "1" (least restrictive) to allow APN restriction rules will be possible when valid values are assigned for new PDP Context(s) from the same MS.

The least or most restrictive values of the APN restriction are applicable only for the Gn SGSN, as the APN restriction can be present in UPCQ/UPCR for Gn SGSN and this configuration is required to determine the PDN to be de-activated when an APN restriction violation occurs during modification procedures in the Gn SGSN. In the case of S4-SGSN, the APN restriction arrives at the S4-SGSN only in Create Session Response during activation. During activation in S4-SGSN, a PDN connection that violates the current Maximum APN restriction is always de-activated. Therefore in the case of S4-SGSN, this CLI is used only for enabling or disabling APN restriction.

Example

The following command applies the lowest level of APN restrictions:

```
apn-restriction update-policy deactivate least-restrictive
```

associate

Associates various MME -specific lists and databases with this call control profile. On an SGSN, this command can be used to associate some of these MME-related items to GPRS and/or SGSN services in support of S4 functionality. For SaMOG, this command can be used to associate various SGW and SGSN CDR triggers for the call control profile.

Product

ePDG

MME

SGSN

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

associate { access-policy *policy_name* **| accounting-policy** *policy_name* **| decor-profile** *profile_name* **access-type { all | eutran | nb-iot } | ho-restrict-list** *list_name* **| hss-peer-service** *service_name* **[s13-interface | s6a-interface | s13-prime-interface | s6d-interface] | scef-service** *service_name* **| tai-mgmt-db** *tai-db_name* **}**
remove associate { access-policy | accounting-policy | decor-profile *profile_name* **access-type { all | eutran | nb-iot } | ho-restrict-list | hss-peer-service [s13-interface diameter-destination-realm** *realm_name* **| s6a-interface diameter-destination-realm***realm_name***| s13-prime-interface | s6d-interface] | tai-mgmt-db }**

remove

Remove the specified association definition from the call control profile.

access-policy *policy_name*

Specifies the access-policy to be associated with the call-control-profile.

policy_name must be an alphanumber string of 1 through 64 characters.

associate monitoring-event-profile *profile_monte*

Specifies the monitioring event profile to be associated with the call-control-profile.

accounting-policy *policy_name*

SaMOG only.

Important With SaMOG mixed license, SaMOG supports both SGSN and SGW CDRs. With SaMOG 3G license, SaMOG supports only SGSN CDRs.

Associates the APN with specific pre-configured policies configured in the same context for SaMOG charging.

policy_name must be an alphanumber string of 1 through 63 characters.

decor-profile *profile_name* access-type { all | eutran | nb-iot }

Specifies the DECOR profile that is associated with the call-control-profile. *profile_name* must be an alphanumerric string of 1 through 63 characters.

A maximum number of 16 decor-profile associations can be configured for the call-control-profile.

access-type: Configures the type of network access for the decor-profile.

- **all** : Specifies allows all access types.

- **eutran**: Specifies the access type as E-UTRAN.
- **nb-iot**: Specifies the access-type as NB-IoT.

ho-restrict-list *list_name*

MME only.

Identifies the handover restriction list that should be associated with this call control profile.

list_name is a string of 1 to 64 characters (any combination of letters and digits).

hss-peer-service *service_name*

Associates a home subscriber server (HSS) peer service with this call control profile.

service_name is an existing HSS peer service expressed as a string of 1 to 63 characters (any combination of letters and digits).

[s13-interface diameter-destination-realm *realm_name* | s6a-interface diameter-destination-realm*realm_name* | s13-prime-interface | s6d-interface]

Optionally, identify the interface to be associated with the HSS service in this call control profile.

The **s13-interface** and the **s6a-interface** options apply to the MME only.

The **s13-prime-interface** and **s6d-interface** options apply to the SGSN only.

The **s6d-interface** is used by the SGSN to communicate with the HSS. It is a Diameter-based interface which supports location management, subscriber data handling , authentication , and fault recovery procedures.

The **s13-prime-interface** is used by the SGSN to communicate with the equiprement identity register (EIR). It is a Diameter-based interface which performs the mobile equipment (ME) identity check procedure.



Important The **s13-prime-interface** can only be used if an **s6d-interface** is configured.

tai-mgmt-db *tai-db_name*

Identifies the tracking area identifier (TAI) database that should be associated with this call control profile.

tai-db_name is a string of 1 to 64 characters (any combination of letters and digits).

This configuration overrides the S-GW selection and TAI list assignment functionality for a call that uses an operator policy associated with this call control profile. The TAI management object provides a TAI list for calls and provides S-GW selection functionality if a DNS is not configured for S-GW discovery for this operator policy or if a DNS discovery fails.

If a TAI management database is associated with a call-control-profile, and if DNS is used for S-GW lookups, then the DNS configuration for S-GW lookups must also be configured within the same call-control-profile using the **dns-sgw** command in the call-control-profile configuration mode.

On the S4-SGSN, use this option to associate a locally configured S-GW address for the RAI address for selection if operators wish to bypass DNS resolution of RAI FQDN. This option is valid only after the following commands have been executed on the S4-SGSN:

- The **tai-mgmt-db** command in *LTE Policy Configuration Mode*

- The **tai-mgmt-obj** command in *LTE TAI Management Database Configuration Mode*.
- The **tai** and **sgw-address** commands in *LTE TAI Management Object Configuration Mode*.

Usage Guidelines

Use this command to associate handover restriction lists, HSS service (and interfaces), and a TAI database with the call control profile. This ensures that the information is available for application when a Request is received.

For SaMOG, use this command to associate the SaMOG call control profile with an accounting policy configured in this context to provide triggers to generate CDRs. If no policy is configured, triggers based on the call control profile will not be generated, and the accounting policy in the SaMOG service context will be used. Even if an accounting policy is also specified in a call control profile, the priority is given to the accounting policy of the APN profile.

Repeat the command as needed to associate each feature.

Example

Link HO restriction list named *HOrestrict1* with this call control profile:

```
associate ho-restrict-list HOrestrict1
```

The following command associates this SaMOG call control profile with an accounting policy called *acct1*:

```
associate accounting-policy acct1
```

attach access-type

Defines attach-related configuration parameters for this call control profile based on the access-type (GPRS, UMTS, or both) and location area list.



Important SGSN only: Before using this command, ensure that the appropriate location area code (LAC) information has been defined via the **location-area-list** command.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > **call-control-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

attach access-type { gprs | umts } { all | location-area-list instance *list_id* **} { failure-code** *code* **| user-device-release { before-r99 failure**

```
code code | r99-or-later failure code code } }
default attach access-type { eps | gprs | umts } { all | location-area-list
 instance list_id } { failure-code | user-device-release { before-r99
failure code | r99-or-later failure code }
```

default

Restores the default values for the for the specified parameter.

access-type *type*

Defines the type of access to be allowed or restricted.

- **gprs**
- **umts**

all

Instructs the SGSN or MME to apply the command action to all location area lists. Location area lists should already have been created with the **location-area-list** command. The location area list consists of one or more LACs, location area codes, where the MS is when placing the call.

location-area-list instance *list_id*

Instructs the SGSN to apply the command action to a specific location area list. Location area lists should already have been created with the **location-area-list** command. The location area list consists of one or more LACs, location area codes, where the MS is when placing the call.

Using this keyword with either the **allow** or **restrict** keywords enables you to configure with more granularity.

list_id: Enter an integer between 1 and 5.

failure-code *fail_code*

Specify a GMM failure cause code to identify the reason an attach did not occur. This GMM cause code will be sent in the reject message to the MS.

Default: 14.

fail_code: Enter an integer from 2 to 111. Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed

- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 -MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified



Note It is mandatory to enable the command **attach restrict access-type gprs all** so that the failure code is saved after a re-boot. The **attach access-type gprs all failure-code < code >** command and the attach restrict access-type gprs all command work together and have to be enabled together.

user-device-release { before-r99 | r99-or-later } failure-code *code*

Default: disabled

Enables the SGSN to reject an Attach procedure based on the detected 3GPP release version of the MS equipment and selectively send a failure cause code in the reject message. The SGSN uses the following procedure to implement this configuration:

1. When Attach Request is received, the SGSN checks the subscriber's IMSI and current location information.
2. Based on the IMSI, an operator policy and call control profile are found that relate to this Attach Request.
3. Profile is checked for access limitations.

4. Attach Request is checked to see if the revision indicator bit is set
   - if not, then the configured common failure code for reject is sent;
   - if set, then the 3GPP release level is verified and action is taken based on the configuration of this parameter

One of the following options must be selected and completed:

- **before-r99**: Indicates the MS would be a 3GPP release prior to R99 and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

- **r99-or-later** : Indicates the MS would be a 3GPP Release 99 or later and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

Usage Guidelines

Once the IMSI of an incoming call is known and matched with a specific operator policy, according to the filter definition of the **mcc** command, then the associated call control profile is selected to determine how the incoming call is handled.

By default, all attaches are allowed. If no access limitations are needed, do not use the **attach** command.



Important Before using this command, ensure that the appropriate LAC information has been defined with the **location-area-list** command.

Use this command to define attach limitations for the call control profile.

Use this command to fine-tune the attach configuration specifying which calls/subscribers can attach and which calls are restricted from attaching and what failure code is included in the Reject message.

Attachment restrictions can be based on any one or combination of the options, such as location area code or access type. It is even possible to restrict all attaches.

The command can be repeated using different keyword values to further fine-tune the attachment configuration.

Related Commands

- Use the **attach restrict** command to restrict attaches.
- Use the **attach allow** command to re-enable restrictions after an **attach restrict** command has been used.

Example

The following example sets all restrictions for access-type gprs and specified release version to the default setting.

```
default attach access-type gprs all user-device-release before-r99
failure-code
```

attach allow

Configures the system to re-enable attaches that were previously restricted using the **attach restrict** command.

Important SGSN only: Before using this command, ensure that the appropriate location area code (LAC) information has been defined via the **location-area-list** command.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

`[ no ] attach allow access-type { eps | gprs | umts } location-area-list instance` *`instance_id`* **`| routing-area-list instance`** *`instance_id`*

no

Deletes the specified attach configuration.

allow

Enables attaches in the configuration after an **attach restrict** command has been used.

access-type *type*

Defines the type of access to be allowed.

- **eps**
- **gprs**
- **umts**

location-area-list instance *instance_id*

Instructs the SGSN to apply the command action to a specific location area list. Location area lists should already have been created with the **location-area-list** command. The location area list consists of one or more LACs, location area codes, where the MS is when placing the call.

instance_id must be an integer from 1 to 5.

routing-area-list instance *instance_id*

Instructs the SGSN to apply the command action to a specific routing area list. Routing area lists should already have been created with the **routing-area-list** command.

instance_id must be an integer from 1 to 5.

Usage Guidelines

Once the IMSI of an incoming call is known and matched with a specific operator policy, according to the filter definition of the **mcc** command, then the associated call control profile is selected to determine how the incoming call is handled.

By default, all attaches are allowed. If no access limitations are needed, then do not use the **attach** command.

Important Before using this command, ensure that the appropriate LAC information has been defined with the **location-area-list** command.

Use this command to define attach limitations for the call control profile.

Use this command to fine-tune the attach configuration specifying which calls/subscribers can attach and which calls are restricted from attaching and what failure code is included in the Reject message.

Attachment restrictions can be based on any one or combination of the options, such as location area code or access type or routing area code. It is even possible to restrict all attaches.

The command can be repeated using different keyword values to further fine-tune the attachment configuration.

Related Commands

- Use the **attach access-type** command to define the type of access to restrict or allow.
- Use the **attach restrict** command to restrict attaches.

Example

For calls under the purview of this call control profile, the following command allows attaches of **all** subscribers using the GPRS access type.

```
attach allow access-type gprs all
```

attach imei-query-type

Defines device Attach limitations for this call control profile if an IMEI is not already present in the Attach Request.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
attach imei-query-type { imei | imei-sv | none } [
verify-equipment-identity [ allow-on-eca-timeout | deny-greylisted |
deny-unknown | verify-emergency ] + ]
remove attach imei-query-type
```

remove

Deletes the specified attach configuration.

imei-query-type { imei | imei-sv | none }

Configures system behavior during Attach procedures if an IMEI is not already present in the Attach Request.

- **imei**: Specifies that the system is required to query the UE for its International Mobile Equipment Identity (IMEI).
- **imei-sv**: Specifies that the system is required to query the UE for its International Mobile Equipment Identity - Software Version (IMEI-SV).
- **none**: Specifies that the system does not need to query for IMEI or IMEI-SV.

verify-equipment-identity [allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency]

Specifies that the identification (IMEI or IMEI-SV) of the UE is to be performed by the Equipment Identity Register (EIR) over the S13 interface.

- **allow-on-eca-timeout**: Configures the MME to allow equipment that has timed-out on ECA during the attach procedure.
- **deny-greylisted**: Configures the MME to deny grey-listed equipment during the attach procedure.
- **deny-unknown**: Configures the MME to deny unknown equipment during the attach procedure.
- **verify-emergency**: Configures the MME to ignore the IMEI validation of the equipment during the attach procedure in emergency cases. This keyword is only supported in release 12.2 and higher.

Usage Guidelines

Configures system settings related to the UE Attach procedure for the specified call control profile

The command can be repeated using different keyword values to further fine-tune the attachment configuration.

Example

The following command configures the system to query the UE for its IMEI and to verify the UE equipment identity with an Equipment

```
attach imei-query-type imei verify-equipment-identity
```

attach implicit-ulr

Configures the implicit sending of ULR during local GUTI attach.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`attach implicit-ulr`

Example

The following command configures the implicit sending of ULR during local GUTI attach

`attach implicit-ulr`

attach restrict

Configures the system to restrict attaches based on access type, routing areas, and location areas (either all or specified location area list) for this call control profile.



Important SGSN only: Before using this command, ensure that the appropriate location area code (LAC) information has been defined via the **location-area-list** command.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ no ] attach restrict access-type { eps [ emm-cause-code` *`code`* **| imsi-attach-fail [emm-cause-code** *`code`* **] | voice-unsupported [`**

emm-cause-code *code* **]] | gprs | umts } { all | location-area-list instance** *instance_id* **| routing-area-list instance** *instance_id* **}**

no

Deletes the specified attach configuration.

access-type *type*

Defines the type of access to be allowed or restricted.

- **eps**
- **gprs**
- **umts**

emm-cause-code *code*

Specifies the EPS Mobility Management (EMM) cause code to return to the UE:

- **eps-service-disallowed**
- **eps-service-not-allowed-in-this-plmn**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

The default cause code is **no-suitable-cell-in-tracking-area**.

Important The **tracking-area-not-allowed** cause code is not supported for the MME.

Important The **roaming-not-allowed-in-this-tracking-area** and **tracking-area-not-allowed** cause codes are not applicable for use with the **imsi-attach-fail** or **voice-unsupported** keywords.

imsi-attach-fail

Directs the MME to restrict EPS attach when IMSI attach fails. If the policy is configured, all IMSI failures will result in a EPS restriction.

The default cause code for calls rejected for imsi-attach-fail is **no-suitable-cell-in-tracking-area**.

voice-unsupported

Directs the MME to restrict EPS attach when voice is not supported, such as when Voice over IMS is not supported and the UE does not support Circuit Switched Fall Back (CSFB).

This setting is applicable when all of the following conditions apply:

- The UE is voice-centric as determined in the UE usage setting of the Voice Domain and UE Settings IE sent in the request.
- The UE does not support CSFB as determined in the EMM Combined procedures Capability bit of the MS Network Capability IE sent in the request, OR if CSFB is not supported on the MME as determined by the SGs service not being associated with the MME service.
- Voice over IMS is not supported in the network as defined by the **network-feature-support-ie ims-voice-over-ps** command.

The default cause code for calls rejected for voice-unsupported is **no-suitable-cell-in-tracking-area**.

all

Instructs the system to apply the command action to all location area lists. Location area lists should already have been created with the **location-area-list** command. The location area list consists of one or more LACs, location area codes, where the MS is when placing the call.

location-area-list instance *instance_id*

Instructs the SGSN to apply the command action to a specific location area list. Location area lists should already have been created with the **location-area-list** command. The location area list consists of one or more LACs, location area codes, where the MS is when placing the call.

Using this keyword with either the **allow** or **restrict** keywords enables you to configure with more granularity.

instance_id must be an integer from 1 to 5.

Important This keyword only applies to the SGSN.

routing-area-list instance *instance_id*

Instructs the SGSN to apply the command action to a specific routing area list. Routing area lists should already have been created with the **routing-area-list** command.

instance_id must be an integer from 1 to 5.

Usage Guidelines

Once the IMSI of an incoming call is known and matched with a specific operator policy, according to the filter definition of the **mcc** command, then the associated call control profile is selected to determine how the incoming call is handled.

By default, all attaches are allowed. If no access limitations are needed, then do not use the **attach** command.

Important Before using this command, ensure that the appropriate LAC information has been defined with the **location-area-list** command.

Use this command to restrict attaches for the call control profile.

Use this command to fine-tune the attach configuration specifying which calls/subscribers can attach and which calls are restricted from attaching and what failure code is included in the Reject message.

Attachment restrictions can be based on any one or combination of the options, such as location area code or access type or routing area code. It is even possible to restrict all attaches.

The command can be repeated using different keyword values to further fine-tune the attachment configuration.

Related Commands

- Use the **attach access-type** command to define the type of access to restrict or allow. The command attach restrict **access-type gprs all** has to be enabled , if the command attach **access-type gprs all failure-code < code >** is used to define a failure code. The failure code is saved after a re-boot only when the command attach restrict access-type gprs all is enabled.
- Use the **attach allow** command to re-enable restrictions after an **attach restrict** command has been used.

Example

For calls under the purview of this call control profile, the following command restricts the attaches of **all** subscribers using the GPRS access type.

```
attach restrict access-type gprs all
```

To change the attach restriction to only restrict attaches of GPRS subscribers from specified LACs included in location area list #2 and include failure-code 45 as the reject cause. This configuration requires two CLI commands:

```
attach restrict access-type gprs location-area-list instance 2
attach access-type gprs location-area-list instance 2 failure-code 45
```

In the case of a dual-access SGSN, it is possible to also add a second definition to restrict attaches of UMTS subscribers within the LACs included in location area list #3.

```
attach restrict access-type UMTS location-area-list instance 3
```

Change the configuration to allow attaches for GPRS access for all previously restricted LACs - note that GPRS attaches would still be limited:

```
no attach restrict access-type gprs all
```

Restrict (deny) all GPRS attach requests (coming from any location area) and assign a single failure code for the reject messages. This is a two command process:

```
attach restrict access-type
gprs all
attach access-type grps
all failure-code 22
```

authenticate

Enables or disables authentication for procedures, such as Attach and Service Request.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
[ no ] authenticate { activate [ access-type { gprs | umts } ] | first [
 access-type { gprs | umts } ] | frequency frequency | primary [ access-type
 { gprs | umts } ] | all-events [ access-type { gprs | umts } | frequency
  frequency | attach [ access-type { gprs | umts } | attach-type { combined
 | gprs-only } [ access-type { gprs | umts } | frequency frequency ] |
frequency frequency | inter-rat [ access-type { gprs | umts } ] ] | detach
 [ access-type { gprs | umts } ] | on-first-vector | rau | service-request
 | sms [ access-type { gprs | umts } | frequency  frequency| sms-type {
mo-sms | mt-sms } { ] | tau }
default authenticate { activate | attach | detach | rau | service-request
 }
remove authenticate on-first-vector
```

no

Disables and removes the defined authentication configuration from the call control profile.

default

Resets all parameters to default values for the authentication process configured for this call control profile.

remove

Removes the defined parameter from the configuration.

activate

This keyword enables/disables authentication for activate requests and optionally works with one or more of the following options to the configuration:

- **access-type** *type*: Select one of the two options:
  - **gprs**
  - **umts**
- **first -** Enables/disables authentication for first activate.
- **frequency** *frequency* - Defines 1-in-N selective authentication of subscriber events - where an event is an Attach Request, RAU, Service Request, Activate-Primary-PDP-Context Request, or Detach Request. If the frequency is set for 12, then the SGSN skips authentication for the first 11 events and authenticates on the 12th event.

  frequency must be an integer from 1 to 16.
- **primary -** Enables/disables authentication for every primary activate request.

all-events

Specifies that procedures - attaches, service requests, RAUs, detaches, and activations - will be authenticated. This can be fine-tuned by adding either or both of the following parameters:

- **access-type** *type* must be one of the two:
  - **gprs**
  - **umts**
- **frequency** *frequency* - Defines 1-in-N selective authentication of subscriber events - where an event is an Attach Request, RAU, Service Request, Activate-Primary-PDP-Context Request, or Detach Request. If the frequency is set for 12, then the SGSN skips authentication for the first 11 events and authenticates on the 12th event.

  frequency must be an integer from 1 to 16.

attach

This keyword configures the Attach authentication parameters. It enables/disables authentication for an Attach with a local P-TMSI or Attaches with an IMSI will be authenticated to acquire the CK (cipher key) and the IK (integrity key).

- **access-type** *type*: Must be one of the following options:
  - **gprs**
  - **umts**
- **attach-type** *type*: Must be one of the following options:
  - **combined**: Authenticates combined GPRS/IMSI Attaches.
  - **gprs-only**: Authenticates GRPS Attaches only.
- **frequency** *frequency* - Defines 1-in-N selective authentication of subscriber events - where an event is an Attach Request, RAU, Service Request, Activate-Primary-PDP-Context Request, or Detach Request. If the frequency is set for 12, then the SGSN skips authentication for the first 11 events and authenticates on the 12th event.

  frequency must be an integer from 1 to 16.
- **inter-rat**: Enables authentication for Inter-RAT Attaches.

detach

This keyword enables/disables and configures the access-type authentication for detach.

access-type *type*: must be one of the following:

- **gprs**
- **umts**

on-first-vector

SGSN only

This keyword configures the SGSN to begin MS authentication immediately after receiving the first vector from the HLR. SAI then runs in parallel.

rau

This keyword enables/disables and configures authentication for routing area updates (RAUs).

- **access-type** *type*: Must be one of the two options:
  - **gprs**
  - **umts**
- **frequency** *frequency* - Defines 1-in-N selective authentication of subscriber events - where an event is an Attach Request, RAU, Service Request, Activate-Primary-PDP-Context Request, or Detach Request. If the frequency is set for 12, then the SGSN skips authentication for the first 11 events and authenticates on the 12th event.

  frequency must be an integer from 1 to 16.
- **periodicity** *duration*: Defines the length of time (number of minutes) that authentication can be skipped.

  duration: Must be an integer from 1 to 10800.
- **update-type**: Defines the type of RAU Request. Select one of the following:
  - **combined-update { access-type | with inter-rat-local-ptmsi }**
  - **imsi-combined-update { access-type | with inter-rat-local-ptmsi }**
  - **periodic { access-type | frequency | periodicity }**
  - **ra-update { access-type | with inter-rat-local-ptmsi }**

service-request

This keyword enables/disables authentication for service request.

- **frequency** *frequency* - Defines 1-in-N selective authentication of subscriber events - where an event is an attach request, RAU, service request, activate-primary-PDP-context request, or detach request. If the frequency is set for 12, then the SGN skips authentication for the first 11 events and authenticates on the 12th event. *frequency* must be an integer from 1 to 16.
- **periodicity** *duration*: Defines the length of time (number of minutes) that authentication can be skipped.

  duration: Must be an integer from 1 to 10800.
- **service-type**: Defines the service request type. Options include:
  - **data**
  - **signalling**
  - **paging response**

sms

Enable/disable authentication for the short message service (SMS) procedure. Disabled by default. This keyword works with one or more of the following optional criteria:

- **access-type** *type*: Must be one of the two options:
  - **gprs** - Currently, MME only works with this access-type.
  - **umts**
- **frequency** *frequency* - Defines 1-in-N selective authentication of subscriber events - where an event is an attach request, RAU, service request, activate-primary-PDP-context request, or detach request. If the frequency is set for 12, then the MME/SGSN skips authentication for the first 11 events and authenticates on the 12th event. *frequency* must be an integer from 1 to 16.
- **sms-type**: Enables authentication for the following SMS types:
  - **mo-sms**: mobile-originated SMS
  - **mt-sms**: mobile-terminated SMS

tau

MME only.

Enable/disable authentication for the tracking area update procedure, optionally with one of the following criteria:

- **frequency** *frequency* - Defines 1-in-N selective authentication of subscriber events - where an event is an attach request, RAU, service request, activate-primary-PDP-context request, or detach request. If the frequency is set for 12, then the MME skips authentication for the first 11 events and authenticates on the 12th event. *frequency* must be an integer from 1 to 16.
- **inter-rat**: Enables authentication for Inter-RAT Attaches.
- **periodicity** *duration*: Defines the length of time (number of minutes) that authentication can be skipped.

  duration: Must be an integer from 1 to 10800.

Usage Guidelines

Use this command with the **frequency** keyword to determine the support for selective execution of the re-authentication and/or P-TMSI reallocation procedure in case of a 3G service request.

For an SGSN, after an initial attach request, some end devices restart themselves after waiting for the PDP to be established. In such cases, the SGSN restarts and a large number of end devices repeat their attempts to attach. The attach requests flood the radio network, and if the devices timeout before the PDP is established then they continue to retry, thus even more traffic is generated. Use of the **on-first-vector** enables the the operator to avoid the high traffic levels during PDP establishment. This keyword is intended to reduce the time needed to retrieve vectors over the Gr interface, reduce traffic, and increase attach rates.

Example

Configure authentication to occur after every tenth event for GPRS access.

```
authenticate all-events frequency 9 access-type gprs
```

Disable authentication for Inter-RAT Attaches, use:**default authenticate attach inter-rat**

Enable authentication for Inter-RAT RAU of the combined IMSI type:

authenticate rau update-type imsi-combined-update with inter-rat-local-ptmsi

Use the following command to configure the SGSN to begin MS authentication immediately after receiving the first vector from the AuC/HLR:

authenticate on-first-vector

Use the following command to reset the default behavior, so that the SGSN waits to receive all vectors requested in the SAI from the AuC/HLR before begining authentication towards the MS:

remove authenticate on-first-vector

authenticate activate

!!! STARTING IN AUGUST 2014 CSCuo56840 - this command is no longer supported - FCS 15.5. !!! Allows the operator to define authentication procedures in response to a received Activate Request.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

authenticate activate [access-type { gprs | umts } | first | frequency *frequency* **| primary] [access-type { gprs | umts }]**
[no | remove] authenticate activate [access-type { gprs | umts } | first | primary] [access-type { gprs | umts }]]

no

Disables the previously specified activate authentication configuration in the call control profile.

remove

Removes the previously specified activate authentication configuration from the call control profile configuration file and returns to the default 'not configured' state.

access-type *type*



Important At this time, authentication for activation is supported only for 3G access. Functionality is invoked only for UMTS access whether or not the **access-type** keyword is explicitly included in the configuration command sequence.

Specifies the network access type for which the authentication process will be performed::

- **gprs**- *Currently, not supported functionally even though it appears as a selectable option and would **appear** in the configuration file as configured.*
- **umts**

The **access-type** keyword can be included with any of the other three keywords available with the **authenticate activate** command.

first

Including this keyword enables authentication only for the first Activate Request for an MS/UE.

frequency *frequency*

This keyword defines 1-in-N selective authentication for Activate Request events. If the frequency is set for 12, then the SGSN skips authentication for the first 11 events and authenticates on the twelfth event.

frequency must be an integer from 1 to 16.

primary

Including this keyword enables authentication for every primary PDP context Activate Request.

Usage Guidelines

Activate Requests are not authenticated by default. Use this command to enable authentication of Activate Requests.

Repeat the commands as needed to configure desired authentication responses to Activate Request messages for the call control profile.

Example

Configure Request Activate authentication for every primary PDP:

```
authenticate activate primary
```

authenticate all-events

Allows the operator to quickly define authentication procedures, based on limited parameters, for all types of events.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
authenticate all-events [ access-type { gprs | umts } | frequency frequency
 [ access-type { gprs | umts } ] | periodicity duration [ access-type {
gprs | umts } ] ]
 no authenticate all-events [ access-type { gprs | umts } ]
remove authenticate all-events [ access-type { gprs | umts } | frequency
 [ access-type { gprs | umts } ] | periodicity [ access-type { gprs |
umts } ]
```

no

Disables the specified authentication configuration in the call control profile.

remove

Removes the specified authentication configuration from the call control profile configuration file.

access-type *type*

One of the following must be selected to identify the type of network access if the **access-type** keyword is included in the command:

- **gprs**
- **umts**

The **access-type** keyword can be included with any of the other three keywords available with the **authenticate all-events** command.

frequency *frequency*

This keyword defines 1-in-N selective authentication for all types of subscriber events. If the frequency is set for 12, then the service skips authentication for the first 11 events and authenticates on the 12th event.

In releases prior to 21.2, the *frequency* is an integer value from 1 up to 16.

From release 21.2 onwards the *frequency* is an integer value from 1 up to 256.

periodicity *duration*

The periodicity configured specifies authentication periodicity. The periodicity is an integer with a range "1" up to "10800" minutes. For example, if the configured periodicity is "20" minutes, the UE is authenticated at every "20" minutes.

Usage Guidelines

By default, authentication is not performed for any subscriber events. Use this command to enable authentication for all types of events at one time, such as but not limited to: Activate Requests, Attach Requests, Detach Requests, Service-Requests.

Important For the SGSN, in releases 15.0 and forward, the authentication on activation functionality has been removed so the SGSN will not authenticate on Activate Requests.

Example

The following command configures all authentication for all subscriber events to occur every tenth time a specific type of event occurs (for example every tenth time an Attach Request is received):

```
authenticate all-events frequency 10
```

The following command configures authentication for all Detach Requests and RAUs to occur if the UE access-type is UMTS:

```
authenticate all-events access-type umts
```

authenticate attach

Allows the operator to define authentication for Attach procedures.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
authenticate attach access-type { gprs | umts }
authenticate attach attach-type { combined | gprs-only } [ access-type {
 gprs | umts } | frequency frequency ]
authenticate attach frequency  frequency [ access-type { gprs | umts } ]
authenticate attach inter-rat [ access-type { gprs | umts } | attach-type
 { combined | gprs-only } [ access-type { gprs | umts } | frequency frequency
 ] | frequency  frequency [ access-type { gprs | umts } ] | periodicity
duration  [ access-type { gprs | umts } ] ]
authenticate attach periodicity duration [ access-type { gprs | umts } ]
{ no | remove } authenticate attach [ access-type { gprs | umts } |
attach-type { combined | gprs-only } | inter-rat | attach-type { combined
 | gprs-only } ] [ access-type { gprs | umts } ] ]
```

no

Disables the defined authentication procedures configured for Attach Requests from the call control profile.

remove

Deletes the defined authentication procedures for Attach Requests from the call control profile configuration file.

access-type *type*

One of the following must be selected to identify the type of network access if the **access-type** keyword is included in the command:

- **gprs**
- **umts**

attach-type

This keyword configures the Attach authentication based on the type of attach requested. The **attach-type** must be one of the following options:

- **combined**: Authenticates combined GPRS/IMSI Attaches.
- **gprs-only**: Authenticates GRPS Attaches only.

frequency *frequency*

This keyword defines 1-in-N selective authentication for this type of subscriber event - Attach Request. If the frequency is set for 12, then the service skips authentication for the first 11 events and authenticates on the twelfth event.

In releases prior to 21.2, the *frequency* is an integer value from 1 up to 16.

From release 21.2 onwards the *frequency* is an integer value from 1 up to 256.

inter-rat

Enables/disables authentication for Inter-RAT Attaches.

periodicity *duration*

The periodicity configured specifies authentication periodicity. For example, if the configured periodicity is "20" minutes, the UE is authenticated at every "20" minutes.

The *duration*is an integer with a range "1" up to "10800" minutes.

Usage Guidelines

Authentication for Attach is disabled by default. This command enables/disables authentication for an Attach with a local P-TMSI or Attaches with an IMSI, which will be authenticated to acquire the CK (cipher key) and the IK (integrity key).

Example

The following command configures authentication to occur after every tenth attach event for GPRS access.

```
authenticate attach frequency 10 access-type gprs
```

The following command disables authentication for Inter-RAT Attaches, use:

```
no authenticate attach inter-rat
```

authenticate context

This command allows you to specify the authentication group, authentication method, context, and type of authentication for the AAA server.

Product

SaMOG

ePDG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

`authenticate context` *`context_name`* **`[ aaa-group`** *`aaa_group_name`* **`] [ auth-type { diameter | radius } ] [ auth-method { [ eap ] [non-eap] } ]`**
`remove authenticate context [ aaa-group ]`

remove

Sets the authentication type to its default value:

Default (SaMOG 3G license): radius

Default (SaMOG Mixed Mode license): diameter

context_name

Specified the name of the context for authentication.

context_name must be an alphanumeric string of 1 through 79 characters.

aaa-group *aaa_group_name*

Optionally, specifies the AAA group for MRME. *aaa_group_name* must be an alphanumeric string of 1 through 63 characters.

auth-type { diameter | radius }

Optionally, specifies the type of authentication supported by the AAA server.

radius: indicates a RADIUS-based authentication

diameter: indicates a Diameter-based authentication

Important This keyword is available only when the SaMOG Mixed Mode license (supporting both 3G and 4G) is configured. However, when an SaMOG 3G license is configured, the authentication type for the AAA server is set to a RADIUS-based authentication.

auth-method { [eap] [non-eap] }

Optionally, specifies the authentication method for the call control profile.

If this configuration is not used, the default value is EAP based authentication method.

Important The SaMOG Web Authorization feature is license dependent. Contact your Cisco account representative for more information on license requirements.

Usage Guidelines Use this command to specify the authentication group, context, and type of authentication for the AAA server. Also specify an authentication method of EAP or non-EAP or both for the call control profile in the operator policy.

Example

The following command configures authentication of a context named *cxtSaMOG*, specifies AAA group named *AAASaMOG*, and sets the authentication to a DIAMETER-based authentication:

```
authenticate context cxtSAMOG aaa-group AAASaMOG auth-type diameter
```

authenticate detach

Allows the operator to enable and define authentication for Detach procedures.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
authenticate detach [ access-type umts ]
[ no | remove ] authenticate detach [ access-type umts ]
```

no

Disables the defined authentication procedures configured for Detach Requests from the call control profile.

remove

Deletes the defined authentication procedures for Detach Requests from the call control profile configuration file.

access-type umts

Optionally, identifies the type of network access if the **access-type umts** keywords are included in the command. By default, access-type UMTS is assumed.

access-type *type*

The type of network access if the **access-type** keyword is included in the command:

- **umts**

Usage Guidelines

Authentication for Detach procedures is disabled by default. This command enables/disables authentication for a Detach Request and allows the operator to limit authentication based on the MS/UE access-type.

Example

The following command configures detach authentication to occur only for UMTS attached subscribers:

```
authenticate detach access-type umts
```

The following command disables authentication for all Detach Requests, use:

```
no authenticate detach
```

authenticate on-first-vector

Allows the operator to enable the SGSN to begin MS authentication immediately after receiving the first vector from the HLR.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
authenticate on-first-vector
remove authenticate on-first-vector
```

remove

Removes the authenticate on-first-vector definition from the configuration file and resets the default behavior so that the SGSN waits to receive all vectors before beginning authentication towards the MS.

Usage Guidelines

After an initial attach request, some end devices restart themselves after waiting for the PDP to be established. In such cases, the SGSN restarts and a large number of end devices repeat their attempts to attach. The attach requests flood the radio network, and if the devices timeout before the PDP is established then they continue to retry, thus even more traffic is generated.

To avoid the high traffic levels during PDP establishment, the SGSN has been modified to reduce the attach time, as much as possible, so that the devices can attach and discontinue sending requests. The current enhancement is intended to reduce the time needed to retrieve vectors over the GR interface by allowing the operator to configure the SGSN to start authentication towards the MS as soon as it receives the first vector from the AuC/HLR. With the new command included in the configuration, the SGSN begins the MS authentication process immediately after receiving the first vector from the HLR while the SAI continues in parallel.

Example

Use the following command to configure the SGSN to begin MS authentication immediately after receiving the first vector from the AuC/HLR:

```
authenticate on-first-vector
```

Use the following command to reset the default behavior, so that the SGSN waits to receive all vectors requested in the SAI from the AuC/HLR before begining authentication towards the MS:

```
remove authenticate on-first-vector
```

authenticate rau

Enables or disables and fine tunes authentication procedures for routing area updates (RAUs)

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

authenticate rau [access-type { gprs | umts } | frequency *frequency* **[access { gprs | umts }] | periodicity** *duration* **[access { gprs | umts }] | update-type { combined-update | imsi-combined-update | periodic | ra-update } [access-type { gprs | umts } | frequency** *frequency* **| periodicity** *duration* **| with { foreign-ptmsi | inter-rat-local-ptmsi | local-ptmsi } [access-type { gprs | umts } | frequency** *frequency* **| periodicity** *duration* **]**

```
no authenticate rau [ access-type { grps | umts } | update-type {
combined-update | imsi-combined-update | periodic | ra-update } [
access-type { gprs | umts } | with { foreign-ptmsi | inter-rat-local-ptmsi
 | local-ptmsi } [ access-type { gprs | umts } ]
remove authenticate rau [ access-type { gprs | umts } | periodicity [
access { gprs | umts } ] | update-type { combined-update |
imsi-combined-update | periodic | ra-update } [ access-type { gprs | umts
 } | periodicity | with { foreign-ptmsi | inter-rat-local-ptmsi |
local-ptmsi } [ access-type { gprs | umts } | periodicity ] ]
```

no

Disables authentication for the RAUs specified in the configuration for the call control profile.

remove

Deletes the authentication configuration for the RAUs from the call control profile in the configuration file.

access-type *type*

One of the following must be selected to identify the type of network access if the **access-type** keyword is included in the command:

- **gprs**
- **umts**

The **access-type** keyword can be included with any of the other keywords available with the **authenticate rau** command.

frequency *frequency*

Defines 1-in-N selective authentication for RAU events. If the frequency is set for 12, then the SGSN skips authentication for the first 11 events and authenticates on the twelfth event.

In releases prior to 21.2, the *frequency* is an integer value from 1 up to 16.

From release 21.2 onwards the *frequency* is an integer value from 1 up to 256.

periodicity *duration*

Defines the length of time (number of minutes) that authentication can be skipped.

duration: Must be an integer from 1 to 10800.

update-type

Defines the type of RAU Request. Select one of the following:

- **combined-update [access-type | with inter-rat-local-ptmsi]**
- **imsi-combined-update [access-type | with inter-rat-local-ptmsi]**
- **periodic [access-type | frequency | periodicity]**
- **ra-update [access-type | with inter-rat-local-ptmsi]**

Usage Guidelines

By default, authentication is not performed for routing area updates (RAUs). Use this command to enable/disable authentication and to fine tune the authentication procedure based on frequency, periods for skipping authentication and the various types of routing area updates.

Example

The following command configures RAU authentication to occur after every tenth event for GPRS access.

```
authenticate rau frequency 10 access-type gprs
```

The following command disables authentication for RAUs based on the combined IMSI with foreign P-TMSIs, use:

```
no authenticate rau imsi-combined-update with foreign-ptmsi
```

The following command deletes all authentication configuration from the call control profile for all RAUs using GPRS access-type:

```
remove authenticate rau access-type gprs
```

authenticate service-request

Enables or disables and fine-tunes authentication procedures for Service Requests.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
authenticate service-request [ frequency frequency | periodicity duration |
 service-type { data | page-response | signaling } [ frequency frequency |
 periodicity  duration ] ]
no authenticate service-request [ service-type { data | page-response |
signaling } ]
remove authenticate service-request [ frequency | periodicity  |
service-type { data | page-response | signaling } [ frequency | periodicity
 ] ]
```

no

Disables authentication for the Service Requests specified in the configuration for the call control profile.

remove

Deletes the authentication configuration for Service Requests from the call control profile in the configuration file.

frequency *frequency*

Defines 1-in-N selective authentication for this type of subscriber event - Service Request. If the frequency is set for 12, then the service skips authentication for the first 11 events and authenticates on the twelfth event.

In releases prior to 21.2, the *frequency* is an integer value from 1 up to 16.

From release 21.2 onwards the *frequency* is an integer value from 1 up to 256.

periodicity *duration*

Defines the length of time (number of minutes) that authentication can be skipped.

duration: Must be an integer from 1 to 10800.

signaling-type

Defines the type of service being requested by the Service Request. Select one of the following:

- **data**
- **page-response**
- **signaling**

Usage Guidelines

By default, authentication is not performed for Service Requests. Use this command to enable/disable authentication and to fine-tune the authentication procedure based on frequency and periods for skipping authentication and the various types of service. Repeat the commands as needed to configure criteria for all service types.

Example

The following command configures authentication Service Requests for data service to only occur every 5 minutes:

```
authenticate service-request service-type data periodicity 5
```

authenticate sms

Enables or disables and fine tunes authentication procedures for Short Message Service (SMS).

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
authenticate sms [ access-type { gprs | umts } | frequency frequency [
access-type { gprs umts } ] | sms-type { mo-sms | mt-sms } [ access-type
 { gprs | umts } | frequency frequency ] ]
[ no | remove ] authenticate sms [ access-type { gprs | umts } | sms-type
 { mo-sms | mt-sms } [ access-type { gprs umts } ] ]
```

no

Disables authentication for the SMS Requests specified in the configuration for the call control profile.

remove

Deletes the authentication configuration for SMS Requests from the call control profile in the configuration file.

access-type *type*

One of the following must be selected to identify the type of network access if the **access-type** keyword is included in the command:

- **gprs**
- **umts**

The **access-type** keyword can be included with any of the other keywords available with the **authenticate sms** command.

frequency *frequency*

Defines 1-in-N selective authentication for SMS Requests. If the frequency is set for 12, then the SGSN skips authentication for the first 11 events and authenticates on the twelfth event.

In releases prior to 21.2, the *frequency* is an integer value from 1 up to 16.

From release 21.2 onwards the *frequency* is an integer value from 1 up to 256.

sms-type

Enables authentication for the following SMS types:

- **mo-sms**: mobile-originated SMS
- **mt-sms**: mobile-terminated SMS

Usage Guidelines

By default, authentication is not performed for short message service (SMS). Use this command to enable/disable authentication and to fine-tune the authentication procedure based on MS/UE access type and the frequency for the selected SMS type. Repeat the commands as needed to configure criteria for all service types.

Example

The following command configures MO-SMS authentication to occur every fifth request:

```
authenticate sms sms-type mo-sms frequency 5
```

authenticate tau

Allows the operator to enable/disable and fine-tune authentication for the tracking area update (TAU) procedures.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
authenticate tau [ freqency frequency | inter-rat | periodicity interval ]
authenticate tau frequency frequency
authenticate tau inter-rat [ frequency frequency | periodicity duration ]
authenticate tau intra-rat [ frequency frequency | periodicity duration ]
authenticate tau normal [ frequency frequency | periodicity duration ]
authenticate tau periodic [ frequency frequency | periodicity duration ]
authenticate tau periodicity duration
remove authenticate tau frequency
remove authenticate tau inter-rat [ frequency | periodicity ]
remove authenticate tau intra-rat [ frequency | periodicity ]
remove authenticate tau normal [ frequency | periodicity ]
remove authenticate tau periodic [ frequency | periodicity ]
remove authenticate tau periodicity
no authenticate tau
```

no

Disables the TAU authentication procedures specified in the call control profile configuration.

remove

This keyword removes the configured TAU authentication procedures.

frequency *frequency*

Defines 1-in-N selective authentication for this type of subscriber event - a tracking area update for an inter-RAT Attach. If the frequency is set for 12, the MME skips authentication for the first 11 events and authenticates on the twelfth event.

In releases prior to 21.2, the *frequency* is an integer value from 1 up to 16.

From release 21.2 onwards the *frequency* is an integer value from 1 up to 256.

inter-rat

Enables authentication for TAU procedures for inter-RAT Attaches.

intra-rat

This keyword specifies authentication to be applied for Intra-RAT TAU.

normal

This keyword specifies authentication to be applied for normal (TA/LA update) TAU.

periodic

This keyword specifies authentication to be applied for periodic TAU.

periodicity *duration*

Defines the length of time (number of minutes) that authentication can be skipped.

duration: Must be an integer from 1 to 10800.

Usage Guidelines

Authentication for TAU procedures is disabled by default. This command enables/disables authentication for a inter-RAT TAU procedures and allows the operator to limit authentication based on the frequency of the events or elapsed intervals between the events.

Example

The following command configures TAU authentication to occur when there is 15 minutes between inter-RAT Attaches:

```
authenticate tau periodicity 15
```

The following command disables authentication for all TAU Inter-RAT Attaches, use:

```
no authenticate tau
```

cc

Defines the charging characteristics to be applied for CDR generation when the handling rules are applied via the Operator Policy feature.

Product

ePDG

MME

SAEGW

S-GW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
cc { behavior-bit no-records bit_value | gen-cdr-for-profile { [ 0 ] [ 1 ]
 [ 10 ] [ 11 ] [ 12 ] [ 13 ] [ 14 ] [ 15 ] [ 2 ] [ 3 ] [ 4 ] [ 5 ] [ 6 ]
 [ 7 ] [ 8 ] [ 9 ] } | local-value behavior bit_value profile index_bit |
prefer { hlr-hss-value | local-value } }
no cc { behavior-bit no-records | gen-cdr-for-profile }
remove cc { behavior-bit no-records | local-value | prefer }
```

no

Disables the no records generation behavior-bit configuration for this call control profile.

In 21.7 and later releases, use the **no cc gen-cdr-for-profile** CLI command to disable the Controlled SGWCDR Generation feature. In other words, the SGWCDR generation will happen as before.



Important The Controlled SGWCDR Generation feature is not fully qualified in release 21.7. It is available only for testing purposes. For more information, contact your Cisco Accounts representative.

remove

Removes the specified charging characteristic configuration from this profile.

behavior-bit no-records *bit_value*

Default: disabled

Specifies the charging characteristic behavior bit. **no-records** instructs the system not to generate any accounting records regardless of what may be configured elsewhere.

bit_value is an integer from 1 through 12.

gen-cdr-for-profile { [0] [1] [10] [11] [12] [13] [14] [15] [2] [3] [4] [5] [6] [7] [8] [9] }



Important The Controlled SGWCDR Generation feature is not fully qualified in release 21.7. It is available only for testing purposes. For more information, contact your Cisco Accounts representative.

Use this CLI command to generate SGWCDR based on certain Charging-Characteristics profile value received in Charging-Characteristics IE inside CSReq.

- **0 … 15**: Configures CC-profile number 0 for SGWCDR generation ... Configures CC-profile number 15 for SGWCDR generation.

Existing CLI commands for SGWCDR generation are not impacted:

- The **cc gen-cdr-for-profile** CLI command takes effect only if the existing **cc behavior-bit no-records** CLI command has no impact based on Charging-Characteristics profile value received.
- The existing **accounting-mode gtpp** CLI command is still required for SGWCDR generation.

The Controlled SGWCDR Generation feature will not work if the **cc prefer local-value** CLI command is configured.

Subsequent configuration of **cc gen-cdr-for-profile** CLI command results in earlier values being discarded.

The values of **cc gen-cdr-for-profile** CLI command are applicable only for new subscribers connected after the CLI is configured.

local-value behavior *bit_value* profile *index_bit*

Defaults: bit_value = 0x0, index_bit = 8

Sets the local value of the behavior bits and profile index for the charging characteristics when the HLR/HSS does not provide values for these parameters.

bit_value is a hexadecimal value between 0x0 and 0xFFF.

index_bit is an integer value from 1 through 15.

Setting the profile index bis selects different charging trigger profiles to be used with the call control profile. Some of the index values are predefined according to 3GPP standard:

- **1** for hot billing
- **2** for flat billing
- **4** for prepaid billing
- **8** for normal billing

If the HLR/HSS provides the charging characteristics with behavior bits and profile index and the operator prefers to ignore the HLR/HSS values, then *also* configure the **prefer local-value** keyword.

prefer { hlr-hss-value | local-value }

Default: **hlr-hss-value**

Specifies a preference for using charging characteristics settings received from HLR or HSS, or those set by the SGSN or MME locally with the **local-value behavior** command.

- **hlr-hss-value** sets the call control profile to use charging characteristics settings received from HLR or HSS. This is the default preference.
- **local-value** sets the call control profile to use charging characteristics settings from the SGSN or MME only. If no charging characteristics are received from the HLR/HSS then local values will be applied.

Usage Guidelines

Use this command to set the behavior for charging characteristic comings from either an HLR/HSS or locally from an MME/SGSN.

These charging characteristics parameters can also be set within an APN profile with the commands of the APN Profile configuration mode. For generation of M-CDRs, the parameters configured in this mode, Call Control Profile configuration mode, will prevail but for generation of S-CDRs the parameters configured in the APN Profile configuration mode will prevail.

The 12 behavior bits (of the **local-value behavior** keyword) can be used to enable or disable CDR generation.

Example

The following command specifies a rule not to generate charging records (CDRs) and sets the charging characteristics behavior bit to *2*:

```
cc behavior-bit no-records 2
```

check-zone-code

Enables or disables the zone code checking mechanism.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
[ no | remove ] check-zone-code
```

no

Included with the command, this keyword disables the mechanism.

remove

Included with the command, this keyword causes the removal of the current **check-zone-code** configuration and returns to the SGSN to the default where zone-code checking is enabled.

Usage Guidelines

Use this command to enable/disable the zone-code checking function.

Example

Disable checking of the zone code:

```
no check-zone-code
```

ciot-optimisation

This command is used to configure Control Plane (CP) CIoT optimization for an UE.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
ciot-optimisation { cp-optimisation { access-type { all | nb-iot |
wb-eutran } |  ciot-capable-ue } | eps-attach-wo-pdn access-type { all |
 nb- iot | wb-eutran } }
remove ciot-optimisation cp-optimisation  ciot-capable-ue
remove ciot-optimisation eps-attach-wo-pdn access-type { all | nb-iot |
wb-eutran }
```

remove

The keyword remove deletes the existing configuration.

cp-optimisation

Use this keyword to enable Control Plane optimization for an UE.

access-type

Use this keyword to specify the access type extension on which control plane optimization should be enabled. Control plane optimization and EPS attach without PDN can be enabled on both NB-IoT and WB-EUTRAN RATs or on either of them.

ciot-capable-ue

Uses only the ue-nw-capability to determine whether CP optimization or not.

all

Use this keyword to enable control plane optimization on both RAT types WB-EUTRAN and NB-IOT. This keyword is provided to the operator for the ease of configuring. Both NB-IoT and WB-EUTRAN will be considered as two independent access types for all functions.

nb-iot

Use this keyword to enable control plane optimization on the RAT type NB-IoT.

wb-eutran

Use this keyword to enable control plane optimization on the RAT type WB-EUTRAN.

eps-attach-wo-pdn

Use this keyword to enable EPS attach without PDN support for an UE.

Usage Guidelines

Use this command to configure the control plane optimization on the RAT type and to configure EPS attach without PDN support for UE. This command is not enabled by default. The call-control-profile can be associated

with the operator-policy or with IME-TAC group, therefore it is possible to either enable or disable CIoT optimization on a per subscriber (IMSI) basis or on a group of subscribers or on per group of IMEI basis. CIoT optimization can be enabled on both NB-IoT and WB-EUTRAN RATs or on either of them. Enabling one RAT type does not disable the other RAT type.

Example

Use the following command to configure control plane optimization by specifying the access type as NB-IoT:

```
ciot-optimisation cp-optimisation access-type nb-iot
```

Use the following command to configure EPS attach without PDN support for UE, specify the access type as WB-EUTRAN:

```
ciot-optimisation eps-attach-wo-pdn access-type wb-eutran
```

ciphering-algorithm-gprs

Defines the order of preference of the ciphering algorithms.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

`ciphering-algorithm-gprs priority` *`priority algorithm`*
`remove ciphering-algorithm-gprs priority` *`priority`*

remove

Delete the priority definition.

priority *priority*

Sets the order in which the algorithm will be selected for use.

priority is an integer from 1 to 4.

algorithm

Identifies the ciphering algorithm to be used.

algorithm is one of the following: gea0, gea1, gea2, gea3.

Usage Guidelines

Define the order in which the ciphering algorithms are chosen for use. The command can be repeated to provide multiple definitions -- multiple priorities.

Example

Define gea1 as the third priority algorithm:

```
ciphering-algorithm-gprs priority 3 gea1
```

csfb

Configures circuit-switched fallback options. CSFB is the mechanism to move a subscriber from LTE to a legacy technology to obtain circuit switched voice or short message.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
csfb { policy {  ho-restriction | not-allowed | not-preferred | sms-only
 | suppress-call-reject } | sms-only }
remove csfb { policy | sms-only }
```

remove csfb { policy | sms-only }

sms-only: Removes the SMS-only restriction allowing the UE to request voice and short message service (SMS) support for circuit-switched fallback (CSFB).

policy: Removes the configured policy.

policy { ho-restriction | not-allowed | not-preferred | sms-only | suppress-call-reject }

ho-restriction: This keyword enables ho-restriction support for CSFB MO Emergency Calls. If this keyword is enabled the MME sets the "Additional CS Fallback Indicator IE" in S1AP UE Context Setup/Modification as "restriction".

not-allowed: Specifies that the CSFB function is not allowed for both voice and SMS.

not-preferred: Specifies that the MME returns a "not-preferred" response for CSFB services. The MME does not enforce this and a voice centric is allowed to make CSFB calls on a not-preferred case if it chooses to do so.

sms-only: Specifies that the CSFB function only supports SMS.

suppress-call-reject: Configures the MME to ignore a paging request for an SMS-only CS call for an attached UE and suppress the paging reject. This allows the MME to process SGs CS call SMS-only paging requests for Ultra Card users where the same MSISDN is allocated to different IMSIs. By default the MME will reject the paging request with a cause:
SGSAP_SGS_CAUSE_MOBILE_TERMINATING_CSFB_REJECTED_BY_USER

sms-only

Specifies that the circuit-switched fallback function only supports SMS.

Important This is a legacy keyword that remains to support earlier versions of the code. It operates identically to the **policy sms-only** keyword.

Usage Guidelines Use this command to restrict the circuit-switched fallback function to SMS only or no support for either voice or SMS.

Example

The following command enforces the SMS-only functionality for UEs requesting circuit-switched fallback:

```
csfb policy sms-only
```

dcnr

Enables Dual Connectivity with New Radio (DCNR) to support 5G Non Standalone (NSA).

Product MME, SGSN

Privilege Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
[ no | remove ] dcnr
```

no

Disables the DCNR configuration.

remove

Removes the configured values for DCNR.

Usage Guidelines Use this command to enable DCNR for 5G NSA support.

decor

This command allows you to locally configure the UE Usage Type for UEs that complies with the Call Control Profile match criteria.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`decor { s6a ue-usage-type [ suppress ] | send-ue-usage-type-in-csr | ue-usage-type` *`usage_type_value`* **`}`**
`remove decor { s6a ue-usage-type | send-ue-usage-type-in-csr | ue-usage-type }`

remove

Removes the specified DECOR configuration from the Call Control Profile.

decor

Specifies the Dedicated Core Network configuration.

s6a ue-usage-type [suppress]

Configures the S6a interface for DECOR configuration.

ue-usage-type: Specifies the UE usage type that needs to be sent in the Authentication-Information-Request message over the S6a interface.

suppress: Suppresses sending the UE usage type in S6a Authentication-Information-Request message.

send-ue-usage-type-in-csr

Enables the sending of ue-usage-type in create-session-request to SPGW.

ue-usage-type *usage_type_value*

Configures the UE Usage Type locally. *usage_type_value* must be an integer from 0 to 255.

Usage Guidelines

Use this command to locally configure the UE Usage Type for UEs that complies with the Call Control Profile match criteria.

Example

The following command configures the UE usage type with value set to *100*:

```
decor ue-usage-type 100
```

description

Allows you to enter a relevant descriptive string.

Product

MME

SAEGW

S-GW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

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

description

Enter an alphanumeric string of 1 to 100 characters. The string may include spaces, punctuation, and case-sensitive letters if the string is enclosed in double quotation marks (").

no

Removes the description from the call control profile.

Usage Guidelines

Define information that identifies this particularly call control profile.

Example

`description "call-control-profile handling incoming from CallTell"`

diameter-result-code-mapping

Maps an EMM (EPS Mobility Management) NAS (Network Access Server) cause code to a Diameter result code.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

diameter-result-code-mapping s6a *diameter_result_code* **mme-emm-cause** *mme_emm_error_code*
remove diameter-result-code-mapping s6a *diameter_result_code*

remove diameter-result-code-mapping s6a *diameter_result_code*

Removes the mapping for the specified Diameter result code.

s6a *diameter_result_code*

Specifies the Diameter result code to which the EMM NAS cause code is mapped.

diameter_result_code: Specify one of the supported Diameter result codes:

- **diameter-authorization-rejected** - s6a result code 5003. Default mapped EMM code: "No suitable cells in tracking area."
- **diameter-error-other** - miscellaneous s6a error result code. Default mapped EMM code: "Network failure."
- **diameter-error-rat-not-allowed** - s6a result code 5421. Default mapped EMM code: "No suitable cells in tracking area."
- **diameter-error-roaming-not-allowed** - s6a result code 5004. Default mapped EMM code: "PLMN not allowed."
- **diameter-error-user-unknown** - s6a result code 5001/5030. Default mapped EMM code: "EPS Service and non-EPS services not allowed."
- **diameter-invalid-avp-value** - s6a result code 5004. Default mapped EMM code: "Network failure."
- **diameter-unable-to-comply** - s6a result code 5012. Default mapped EMM code: "Network failure."
- **diameter-unknown-eps-subscription** - s6a result code 5420. Default mapped EMM code: "No suitable cells in tracking area."
- **diameter-unsupported-feature** - s6a result code 5011. Default mapped EMM code: "Network failure."

mme-emm-cause *mme_emm_error_code*

Specifies the EMM NAS cause code to be mapped to the Diameter result code.

mme_emm_error_code: Specify one of the supported EMM NAS error codes:

- **eps-non-eps-not-allowed**: Specifies that the EMM NAS cause code #8 "EPS services and non-EPS services not allowed" is to be mapped to the specified Diameter result code.
- **network-failure**: Specifies that the EMM NAS cause code #17 "Network failure" is to be mapped to the specified Diameter result code.
- **no-suitable-cell-in-tracking-area**: Specifies that the EMM NAS cause code #15 "No suitable cells in tracking area" is to be mapped to the specified Diameter result code.
- **plmn-not-allowed**: Specifies that the EMM NAS cause code #11 "PLMN not allowed" is to be mapped to the specified Diameter result code.
- **roaming-not-allowed-in-this-tracking-area**: Specifies that the EMM NAS cause code #13 "Roaming not allowed in this tracking area" is to be mapped to the specified Diameter result code.

- **severe-network-failure**: Specifies that the EMM NAS cause code #42 "Severe network failure" is to be mapped to the specified Diameter result code.
- **tracking-area-not-allowed**: Specifies that the EMM NAS cause code #12 "Tracking area not allowed" is to be mapped to the specified Diameter result code.

Usage Guidelines Use this command to map a selected EMM NAS cause code to a specific Diameter result code.

Example

The following command maps the EMM NAS cause code "Roaming not allowed in this tracking area" to the Diameter result code "S6a Diameter error RAT not allowed":

```
diameter-result-code-mapping s6a diameter-error-rat-not-allowed
mme-emm-cause roaming-not-allowed-in-this-tracking-area
```

direct-tunnel

Enables setup of a direct tunnel if direct tunneling is supported by the destination node.



Important Direct tunneling must be enabled at both of these two points to allow direct tunneling for the MS/UE.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

```
direct-tunnel attempt-when-permitted [ to-ggsn | to-sgw ]

remove direct-tunnel [ to-ggsn | to-sgw ]
```

remove

Removes the configured setting from the call control profile. An existing configuration to enable direct tunneling must be removed before creating a new direct tunnel enabling configuration.

attempt-when-permitted

Enables direct tunneling if the destination node allows it. Default: disabled.

[to-ggsn | to-sgw]

Beginning with Release 19.3.5, including one of these keyword filters allows the operator to select the interface for the direct tunnel.

- **to-ggsn** enables only the GTP-U interface between the RNC and the GGSN for the direct tunnel.
- **to-sgw** enables only the S4's S12 interface between the RNC and the SGW for the direct tunnel.

Usage Guidelines

By default, the direct tunnel feature is not enabled. Use this command to enable the direct tunnel feature.

To ensure that direct tunnel is fully configured for support by the SGSN, check the settings for **direct-tunnel** in

- the APN profile -- from the Exec mode, use command: **show apn-profile** <*profile_name*> **all**
- the RNC (radio network controller) configuration -- from the Exec mode, use command: **iups-service** <*service_name*> **all**

There are three optional configurations:

1. **attempt-when-permitted** enables both the GTP-U interface towards the GGSN and the S12 interface towards the SGW.
2. **attempt-when-permitted to-ggsn** enables only the GTP-U interface towards the GGSN.
3. **attempt-when-permitted to-sgw** enables only the S12 interface towards the SGW.



Important All three forms of the CLI function independently. This means that the configuration created with one command (for example: **direct-tunnel attempt-when-permitted to-ggsn** is not overwritten by the entry of one of the other commands (for example: **direct-tunnel attempt-when-permitted**). The existing configuration must be removed to disable the configuration and then the next configuration must be added.

Example

The following command sets the configuration to instruct the SGSN to attempt to setup a direct tunnel if permitted at the destination node:

```
direct-tunnel attempt-when-permitted
```

The following command allows the operator to select the direct tunnel interface and sets the configuration to instruct the S4-SGSN to attempt to setup a direct tunnel using an S12 interface to the destination SGW if the SGW permits direct tunnels:

```
direct-tunnel attempt-when-permitted to-sgw
```

dns-ggsn

Defines the context to be used to do DNS lookup for GGSNs.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

dns-ggsn context *ctxt_name*
no dns-ggsn context *ctxt_name*

no

Removes the dns-ggsn configuration from this call control profile.

context *ctxt_name*

Specifies the context to be used to do DNS lookup for GGSNs as an alphanumeric string of 1 through 64 characters.

Usage Guidelines

Use this command to define the context to be used to do DNS lookup to find the GGSN address.

Example

dns-ggsn context sgsn1

dns-mrme

This command is used to configure the DNS client context and DNS query type used for the PGW/GGSN resolution for MRME.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

dns-mrme { context *context_name* **[query-type { a-aaa | snaptr }] | query-type { a-aaa | snaptr } }**
no dns-mrme context
default dns-mrme query-type

no

Removes the dns-mrme configuration from this call control profile.

default

Sets the default value for the query-type and context will not be modified.

Default (SaMOG 3G license): a-aaa

Default (SaMOG Mixed Mode license): snaptr

Important The **default dns-mrme query-type** command is available only when the SaMOG Mixed Mode license (supporting both 3G and 4G) is configured.

context_name

Specifies the DNS client context to be used for DNS lookup. *context_name* must be an alphanumeric string of 1 through 79 characters.

query-type { a-aaa | snaptr }

Specifies the the type of DNS query used for the PGW/GGSN resolution for MRME.

a-aaa: Specifies to use A-AAA queries using pre-release 8 DNS procedures.

snaptr: Specifies to use SNAPTR queries using post-release 7 DNS procedures. This is the default value when SaMOG Mixed Mode license is configured.

Important This keyword is available only when the SaMOG Mixed Mode license (supporting both 3G and 4G) is configured. However, when an SaMOG 3G license is configured, the query type for the DNS query is set to use A-AAA queries using pre-release 8 DNS procedures.

Usage Guidelines Use this command to configure the DNS client context and DNS query type used for the PGW/GGSN resolution for MRME. The DNS context configuration is used to provide the context name where the DNS client for this AAA server is configured. The default dns-context is configured under the MRME Service Configuration Mode. If no DNS context is configured under the MRME Service Configuration Mode, the DNS context will be used as the context for the MRME service.

Example

```
dns-mrme context mrme1 query-type snaptr
```

dns-msc

Defines the context to be used to do DNS lookup for Mobile Switching Centers (MSCs).

Product MME

Privilege Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

dns-msc context *ctxt_name*
remove dns-msc

remove

Deletes this definition from the call control profile.

context *ctxt_name*

Specifies the context to be used to do DNS lookup for MSCs as an alphanumeric string of 1 through 64 characters.

This specifies the name of the context where the DNS client is configured that will be used for DNS resolution of MSCs for Single Radio Voice Call Continuity (SRVCC).

Usage Guidelines

This feature requires that a valid SRVCC license key be installed.

Use this command to configure the context ID for the DNS lookup.

MSC selection using DNS takes precedence over locally configured MSCs. If DNS lookup fails, the MME will select the MSC from local configuration.

DNS based MSC selection can be defined for an MME service, or for a Call Control Profile. Both configuration options specify the context in which a DNS client configuration has been defined. Configuration via Call Control Profile takes precedence in cases where DNS selection is also configured in the MME service

Example

The following command associates a pre-configured context *dns_ctx1* where a DNS client service is configured for DNS query to MSC for this Call Control Profile.

dns-msc context dns_ctx1

dns-sgsn

Identifies the context to be used to do DNS to find an SGSN address.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

[no] dns-sgsn context *ctxt_name*

no

Removes the dns-sgsn configuration from this call control profile.

context *ctxt_name*

Identify the context where the DNS client is configured to send the DNS query to get the peer SGSN address.

context_name: Enter a string of 1 to 79 alphanumeric characters to identify the context.

This configuration would override any similar configuration for **dns-sgsn context** in the SGTP service configuration.

Usage Guidelines

Use this command to configure the context ID for the SGSN address that will be used to do the DNS lookup.

Example

Configure context *sgsn1* for DNS lookup:

```
dns-sgsn context sgsn1
```

dns-pgw

Defines the context to be used to do DNS lookup for P-GWs.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

[remove] dns-pgw context *ctxt_name*

remove

Deletes this definition from the call control profile.

context *ctxt_name*

Specifies the context to be used to do DNS lookup for P-GWs as an alphanumeric string of 1 through 64 characters.

On the S4-SGSN, if the interface selected for a UE is S4 and if there is no DNS-PGW context configured under a call control profile, then by default the system will look for the DNS client in the context where the eGTP service is defined. If the interface selected for a UE is Gn-Gp and if there is no **dns-pgw context** configured in a call control profile, then by default the S4-SGSN will look for the DNS client in the context where the SGTP service is configured for selecting a co-located PGW/GGSN if:

- the UE is EPC capable and,
- **apn-resolve-dns-query snaptr** is configured in an APN profile using *APN Profile Configuration Mode*.

If the **dns-pgw context** is deleted with the **remove** option, the S4-SGSN chooses the DNS client from the context where the eGTP service is configured.

Usage Guidelines Use this command to configure the context ID for the DNS lookup.

Important It is recommended to execute the S4 SGSN configuration commands during the maintenance window. After configuring the node, re-start the node to activate the configuration commands. This will ensure that the node is in a consistent state and S4 SGSN service instability scenarios are avoided.

Example

```
dns-pgw context pgw1
```

dns-sgw

Defines the context to be used to do DNS lookup for S-GWs.

Product MME

SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description **`[ remove ] dns-sgw context`** *`ctxt_name`*

remove

Deletes this definition from the call control profile.

context *ctxt_name*

Specifies the context to be used to do DNS lookup for S-GWs as an alphanumeric string of 1 through 64 characters.

This command must be used to configure DNS client settings when using dynamic S-GW selection where the tai-mgmt-db has been associated with a call-control-profile.

On the S4-SGSN, this specifies the name of the context where the DNS client is configured that will be used for DNS resolution of S-GWs. If **dns-sgw context** is not specified, the S4-SGSN uses the DNS client configured in the context where the eGTP service is configured to query the S-GW DNS address.

Usage Guidelines

Use this command to configure the context ID for the DNS lookup.



Important

It is recommended to execute the S4 SGSN configuration commands during the maintenance window. After configuring the node, re-start the node to activate the configuration commands. This will ensure that the node is in a consistent state and S4 SGSN service instability scenarios are avoided.

Example

```
dns-sgw context sgw1
```

ecn

This command enables explicit congestion notification (ECN) in normal mode or compatible mode for the GTP tunnel over S2b interface.

Product

ePDG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
ecn gtp mode normal
remove ecn gtp mode
```

ecn

Specifies ECN over GTP tunnel in normal mode.

gtp

Enables ECN handling over GTP tunnel.

mode

Specifies the tunnel ingress encapsulation mode.

normal

Specifies the normal mode of encapsulation.

remove

Enables ECN in compatible mode for GTP tunnel over the S2b interface. The default mode is the compatible mode, supported for backward compatibility.

Usage Guidelines

Use this command to enable ECN in normal mode or compatible mode for the GTP tunnel over S2b interface.

Example

The following command enables ECN in normal mode for the GTP tunnel:

```
ecn gtp mode normal
```

edrx

This command enables Extended Discontinuous Reception (eDRX) and configures its respective parameters, on the MME.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax

```
edrx { ptw ptw_value edrx-cycle cycle_length_value | ue-requested } [
dl-buf-duration [ packet-count packet_count_value ] ]
remove edrx
```

remove

The keyword **remove**disables the eDRX configuration on the MME.

ptw *ptw_value*

This keyword is used to configure the PTW value.

In releases prior to 21.2: The *ptw_value* is an integer ranging from "0" up to "20".

In 21.2 and later releases: The *ptw_value* is an integer ranging from "0" up to "15".

ue-requested

The keyword **ue-requested**specifies the UE requested values of the Paging Time Window (PTW) and the eDRX cycle length received from the UE in the Attach Request/TAU Request message be accepted.

edrx-cycle *cycle_length_value*

The keyword **edrx-cycle**is used to configure the eDRX cycle length. The *cycle_length_value* is an integer value from " 512" up to "262144". It is a multiple of 2 starting from 512 up to 262144 (for example: 512, 1024, 2048, and so on).

dl-buf-duration

The keyword **dl-buf-duration** is used to send downlink buffer duration in DDN ACK when unable to page UE.

packet-count*packet_count_value*

The keyword **packet-count** is used to send 'DL Buffering Suggested Packet Count' in DDN ACK when unable to page UE. The *packet_count_value* is an integer value from "0" up to "65535". If the *packet_count_value* is not configured locally, the subscription provided value for the *packet_count_value* is used. The subscription value can be "0" in which case packet count IE will not be sent for that subscriber even if it is configured locally.

Usage Guidelines

Use this command to enable eDRX on the MME. This command is configured as part of the eDRX feature for MME - it allows UEs to connect to the network on a need basis. With eDRX, a device can remain inactive or in sleep mode for minutes, hours or even days based on the H-SFN synchronization time (UTC Time). The H-SFN synchronization time for eDRX is configured at an MME-Service level. See *MME Service Configuration Mode Commands* chapter for configuration information on H-SFN synchronization. This command is not enabled by default.

Example

The following command is used to configure the PTW and eDRX cycle length. The command is also used to send the downlink buffer duration in the DDN ACK along with a suggested packet count:

```
edrx ptw 10 edrx-cycle 512 dl-buf-duration packet-count 10
```

egtp

Configures the type of PLMN sent in either the user location information (ULI) IE or the Serving Network IE.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
egtp network-sharing-plmn { serving-network { use-common-plmn |
use-selected-plmn | use-ue-plmn } | uli { use-common-plmn |
use-selected-plmn | use-ue-plmn } }
remove egtp network-sharing-plmn { serving-network | uli }
```

remove

Erases the IE choice from the call control profile configuration.

use-common-plmn

Instructs the SGSN to identify the Common PLMN for the shared network.

use-selected-plmn

Instructs the SGSN to identify the Selected PLMN for the shared network.

use-ue-plmn

Instructs the SGSN to identify the UE selected PLMN that is available in the shared network.

Usage Guidelines

The SGSN supports location change reporting on the S4 interface, when requested by the P-GW, using a ULI IE in GTPv2 messages. When the network sharing feature is enabled the operator can determine which PLMN to send to the P-GWin the ULI IE and Serving Network IE. The command can be issued multiple times to configure the PLMN type for each IE.

The selections made for this configuration must match those configured for the call control profile's GTP configuration.

This command can only be used if network sharing is enabled and the appropriate "Location-reporting in connected-mode" feature license is installed. For details, check with your Cisco Representative.

Example

Configure the ue-plmn type PLMN to be sent in the Serving Network IE:

```
egtp network-sharing-plmn serving-network ue-plmn
```

eir-profile

Identifies and associates an EIR profile to be used by the SGSN for EIR selection.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

`[ no ] eir-profile` *`profile_name`*

no

Disassociates the EIR profile with the call control profile.

Usage Guidelines

The equipment identify register (EIR) profile contains all the parameters needed to identify and work with an EIR to perform check IMEI procedures and to address multiple EIR through a single EIR address. The configuration in the EIR profile associated with the call control profile take precedence over the EIR parameters configured in the MAP service.

Example

Associate the EIR profile called *LondonEIR1*:

```
eir-profile LondonEIR1
```

encryption-algorithm-lte

Defines the priorities for using the encryption algorithms.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

```
encryption-algorithm-lte priority1 { 128-eea0 | 128-eea1 | 128-eea2 |
128-eea3 } [ priority2 { 128-eea0 | 128-eea1 | 128-eea2 | 128-eea3 } ] [
 priority3 { 128-eea0 | 128-eea1 | 128-eea2 | 128-eea3 } ] [ priority4 {
 128-eea0 | 128-eea1 | 128-eea2 | 128-eea3 } ]
remove encryption-algorithm-lte
```

remove

Deletes the priorities definition from the call control profile configuration.

priority1

Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 1.

priority2

Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 2.

priority3

Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 3.

priority4

Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 4.

128-eea0

Sets the Null ciphering algorithm (128-EEA0) for LTE encryption as the encryption algorithm for security procedures.

Default: priority1

128-eea1

Sets the SNOW 3G synchronous stream ciphering algorithm (128-EEA1) for LTE encryption as the encryption algorithm for security procedures. SNOW 3G is a stream cipher that forms the base of the 3GPP confidentiality algorithm UEA2 and the 3GPP integrity algorithm UIA2.

Default: priority2

128-eea2

Sets the Advance Encryption Standard (AES) ciphering algorithm (128-EEA2) for LTE encryption as the encryption algorithm for security procedures.

Default: priority3

128-eea3

Sets the ZUC algorithm (128-EEA3) for LTE encryption as the encryption algorithm for security procedures.

Default: priority4

Usage Guidelines

Set the order or priority in which the MME will select an encryption algorithm for use. All three priorities must be set or the definition is invalid. The command can be re-entered to change the priorities without removing the configuration.

Example

The following command sets the 128-EEA2 as the LTE encryption algorithm with priority 3 for security procedures with the call control profile:

```
encryption-algorithm-lte priority1 128-eea2 priority3
```

encryption-algorithm-umts

Defines the priorities for using the encryption algorithms.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description **`encryption-algorithm-umts { uea0 | uea1 | uea2 } [ then-uea# | then-uea# ]`**
`no encryption-algorithm-lte`

no

Deletes the priorities definition from the call control profile configuration.

{ *uea0* | *uea1* | *uea2* }

Enter one of the three options to define the first priority algorithm.

[then-uea# | then-uea#]

If a second algorithm is to be included as an option, give it second priority. Enter 0, 1, or 2 at the end of **then-uea** to define the algorithm being given second priority.

then-uea#

If a third algorithm is to be included as an option, give it third priority. Enter 0, 1, or 2 at the end of **then-uea** to define the algorithm being given third priority.

Usage Guidelines Set the order or priority in which the SGSN will select a UEA algorithm for use. It is not necessary to define priorities for all three priority levels. The command can be re-entered to change the priorities without removing the configuration.

Example

Configure algorithm UEA2 as the first priority encryption algorithm with no others to be considered:

`encryption-algorithm-umts uea2`

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.

epdg-s2b-gtpv2

Configures S2b GTPv2 IE Options.

Product ePDG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description **`[ remove ] epdg-s2b-gtpv2 send 5g-uli { aaa-server-id | message { mbr trigger mobike } | serving-network { value uli } | ue-local-ip-port | uli | wlan-location-info-timestamp }`**

remove

Using the "remove" keyword will remove the configuration and restore the default behavior. By default the inclusion of the AVPs in the Create Session Request Message will be disabled.

send

Configure the IE or message options in send direction.

5g-uli

Enables 5G cell ID feature under the call control profile and sends custom 5g-uli IE.

aaa-server-id

This is used to send AAA origin-host and origin-realm in Node Identifier IE.

message

This is used to configure the message options to be sent.

serving-network

This is used to send serving-network IE.

ue-local-ip-port

This is used to send UE Local IP IE and UE UDP Port IE.

uli

This is used to send uli IE.

wlan-location-info-timestamp

This is used to send UE Wlan Location Information and Timestamp IE.

epdg-s2b-gtpv2 send 5g-uli

Enables sending of 5G ULI on the s2b interface.



Note ULI for 5G is sent only when ePDG decides to latch the call on SMF+PGW-C. Selection of PGW/SMF+PGW-C is enabled through the 5GIWK feature, which is a licensed feature.

remove epdg-s2b-gtpv2 send 5g-uli

Disables sending of 5G ULI on the s2b interface.



Note If the ePDG receives a 4G TAI and/or ECGI, and if the epdg-s2b-gtpv2 send uli has been configured, the ePDG will include the ULI values in the CSReq message, irrespective of whether P-GW or SMF+PGW-C is chosen.

Usage Guidelines Use this command to Enable/Disable the inclusion of the "UE Local IP Address" and "UE UDP Port" AVPs in the GTPv2 Create Session Request message from ePDG to PGW.

Example

Use the following command to include "UE Local IP Address" and UE UDP Port" AVPs in the GTPv2 Create Session Request message from ePDG to PGW.

```
epdg-s2b-gtpv2 send ue-local-ip-port
```

Use the following command to disable 5g cell ID feature under the call control profile.

```
[ remove ] epdg-s2b-gtpv2 send 5g-uli
```

epdg-swm

Configures Swm Message Options for ePDG.

Product ePDG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

```
epdg-swm send message aar trigger location-retrieval epdg-swm receive
nci-spare-nibble-trail
```

```
[ remove ] epdg-swm send message aar [ trigger ] [ receive ]
nci-spare-nibble-trail
```

remove

Using the "remove" keyword will remove the configuration and restore the default behavior.

send

Configure the IE or message options in send direction.

message

This is used to configure the message options to be sent.

aar

Authorisation and Authentication Request.

trigger

This is used to set trigger on which message shall be sent.

location-retrieval

Sets Trigger as location-retrieval.

[receive] nci-spare-nibble-trail

receive: Configures the AVP or message options in the receive direction.

nci-spare-nibble-trail: Enables the trailing spare nibble format of NCI. By default, NCI is with leading spare nibble

Usage Guidelines

Use this command to Swm Message Options for ePDG.

Example

Use the following command to configure Swm Message Options like sending a message with authorisation and authentication request setting trigger as location retrieval .

```
epdg-swm send message aar trigger location-retrieval
```

equivalent-plmn

Configures the definition for an equivalent public land mobile network identifier (PLMN ID) and the preferred radio access technology (RAT). This is a of PLMNs which should be considered by the mobile as equivalent to the visited PLMN for cell reselection and network selection. When configured, the equivalent PLMN list

will be sent to the UE in NAS ATTACH ACCEPT / TAU ACCEPT messages (up to 15 PLMNs in each message).

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

equivalent-plmn radio-access-technology { 2G | 3g | 4g | any } plmnid mcc *mcc_number* **mnc** *mnc_number* **priority** *priority*
no equivalent-plmn radio-access-technology { 2G | 3g | any } plmnid mcc*mcc_number* **mnc** *mnc_number*

no

Removes the equivalent-PLMN configuration from this call control profile.

radio-access-technology { 2G | 3g | 4g | any }

Identify the RAT type of the equivalent PLMN:

- **2G**: 2nd generation
- **3G**: 3rd generation
- **4G**: 4th generation
- **any**: Any RAT

plmnid mcc *mcc_number* mnc *mnc_number*

- **mcc**: Specifies the mobile country code (MCC) portion of the PLMN ID. The number can be any integer between 100 and 999.
- **mnc**: Specifies the mobile network code (MNC) portion of the PLMN ID. The number can be any 2- or 3-digit integer between 00 and 999.

priority *priority*

Enter an integer between 1 and 15 with the highest priority assigned to the integer of the lowest numeric value.

Usage Guidelines

Use the command to identify an 'equivalent PLMN' and assign it a priority to define the preferred equivalent PLMN to be used. This command can be entered multiple times to set priorities of usage.

Example

The following command sets up a secondary equivalent PLMN definition that allows for any RAT with a PLMN ID of MCC121.MNC767:

```
equivalent-plmn radio_access_technology any plmnid mcc 121 mnc 767 priority
 2
```

esm t3396-timeout

This command is used to configure the ESM T3396 timer to be sent to UE in ESM reject messages.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

esm t3396-timeout *timeout_value* **cause** *cause_code_value*
remove esm t3396-timeout cause *cause_code_value*

remove

Removes the T3396 timeout configuration for the specified cause code from Call Control profile. The T3396 timeout will then be applied from the MME-service.

t3396-timeout *timeout_value*

Configures the value for ESM backoff timer (in seconds) to be sent to UE for ESM reject cause 'insufficient resources' and 'missing or unknown apn'. This value overrides the MME-service level configuration.

The *timeout_value* is an integer from 0 to 1116000.

cause *cause_code_value*

Configures the cause code value as an integer that is either 26 or 27. If the configured value is present in the ESM reject messages, the T3396 back-off timer will be included.

- The following cause values are supported:
  - 26 - Insufficient resources
  - 27 - Missing or Unknown APN
- Only one cause value can be configured with the **cause** keyword. Multiple cause values cannot be configured.

Usage Guidelines This command configures the ESM T3396 timer to be sent to UE in ESM reject messages. There is no specified default value for T3396 timeout for a given cause code.

- To configure the T3396 timeout for different cause codes, the configuration must be done in multiple lines. For example:

```
esm t3396-timeout 1100 cause 26
esm t3396-timeout 1500 cause 27
```

- The new configuration for T3396 timeout for a given cause code will override the previous configuration. For example:

```
esm t3396-timeout 1500 cause 26
esm t3396-timeout 1800 cause 26
```

  The final T3396 timeout that will be applied for cause code 26 is 1800 seconds.

Example

The following command sets the ESM T3396 timeout value as *1860* seconds for cause code value *26*:

```
esm t3396-timeout 1860 cause 26
```

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.

gbr-bearer-preservation-timer

Configures the system to preserve GBR bearers for a configurable timer value.

Product MME

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

gbr-bearer-preservation-timer *timer_value*
remove gbr-bearer-preservation-timer

remove

Disables the timer configuration.

gbr-bearer-preservation-timer

The above command allows the operator to set the preservation time for the Bearer on receiving the UE Context Release with the Radio Connection With UE Lost cause code.

timer_value

Specifies the duration for preserving the bearers in seconds. *timer_value* must be an integer from 1 to 600.

Usage Guidelines

MME provides a configurable timer. Operators can configure a timer value for which the GBR bearers are preserved when the subscriber is out of coverage during a VoLTE call.

Example

The following command preserves the GBR bearers for 300 seconds.

gbr-bearer-preservation-timer 300

gmm Extended-T3312-timeout

This command enables the operator to determine how the SGSN handles Extended T3312 timer values at the Call-Control Profile level.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

gmm Extended-T3312-timeout { value *exT3312_minutes* **| when-subscribed } [low-priority-ind-ue]**
no gmm Extended-T3312-timeout

no

This command filter instructs the SGSN to remove the Extended T3312 configuration from the Call-Control Profile configuration.

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 (insert subscriber data) 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".

Usage Guidelines

An **Extended-T3312-timeout** configuration in the Call-Control Profile will override an **Extended-T3312-timeout** configuration done for either the GPRS or SGSN services. As well, a Call-Control Profile configuration enables the operator to finetune for Homers and Roamers.

Example

Use a command similar to the following to instruct the SGSN to only send the Extended T3312 value when the Attach/RAU Request includes a LAPI and when the received "MS Network Feature Support" information indicates the the user is subscribed for this timer:

```
gmm Extended-T3312-timeout when-subscribed low-priority-ind-ue
```

Use the following command to remove the Extended T3312 timer configuration from the Call-Control Profile.

```
no gmm Extended-T3312-timeout
```

gmm information-in-messages

Provides the configuration to include the information in messages for the GPRS mobility management (GMM) parameters.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
gmm information-in-messages access-type { { gprs | umts } [ network-name
 { full-text name | short-text name } | [ send-after { attach | rau } ] }
[ default | no ] gmm { information-in-messages access-type { gprs | umts
 }
```

no

Disables the GMM configuration from this call control profile.

default

Sets up a GMM configuration with system default values.

access-type

Must select one of the following options:

- **gprs** - General Packet Radio Service network
- **umts** - Universal Mobile Telecommunications System network

After selecting the access-type, an additional parameter can be configured:

- **network-name**: identifies the network name in either short text or full text.
- **send-after**: configures the information in message to send after attachment or Routing Area Update (RAU).

network-name { full-text *name* | short-text *name* }

This keyword provides the option to add the network name to the message. The network name will in full text or short text. Possible options are:

- full-text *name*: Indicate the network name in full text
- short-text *name*: Indicate the network name in short text

send-after { attach | rau }

This keyword configures the information in message to send after attachment or RAU message. Possible options are:

- **attach**: Information sent after attachment
- **rau**: Information sent after routing area update

Usage Guidelines

Use this command to configure identifying information about the network that will be included in GMM messages.

Example

Set default settings for calls coming from 2.5G networks:

```
default gmm information-in-messages access-type gprs
```

gmm rau-accept

Provides the configuration to set the Follow-On Proceed (FOP) bit in the Routing Area Update Accept (RAU) message.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

```
gmm rau-accept follow-on-proceed { on-following-nw-procedure |
only-on-ue-request }
remove gmm rau-accept follow-on-proceed
```

remove

Disables the SGSN from sending the Follow On Proceed bit in the RAU response.

follow-on-proceed

This keyword configures the SGSN to send FOP bit in RAU Accept message.

on-following-nw-procedure

This keyword configures the SGSN to send FOP bit when there is a following Network Procedure.

only-on-ue-request

This keyword configures the SGSN to send FOP bit only when UE requests for it.

Usage Guidelines

Use this command to configure the setting of Follow On Proceed bit in Routing Area Accept Message. The FOP bit can be set only when the UE requests for it by configuring the command option **only-on-ue-request** or the FOP bit can be set when there is a following network procedure by configuring the CLI option **on-following-nw-procedure**. By default, the configuration is **gmm rau-accept follow-on-proceed only-on-ue-request**.

Example

Use this command to configure the SGSN to send the Follow On Proceed bit when there is a following Network Initiated Procedure.

```
gmm rau-accept follow-on-proceed on-following-nw-procedure
```

gmm retrieve-equipment-identity

Configures the International Mobile Equipment Identity (IMEI) or software version (SV) retrieval and validation procedure.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`gmm retrieve-equipment-identity { imei | imeisv [ unciphered ] [ then-imei ] } [ verify-equipment-identity [ deny-greylisted ] [ allow-unknown ] ] [ no | default ] gmm retrieve-equipment-identity`

no

Disables the equipment identity retrieval procedure configured for this call control profile.

default

Sets the default action for equipment identity retrieval (EIR) procedure:

- **retrieve-equipment-identity**: Default action is disabled - no retrieval of IMEI/IMEI-SV
- **verify-equipment-identity**: Default action is disabled - no verification with Equipment Identity Register (EIR)

equipment-identity-type

Default: disabled

Indicates the type of equipment identification, with the possible values:

- **imei**: International Mobile Equipment Identity
- **imeisv**: International Mobile Equipment Identity - Software Version

imei

Indicates the equipment identity retrieval type to International Mobile Equipment Identity (IMEI). IMEI is a unique 15-digit number consisting of a TAC (Technical Approval Code), a FAC (Final Assembly Code), an SNR (Serial Number), and a check digit.

imeisv [unciphered] [then-imei]

Indicates the equipment identity retrieval type to IMEI with software version (SV). IMEI with SV is a unique 16-digit number consisting of a TAC (Technical Approval Code), a FAC (Final Assembly Code), an SNR (Serial Number), and a 2-digit software version number.

- **unciphered**: This optional keyword enables the unciphered retrieval of IMEI-SV. If this option is enabled the retrieval procedure will get IMEISV (if auth is still pending, get as part of Authentication and Ciphering Response otherwise, via explicit Identification Request after Security Mode Complete).
- **then-imei**: This optional keyword enables the retrieval of software version number before the IMEI. If this option is enabled the equipment identity retrieval procedure will get IMEISV on secured link (after Security mode procedure via explicit GMM Identification Request), and if MS is not having IMEISV (responded with NO Identity), SGSN will try to get IMEI.

If no other keyword is provided, imeisv will get IMEISV on a secured link (after a Security mode procedure via explicit GMM Identification Request).

verify-equipment-identity [deny-greylisted] [allow-unknown]

Default: disabled

This keyword enables the equipment identity validation and validates the equipment identity against the EIR.

- **deny-greylisted**: This keyword fine-tunes the configuration and enables the restriction to the user having mobile equipment with an IMEI in the EIR grey list.
- **allow-unknown**: If this keyword is configured and EIR sends equipment status as "UNKNOWN EQUIPMENT" then the call will be allowed to continue in SGSN.

Usage Guidelines

Use this command to enable and configure the procedures for mobile equipment identity retrieval and validation from the EIR identified in the MAP Service Configuration mode.

Example

The following command enables the SGSN to send "check IMEI" messages to the EIR:

```
gmm retrieve-equipment-identity imei verify-equipment-identity
```

gmm t3346

The **gmm** command includes a new keyword to set the MM T3346 back-off timer for a Call-Control Profile.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

gmm t3346 min *minimum_minutes* **max** *maximum_minutes*
no gmm t3346

no

Including this filter with the command removes the MM back-off timer definition from the Call-Control Profile configuration.

min *minimum_minutes*

Enter an integer from 1 to 15 to identify the minimum number of minutes the timer should run; default is 15 minutes.

max *maximum_minutes*

Enter an integer from 1 to 30 to identify the maximum number of minutes the timer should run; default is 30 minutes.

Usage Guidelines

- Under congestion, the SGSN can assign the T3346 back-off timers to the UEs and request the UEs not to access the network for a given (timer value) period of time.
- 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.
- If T3346 timer value is configured in a Call-Control Profile then it will override the back-off timer values defined for either the SGSN Service or GPRS Service configurations.
- The timer will be ignored if an Attach Request or RAU Request is received after congestion has cleared.

Example

Use a command similar to the following to define a T3346 with a timeout range of *2 to 15* minutes.

```
gmm t3346 min 2 max 15
```

gs-service

Associates the context of a Gs service interface with this call control profile.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

gs-service *gs_srvc_name* **context** *ctx_name*
no gs-service *svc_name*

no

Removes/disassociates the named Gs service from the call control profile.

gs-service *gs_srvc_name*

Specifies the name of a specific Gs service for which to display information. *gs_srvc_name* is the name of a configured Gs service expressed as an alphanumeric string of 1 through 63 characters that is case sensitive.

context *ctx_name*

Specifies the specific context name where Gs service is configured. If this keyword is omitted, the named Gs service must exist in the same context as the GPRS/SGSN service.

ctx_name is name of the configured context of Gs service expressed as an alphanumeric string from 1 through 63 characters that is case sensitive.

Usage Guidelines

Use this command to associate a specific Gs service interface with this GPRS service instance.

Important A Gs service can be used with multiple SGSN and/or GPRS service.

Example

The following command associates a Gs service instance named *stargs1*, which is configured in context named *star_ctx*, with a call control profile:

```
gs-service stargs1 context star_ctx
```

gtp send

Configures which information elements (IE) the SGSN sends in GTP messages. These are required by the GGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
gtp send { imeisv [ derive-imeisv-from-imei ] | ms-timezone | rai [
use-local-plmn [ network-sharing { use-selected-plmn | use-ue-plmn |
use-common-plmn } ] ] | rat | uli [ use-local-plmn [ network-sharing {
use-selected-plmn | use-ue-plmn | use-common-plmn } ] ] }
```

```
remove gtp send { imeisv | ms-timezone | rai | rat | uli }
no gtp send
```

remove

Removes the specified GTP send definition from the system configuration.

no

Disables the specified GTP send configuration.

imeisv

Instructs the SGSN to include the IMEISV (International Mobile Equipment Identity with Software Version) of the mobile when sending GTP messages of the type Create PDP Context Request.

By default, this function is disabled.

derive-imeisv-from-imei

This is a filter for the **imeisv** keyword. It allows the operator to configure the SGSN to send IMEI to the GGSN as IMEI-SV.

This filter instructs the SGSN to add four 1s (1111) to the final semi-octet of the CPCQ (Create PDP Context Request) message which enables the SGSN to deduce the IMEI-SV value from the IMEI. If this filter is used, then IMEI is also sent as IMEI-SV when the **gmm retrieve-equipment-identity** command is configured.

ms-timezone

Instructs the SGSN to include this IE in GTP messages of the type Create PDP Request and Update PDP Context Request. This IE specifies the offset between universal time and local time, where the MS currently resides, in 15-minute steps.

This IE is sent by default.

rai

Configures the SGSN to include the Routing Area Identity (RAI) of the SGSN in the following situations:

- 2G new SGSN RAU
- 3G new SGSN SRNS
- 2G -> 3G HO (only if PLMN Id has changed)
- 3G -> 2G HO (only if PLMN Id has changed)
- multiple IUPS service RAU (only if PLMN Id has changed)
- multiple GPRS service RAU (only if PLMN Id has changed)
- 3G new SGSN RAU (change in behavior)
- 3G primary and secondary PDP activation (change in behavior)
- 2G primary and secondary PDP activation (change in behavior)

Optionally, this keyword can be followed with the keyword selection for the PLMN - **use-local-plmn**.

rat

Specifies which radio access technology (RAT) is being used by the MS (GERAN, UTRAN, or GAN). Including this keyword instructs the SGSN to include this IE when sending GTP messages of the type Create PDP Request and Update PDP Context Request.

This IE is sent by default.

uli

Specifies the CGI (MCC, MNC, etc.) and SAI of the MS where it is registered. Including this keyword instructs the SGSN to include the IE when sending GTP messages of the type Create PDP Request and Update PDP Context Request.

This IE is not sent by default.

Optionally, this keyword can be followed with the keyword selection for the PLMN - **use-local-plmn**.



Important Currently, the next 5 (five) keywords, are only used with parameters **rai** or **uli**.

use-local-plmn

This keyword selects the local PLMN when network is not shared.

network-sharing

This keyword is used to configure network-sharing.

use-selected-plmn

This keyword selects the Selected PLMN when network is shared.

use-ue-plmn

This keyword selects Selected PLMN for supporting UE and Common PLMN for non-supporting UE when network is shared.

use-common-plmn

This keyword selects the Common PLMN when network is shared.

Usage Guidelines

Use this command to define a preferred set of information to include when GTP messages are sent. Repeat this command multiple times to enable or disable multiple options. This instruction will be implemented when the specific operator policy and call control profile are applied.

The PLMN value in RAI/ULI can be selected if 3G network-sharing is enabled.

Example

The following command series instructs the SGSN (1) not to send MS' timezone IE, and (2) to identify the MS' radio access technology info in the GTP messages:

no gtp send ms-timezone
gtp send rat

The next set of commands provides examples indicating the usage of keywords to select PLMN values in RAI/ULI.

On executing the following command, ULI is sent and PLMN will be "use-selected-plmn" if network-sharing is enabled. If network-sharing is not enabled, PLMN will be "use-local-plmn".

gtp send uli

On executing the following command, ULI is sent and PLMN will be "use-selected-plmn" if network-sharing is enabled. If network-sharing is not enabled, PLMN will be "use-local-plmn".

gtp send uli use-local-plmn

On executing the following command, ULI is sent and PLMN will be "use-selected-plmn" if network-sharing is enabled. If network-sharing is not enabled PLMN will be "use-local-plmn".

gtp send uli use-local-plmn network-sharing use-selected-plmn

On executing the following command, ULI is sent and PLMN will be "use-common-plmn" if network-sharing is enabled. If network-sharing is not enabled PLMN will be "use-local-plmn".

gtp send uli use-local-plmn network-sharing use-common-plmn

gtpp

Enables secondary GTPP accounting for an S-GW call control profile. By default, secondary GTPP accounting is disabled.

Product

S-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

gtpp secondary-group *group_name* **[accounting context** *ctx_name* **]**
no gtpp secondary-group

no

Disables secondary GTPP accounting.

secondary-group *group_name*

Enables secondary GTPP accounting and specifies a GTPP group name.

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

accounting context *ctx_name*

Specifies the specific accounting context to be used for secondary GTPP accounting. If this keyword is omitted, source context will be used for secondary GTPP accounting.

ctx_name must be an alphanumeric string of 1 through 79 characters.

Usage Guidelines

Use this command to enable or disable secondary GTPP accounting for an S-GW call control profile.

Example

The following command enables secondary GTPP accounting for an S-GW call control profile and specifies a GTPP group named *gtpp-grp1*:

```
gtpp secondary-group gtpp-grp1
```

gtpu fast-path

Enables or disables the network processing unit (NPU) Fast Path support for NPU processing of GTP-U packets of user sessions at the NPU.



Important This command is deprecated from StarOS release 16.2 onwards as the NPU FastPath feature is not supported from the StarOS 16.2 release.

Product

SAEGW

SGSN

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
[ remove ] gtpu fast-path
```

remove

Removes the NPU fast path functionality configuration from the call control profile.

Usage Guidelines

Use this command to enable/disable the NPU processed fast-path feature for processing of GTP-U data packets received from GGSN/RNC or P-GW/eNodeB. This feature enhances the GTP-U packet processing by adding the ability to fully process and forward the packets through the NPU itself.

Important When enabled/disabled, fast-path processing will be applicable only to new subscriber who establishes a PDP context after issuing this command (enabling GTP-U fast path). No existing subscriber session will be affected by this command.

Example

The following command enables the NPU fast path processing for all new subscribers' session established with this call control profile:

```
gtpu fast-path
```

guti

This command is used to configure the periodicity (time interval) / frequency of GUTI reallocation for a UE.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

`[ remove ] guti reallocation [ frequency` *`frequency`* **`| periodicity`** *`duration`* **`]`**

remove

The **remove** keyword is used to remove the configured GUTI reallocation frequency and periodicity specified in the call control profile configuration.

guti

The keyword **guti** identifies the Globally Unique Temporary UE Identity (GUTI).

reallocation

The keyword **reallocation** specifies reallocation of GUTI.

frequency *frequency*

The frequency configured specifies the GUTI reallocation frequency. The frequency is an integer with a range "1" up to "65535" requests. A configured frequency of "n" requests triggers GUTI Reallocation for every 'nth' ATTACH / TAU / SERVICE REQUEST received from the UE.

periodicity *duration*

The periodicity configured specifies GUTI reallocation periodicity. The periodicity is an integer with a range "1" up to "65535" minutes. A configured periodicity of "t" minutes triggers GUTI Reallocation at every "t" minutes for a UE.

Usage Guidelines

GUTI reallocation is disabled by default. Use this command to configure the periodicity (time interval) / frequency of GUTI reallocation for a UE.

Example

The following command is used to configure the frequency of GUTI reallocation for a UE as "10".

```
guti reallocation frequency 10
```

gw-selection

Configures the parameters controlling the gateway selection process.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
[ remove ] gw-selection { co-location [ weight [ prefer { sgw | pgw } ] ]| gtp-weight | pgw weight | sgw weight | topology [ weight [ prefer { sgw | pgw } ] ] }
```

remove gw-selection

Deletes the gw-selection definition from the call control profile.

co-location [weight [prefer { sgw | pgw }]]

Selects "co-location" as the determining factor for gateway selection. Collocation should be configured for both P-GW and S-GW selection for collocation to function. If a collocated PGW/SGW node cannot be found, then topologically closest nodes are chosen next. Host names with both "topon" and "topoff" labels will be considered in collocation.

weight: Enables weighted selection if there are multiple co-located pairs.

prefer { pgw | sgw}: Configures which weight to be used for weighted selection.

gtp-weight

Is the weight value calculated from the Load Control Information received from the GTP peers. The option enables the MME selection of SGW and PGW based on the advertised load control information. This configuration can be applied selectively to subscribers.

pgw weight

Selects PDN-Gateway as the determining factor for gateway selection.

sgw weight

Selects Serving Gateway as the determining factor for gateway selection.

topology [weight [prefer { sgw | pgw }]]

Selects topology as the determining factor for gateway selection. Topological selection is done only during initial attach, and not used during S-GW relocation or additional-pdn-connection.

weight: Enables weighted selection if there are multiple pairs with the same degree of topological closeness.

prefer { pgw | sgw}: Configures which weight to be used for weighted selection.

Usage Guidelines

Use this command to define the criteria for gateway selection.

Selection of a co-located gateway (GW) node or a topologically closer GW node is based on string comparison of canonical node names included in two or more sets of records received in DNS S-NAPTR query result. For comparison, the canonical node names are derived from the hostnames received in the DNS records. The hostnames must adhere to the following format:

```
<topon|topoff>.<single-label-interface-name>.<canonical-node-name>;
```

Where "topon" or "topoff" is a prefix of the hostname and indicates whether or not the canonical node name can be used for topology matching.

The table below lists the behaviors with various CLI options:

Table 1: CLI Behavior Options

Option	Keyword Selected	Prefix in Hostname	Topological Match Nodes Selected	Comments
1	co-location	topon	Yes	Co-located nodes are selected if available as they are listed before topologically closer nodes in the DNS records.
2	co-location	topoff	Yes	Co-located nodes are selected if available as they are listed before topologically closer nodes in the DNS records.
3	topology	topon	Yes	Co-located nodes are selected if available as they are listed before topologically closer nodes in the DNS records.

Option	Keyword Selected	Prefix in Hostname	Topological Match Nodes Selected	Comments
4	topology	topoff	No	Nodes with prefix 'topoff' are ignored for topological matching purposes. If no nodes are present with 'topon' as prefix then nodes are selected independently based on Order/Priority mentioned in DNS Records.
5	co-location	neither	Yes	Will strip only the first label from hostname to fetch canonical node name for topology matching. Co-located nodes are selected if available as they are listed before topologically closer nodes in the DNS records.
6	topology	neither	No	No co-located node pair listing; topologically closer node listing used if available (Same behavior as defined for (4).

Example

The following command instructs the MME or SGSN to determine gateway selection on the basis of topology:

```
gw-selection topology
```

hss

This command defines the HSS message specific configurations. Using this command the operator can control GPRS Subscription Data Requests in Update Location Request (ULR) messages to the HSS.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
hss message update-location-request gprs-subscription-indicator { never
| non-epc-ue }
remove hss message update-location-request gprs-subscription-indicator
```

remove

Use this keyword to remove the configuration to GPRS Subscription Data requests in the ULR messages to the HSS.

message

Use this keyword to define the HSS message specific configurations.

update-location-request

Use this keyword to specify Update Location Request (ULR) message configuration.

gprs-subscription-indicator

The HSS includes the GPRS Subscription data in the ULA command if **gprs-subscription-indicator** keyword is set in the ULR message. By default, GPRS Subscription Data is always requested from the HSS.

never

Use this keyword to specify that GPRS Subscription Data should never be requested from the HSS.

non-epc-ue

Use this keyword to specify that GPRS Subscription Data should be requested from the HSS when the UE is not an EPC-capable device.

Usage Guidelines

This command provides operator control over GPRS Subscription Data Requests in ULR messages to the HSS. If this command is configured, the parameter GPRS-Subscription-Data-Indicator is set in the ULR message. The HSS includes the GPRS subscription data in the ULA command. If the GPRS subscription data is available in the HSS and GPRS-Subscription-Data-Indicator bit is set in the ULR message, the HSS includes the GPRS Subscription data in the ULA command. By default, GPRS Subscription Data is always requested from the HSS.

Example

Use the following command to ensure the SGSN will not request GPRS Subscription Data from the HSS.

```
hss message update-location-request gprs-subscription-indicator never
```

Use the following command to ensure the SGSN will request GPRS Subscription Data from the HSS for Non-EPC-capable UEs.

```
hss message update-location-request gprs-subscription-indicator non-epc-ue
```

ie-override

This command is used to override the RAT type AVP value with the configured value for messages sent from MME to HSS.

Important This command ensures backward compatibility with previous releases as the HSS does not support the new NB-IoT RAT type.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

`[ remove ] ie-override s6a rat-type wb-eutran`

remove

The keyword remove deletes the existing configuration.

ie-override

This keyword allows the operator to configure IE override in messages sent from MME to HSS.

s6a

This keyword is used to specify the interface as s6a. The s6a interface used by the MME to communicate with the Home Subscriber Server (HSS).

rat-type

Use this keyword to configure the supported RAT type AVP IE.

wb-eutran

Use this keyword to specify the WB-EUTRAN AVP Value.

Usage Guidelines

Use this command to override the RAT type AVP value with the configured value for messages sent from MME to HSS over the s6a interface. If the configured RAT type is NB-IoT, it is changed to wb-eutran for messages sent from the MME to HSS. This command is not enabled by default.

Example

The following command is used to enable override of the RAT type AVP value with the configured value of WB-EUTRAN:

`ie-override s6a rat-type wb-eutran`

ignore-ul-data-status

This command is used to enable or disable processing of Uplink Data Status IE in Service Request.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ remove ] ignore-ul-data-status`

remove

Use this keyword to enable processing of Uplink Data Status IE in Service Request.

Usage Guidelines

This feature is enabled by default, to disable the feature use the command **ignore-ul-data-status**. To enable this feature use the command **remove ignore-ul-data-status**. When this feature is enabled, RAB is established for NSAPIs present in the Uplink data status IE. RABs are not established if the NSAPI PDPs are not present in the SGSN. If the Uplink data Status IE contains NSAPI not known to the SGSN, the SGSN establishes all the RAB's. RAB's are not established if corresponding NSAPI is absent in the PDP-Context Status IE. When this feature is disabled, if Uplink data status IE is received in service request the SGSN ignores it and establishes RAB's for all the PDP's.

Example

Use the following command to disable processing of Uplink Data Status IE in Service Request:

`ignore-ul-data-status`

idle-mode-signaling-reduction

Enables or disables the Idle-Mode-Signaling-Reduction (ISR) feature on the S4-SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description `[ remove ] idle-mode-signaling-reduction access-type [ gprs | umts ]`

remove

Disables the ISR feature configuration from this call control profile.

idle-mode-signaling-reduction

Configures ISR for this call control profile.

access-type

Specifies the network access type for the ISR feature. Select one of the following options:

- **gprs** - General Packet Radio Service network. Specifies 2G network access support for the ISR feature. *This option is only supported for Release 15.0 and beyond.*
- **umts** - Universal Mobile Telecommunications System network. Specifies 3G network access support for the ISR feature.

Usage Guidelines Use this command to enable or disable the ISR feature on the S4-SGSN. Note that ISR is supported on the S4-SGSN only.

This command is available only if the *Idle Mode Signaling Reduction* license is enabled on the SGSN.

When 3G ISR is enabled, operators should set the ISR deactivation timer value sent by the S4-SGSN to the UE in Attach Accept and Routing Area Update Accept messages. Use the **gmm T3323-timeout** command in *SGSN Service Configuration Mode* to set the ISR deactivation timer value.

When 2G ISR is enabled, operators should set the implicit detach timeout value to use for 2G ISR. Use the **gmm implicit-detach-timeout** command in *GPRS Service Configuration Mode*.

Example

```
idle-mode-signaling-reduction access-type umts
```

ims-apn

Use this command to add or remove network identifier in Call Control Profile.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description **`ims-apn network-identifier`** *`network_identifier_name`*

remove ims-apn network-identifier

network_identifier_name

Configures the network identifier on MME. Once configured APN is considered as IMS APN and UE is allowed attempt IMS PDN connection only if it is subscribed to that APN. network_identifier_name Must be string of 1 through 63 characters. It should consist only of alphabetic characters (A-Z and a-z), digits (0-9), dot(.) and the dash (-).

remove

Removes the network identifier configured for IMS APN.

Example

Use the following command to add or remove network identifier in Call Control Profile:

ims-apn network-identifier *network_identifier_name*

integrity-algorithm-lte

Specifies the order of preference for using an Integrity Algorithm.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
integrity-algorithm-lte priority1 { 128-eia0 | 128-eia1 | 128-eia2 |
128-eia3 } [ priority2 { 128-eia0 | 128-eia1 | 128-eia2 | 128-eia3 } ] [
 priority3 { 128-eia0 | 128-eia1 | 128-eia2 | 128-eia3 } ] [ priority4 {
 128-eia0 | 128-eia1 | 128-eia2 | 128-eia3 } ]
remove integrity-algorithm-lte
```

remove

Deletes the priorities definition from the call control profile configuration.

priority1

Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 1.

This is the mandatory and default priority keyword.

priority2

Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 2.

priority3

Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 3.

priority4

Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 4.

128-eia0

Sets the Null ciphering algorithm (128-EIA0) for LTE integrity as the integrity algorithm for security procedures.

Default: priority1

128-eia1

Sets the SNOW 3G synchronous stream ciphering algorithm (128-EIA1) for LTE integrity as the integrity algorithm for security procedures. SNOW 3G is a stream cipher that forms the base of the 3GPP confidentiality algorithm UEA2 and the 3GPP integrity algorithm UIA2.

Default: priority2

128-eia2

Sets the Advance Encryption Standard (AES) ciphering algorithm (128-EIA2) for LTE integrity as the integrity algorithm for security procedures.

Default: priority3

128-eia3

Sets the ZUC algorithm (128-EIA3) for LTE integrity as the integrity algorithm for security procedures.

Default: priority4

Usage Guidelines

Set the order or priority in which the MME will select an integrity algorithm for use. All the priorities must be set or the definition is invalid. The command can be re-entered to change the priorities without removing the configuration.

Example

Configure 128-EIA0 as first priority integrity algorithm:

```
integrity-algorithm-lte priority1 128-eia 0 priority2 128-eia 2 priority3
 128-eia 1
```

integrity-algorithm-umts

Configures the order of preference for the Integrity Algorithm used for 3G.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

integrity-algorithm-umts *type* **then_** *type*
default integrity-algorithm-umts

default

Specifies the default preference based on system defaults.

type

Creates a configuration defining an order of preference. Enter one or more of the following options in the order of preference:

- **uia1** - uia1 Algorithm
- **uia2** - uia2 Algorithm

Usage Guidelines

Use this command to determine which integrity algorithm is preferred 3G. This command is configured in tandem with the algorithm type for **encryption-algorithm-umts** command.

Example

default integrity-algorithm-umts

lcs-mo

This command enables/disables mobile-originating Location Requests by access-type when Location Services functionality is enabled.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > **call-control-profile** *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description **`lcs-mo { allow | restrict } access-type { gprs | umts }`**

allow

Enables mobile-originating Location Requests. This is the default state when Location Services are enabled.

Usage Guidelines This command ties Location Service functionality to a call-control profile by IMSI so that Location Services can optionally be determined by an operator policy for incoming calls.

Example

Use the following command to disable or disallow mobile-originating Location Requests within a GPRS network:

`lcs-mo restrict access-type gprs`

lcs-mt

This command enables/disables mobile-terminating Location Requests by access-type when Location Services functionality is enabled.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > **call-control-profile** *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description **`lcs-mt { allow | restrict } access-type { gprs | umts }`**

allow

Enables mobile-terminating Location Requests. This is the default state when Location Services are enabled.

Usage Guidelines This command ties Location Service functionality to a call-control profile by IMSI so that Location Services can optionally be determined by an operator policy for incoming calls.

Example

Use the following command to disable or disallow mobile-terminating Location Requests within a UMTS network:

```
lcs-mt restrict access-type umts
```

lcs-ni

This command enables/disables network-initiated Location Requests by access-type when Location Services functionality is enabled.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

`lcs-ni { allow | restrict } access-type { gprs | umts }`

allow

Enables network-initiated Location Requests . This is the default state when Location Services are enabled.

Usage Guidelines

This command ties Location Service functionality to a call-control profile by IMSI so that Location Services can optionally be determined by an operator policy for incoming calls.

Example

Use the following command to enable or allow network-initiated Location Requests within a UMTS network if this function has been restricted previously:

```
lcs-ni allow access-type umts
```

local-cause-code-mapping apn-mismatch

Configures the reject cause code to send to a UE when an APN mismatch occurs.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

```
local-cause-code-mapping apn-mismatch emm-cause-code {
eps-service-not-allowed-in-this-plmn | esm-failure esm-cause-code
unknown-apn | no-suitable-cell-in-tracking-area | plmn-not-allowed |
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }
remove local-cause-code-mapping apn-mismatch
```

remove local-cause-code-mapping apn-mismatch

Removes the configured cause code mapping.

apn-mismatch emm-cause-code { eps-service-not-allowed-in-this-plmn | esm-failure esm-cause-code unknown-apn | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when an APN mismatch occurs.

- **eps-service-not-allowed-in-this-plmn**
- **esm-failure esm-cause-code unknown-apn** - Default.

  For the **esm-failure** cause code only, the **unknown-apn** ESM code is also reported to the UE.

- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Usage Guidelines

Use this command to configure the cause code returned to a UE when an APN mismatch occurs, such as when an APN is present in the HSS subscription but the HSS subscription for this IMSI has other APNs present in the subscription.

If a condition is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

The following command maps the "PLMN not allowed" cause code to the APN mismatch condition:

```
local-cause-code-mapping apn-mismatch emm-cause-code plmn-not-allowed
```

local-cause-code-mapping apn-not-subscribed

Gives the operator the option to specify the local cause-code mapping when the UE-requested APN is not subscribed.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`local-cause-code-mapping apn-not-subscribed esm-cause-code requested-service-option-not-subscribed`
`remove local-cause-code-mapping apn-not-subscribed`

remove

Deletes the local cause code mapping from the configuration.

Usage Guidelines

The operator can specify "Requested-Option-Not-Subscribed" cause code value #33 will be sent in the Reject message when the PDN Connectivity Request is rejected because no subscription is found. If the command option is not configured, then by default the MME uses the cause code value #27 (Unknown or Missing APN) in standalone PDN Connectivity Reject message when the UE-requested APN is not subscribed.

The new keyword apn-not-subscribed is added to specify the local cause-code mapping when the UE-requested APN is not subscribed for that subscriber. If cause code mapping for apn-not-subscribed is explicitly configured with requested-service-option-not-subscribed in either the Call-Control-Profile or MME-Service configuration mode, then the new code "Requested-Option-Not-Subscribed" (cause-code #33) will be sent in the Reject message when the PDN Connectivity Request is rejected because no subscription is found.

Example

The following instructs the MME to use cause code #33 ("Requested-Option-Not-Subscribed") in place of the default #27 (Unknown or Missing APN):

`local-cause-code-mapping apn-not-subscribed esm-cause-code requested-service-option-not-subscribed`

local-cause-code-mapping apn-not-supported-in-plmn-rat

In support of 3GPP Release 11 EMM/ESM cause code #66, this command remaps the EMM/ESM/SM cause codes to operator-preferred codes in the Call Control Profile. These replacements codes are sent in Reject messages when the activation rejection is due to the APN not being supported in the requested PLMN/RAT.

Product

SGSN

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
local-cause-code-mapping apn-not-supported-in-plmn-rat { emm-cause-code
emm_cause_number esm-cause-code esm_cause_number [ attach ] [ tau ] } |
esm-cause-code esm_cause_number esm-proc | sm-cause-code sm_cause_number }
remove local-cause-code-mapping apn-not-supported-in-plmn-rat [ attach |
 esm-proc | sm-cause-code | tau ]
```

remove

Removes the configured cause code mapping.

apn-not-supported-in-plmn-rat

The keyword **apn-not-supported-in-plmn-rat** specifies that the MME is to use the mapped operator-preferred replacement cause codes when a call is rejected because the requested APN is not supported in current RAT and PLMN combination.

emm-cause-code *emm_cause_number* esm-cause-code *esm_cause_number* [attach] [tau]

MME only.

The keyword **emm-cause-code** configures the operator-preferred EMM cause code to be used if a NAS Request is rejected due to this configuration.

- *emm_cause_number* specifies the EMM code replacement integer. The system accepts a value in the range 0 through 255, however, the standards-compliant valid values are in the range 2 through 111.
- **esm-cause-code** configures the operator-preferred ESM cause code to be used if a NAS Request is rejected due to this configuration.
- *esm_cause_number* specifies the ESM code replacement integer. The system accepts a value in the range 0 through 255, however, the standards-compliant valid values are in the range 8 through 112.
- The **attach** keyword filter instructs the MME to use the mapped replacement cause code if an Attach procedure is rejected due to the noted APN not supported error condition.
- The **tau** keyword filter instructs the MME to use the mapped replacement cause code if an TAU procedure is rejected due to the noted APN not supported error condition.

esm-cause-code *esm_cause_number* esm-proc

MME only.

esm-cause-code configures the operator-preferred ESM cause code to be used if a bearer management Request is rejected due to this configuration.

- *esm_cause_number* specifies the ESM cause code replacement integer in the range 0 through 255.
- The **esm-proc** keyword filter instructs the MME to use the mapped replacement cause code if an ESM procedure is rejected due to the noted APN not supported error condition.

sm-cause-code *sm_cause_number*

SGSN only.

The keyword **sm-cause-code** identifies the operator-preferred SM cause code to be used towards the UE. *sm_cause_number* value can be any integer in the range 0 through 255.

Usage Guidelines

This command specifies the cause codes that operator would prefer to send our in Reject messages when the cause of the call rejection is the APN not being supported in the current RAT and PLMN combination. This mapping is not done by default.

- The **emm-cause-code** keyword is used to specify the EMM cause code to be used if a NAS request is rejected due to this configuration.
- The **esm-cause-code** keyword is used to specify the ESM cause code to be used if a bearer management request is rejected due to this configuration.
- The **sm-cause-code** keyword is used to specify the SM cause code used towards UE.

Example

The following command maps cause code *20* in place of standard cause code #66 for the SGSN to send in activate rejection messages.

```
local-cause-code-mapping apn-not-supported-in-plmn-rat sm-cause-code 20
```

local-cause-code-mapping auth-failure

Configures the reject cause code to send to a UE when an authentication failure occurs.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
local-cause-code-mapping auth-failure emm-cause-code {
eps-service-not-allowed-in-this-plmn | network-failure |
no-suitable-cell-in-tracking-area | plmn-not-allowed |
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }
remove local-cause-code-mapping auth-failure
```

remove local-cause-code-mapping auth-failure

Removes the configured cause code mapping.

auth-failure emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when an authentication failure occurs.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-suitable-cell-in-tracking-area**

- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Usage Guidelines

Use this command to configure the cause code returned to a UE when an authentication failure occurs. By default, the MME sends the UE the **#3 - Illegal MS** cause code when encountering an authentication failure.

This condition occurs for TAU and ATTACH procedures in the following cases:

- The Authentication response from the UE does not match the expected value in the MME.
- Security Mode Reject is sent by the UE.
- The UE responds to any identity request with a different type of identity (for example, the MME could query for IMSI and the UE responds with IMEI).

The following are **not** considered for the authentication failure condition:

- HSS returning a result code other than SUCCESS.
- HSS not available.
- EIR failures.
- UE not responding to requests.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

The following command maps the "network-failure" cause code to the authentication failure condition:

```
local-cause-code-mapping auth-failure emm-cause-code network-failure
```

local-cause-code-mapping congestion

Configures the reject cause code to send to a UE when a procedure fails due to a congestion condition.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
local-cause-code-mapping congestion emm-cause-code { congestion [
esm-cause-code { congestion | insufficient-resources |
service-option-temporarily-out-of-order } ] |
eps-service-not-allowed-in-this-plmn | network failure |
no-suitable-cell-in-tracking-area | plmn-not-allowed |
```

```
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }
remove local-cause-code-mapping congestion
```

remove local-cause-code-mapping congestion

Removes the configured cause code mapping.

congestion emm-cause { congestion [esm-cause-code { congestion | insufficient-resources | service-option-temporarily-out-of-order }] | eps-service-not-allowed-in-this-plmn | network failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when a UE requests access when the system is exceeding any of its congestion control thresholds.

- **congestion** - Default
- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

esm-cause-code { congestion | insufficient-resources | service-option-temporarily-out-of-order }

Specifies the EPS Session Management (ESM) cause code to return when a UE requests access when the system is exceeding any of its congestion control thresholds.

- **congestion** - Default
- **insufficient-resources**
- **service-option-temporarily-out-of-order**

Usage Guidelines

Use this command to configure the cause code returned to a UE when a UE procedure fails due to a congestion condition on the MME.

To set the cause codes for situations where a call control profile cannot be attached to a call (for example new-call restrictions, congestion during new call attempt, etc.), use the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

The following command maps the "network failure" cause code to the congestion event:

```
local-cause-code-mapping congestion emm-cause-code network-failure
```

local-cause-code-mapping ctxt-xfer-fail-mme

Configures the reject cause code to send to a UE when a UE context transfer failure from a peer MME occurs.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`local-cause-code-mapping ctxt-xfer-fail-mme emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed } remove local-cause-code-mapping ctxt-xfer-fail-mme`

remove local-cause-code-mapping ctxt-xfer-fail-mme

Removes the configured cause code mapping.

ctxt-xfer-fail-mme emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when a UE context transfer failure from a peer MME occurs.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Usage Guidelines

Use this command to configure the cause code returned to a UE when a UE context transfer failure from a peer MME occurs. By default, the MME sends the UE the **#9 - MS identity cannot be derived by the network** cause code for this condition.

After the peer node has been identified, the MME sends a Context Request to the peer node. If the peer node is an MME, and if the context transfer procedure fails, this condition is detected.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

The following command maps the "network-failure" cause code to the context transfer failure from MME condition:

`local-cause-code-mapping ctxt-xfer-fail-mme emm-cause-code network-failure`

local-cause-code-mapping ctxt-xfer-fail-sgsn

Configures the reject cause code to send to a UE when a UE context transfer failure from a peer SGSN occurs.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
local-cause-code-mapping ctxt-xfer-fail-sgsn emm-cause-code {
eps-service-not-allowed-in-this-plmn | network-failure |
no-suitable-cell-in-tracking-area | plmn-not-allowed |
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }
remove local-cause-code-mapping ctxt-xfer-fail-sgsn
```

remove local-cause-code-mapping ctxt-xfer-fail-sgsn

Removes the configured cause code mapping.

ctxt-xfer-fail-sgsn emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when a UE context transfer failure from a peer SGSN occurs.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Usage Guidelines

Use this command to configure the cause code returned to a UE when a UE context transfer failure from a peer SGSN occurs. By default, the MME sends the UE the **#9 - MS identity cannot be derived by the network** cause code when encountering this condition.

After the peer node has been identified, the MME sends a Context Request to the peer node. If the peer node is an SGSN, and if the context transfer procedure fails, this condition is detected.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

The following command maps the "network-failure" cause code to the context transfer failure from SGSN condition:

```
local-cause-code-mapping ctxt-xfer-fail-sgsn emm-cause-code network-failure
```

local-cause-code-mapping gw-unreachable

Configures the reject cause code to send to a UE when a gateway (S-GW or P-GW) does not respond during an EMM procedure.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
local-cause-code-mapping gw-unreachable emm-cause-code {
eps-service-not-allowed-in-this-plmn | network-failure |
no-suitable-cell-in-tracking-area | plmn-not-allowed |
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }
[ attach [ tau ] | tau [ attach ] ] | { no-bearers-active tau }
remove local-cause-code-mapping gw-unreachable [ attach | tau ]
```

remove local-cause-code-mapping gw-unreachable [attach | tau]

Removes the configured cause code mapping.

gw-unreachable emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when a gateway does not respond.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-bearers-active**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

[attach [tau] | tau [attach]] | { no-bearers-active tau }

Optionally, the MME can return separate cause codes for Attach procedures and TAU procedures. This capability is available for any of the above EMM cause codes except **no-bearers-active**, which can only be defined for TAU procedures.

Usage Guidelines

Use this command to configure the cause code returned to a UE when a gateway (S-GW or P-GW) does not respond during an EMM procedure.

Defaults:

Prior to StarOS 15.0 MR5, the MME sends the UE the **#19 - ESM Failure** cause code when encountering this condition.

In StarOS 15.0 MR5 and higher releases, the MME sends the UE the **#19 - ESM Failure** cause code for Attach procedures, and **#40 - NO-EPS-BEARER-CONTEXT-ACTIVATED** for TAU procedures.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

The following command maps the "network-failure" cause code to the gateway unreachable condition:

```
local-cause-code-mapping gw-unreachable emm-cause-code network-failure
```

local-cause-code-mapping hss-unavailable

Configures the reject cause code to send to a UE when the HSS does not respond.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
local-cause-code-mapping hss-unavailable emm-cause-code {
eps-service-not-allowed-in-this-plmn | network-failure |
no-suitable-cell-in-tracking-area | plmn-not-allowed |
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }
remove local-cause-code-mapping hss-unavailable
```

remove local-cause-code-mapping hss-unavailable

Removes the configured cause code mapping.

hss-unavailable emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when the HSS does not respond.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Usage Guidelines

Use this command to configure the cause code returned to a UE when the HSS is unavailable. By default, the MME sends the UE the **#17 - Network failure** cause code when encountering this condition.

This condition is detected in the following cases:

- HSS resolution fails in the MME.
- HSS does not respond in time.

The cause code configured for this condition will be signaled in TAU and ATTACH REJECT messages.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

The following command maps the "tracking-area-not-allowed" cause code to the HSS unavailable condition:

```
local-cause-code-mapping hss-unavailable emm-cause-code
tracking-area-not-allowed
```

local-cause-code-mapping map-cause-code

Configures the operator-preferred GMM reject cause code to send to a UE in response to some failures, such as Inbound RAU Context Transfer failure .

Product

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
local-cause-code-mapping map-cause-code { roaming-not-allowed
gmm-cause-code gmm-cause | unknown-subscriber { gmm-cause-code gmm-cause |
map-diag-info { gprs-subscription-unknown gmm-cause-code gmm-cause |
imsi-unknown gmm-cause-code gmm-cause } } }
remove local-cause-code-mapping map-cause-code { roaming-not-allowed |
unknown-subscriber { gmm-cause-code  | map-diag-info {
gprs-subscription-unknown  | imsi-unknown  } } }
```

remove

Removes the specified, previously configured cause code mapping .

roaming-not-allowed

Instructs the SGSN to send a different GPRS mobility management (GMM) cause code to a UE when the UE's access request is rejected due to map cause 'roaming not allowed'. Specify one of the GMM cause codes listed below.

unknown-subscriber

Instructs the SGSN to send a different GPRS mobility management (GMM) cause code to a UE when the UE's access request is rejected due to map cause 'unknown-subscriber'. As well, the Operator is given the *option* to include MAP diagnostic information in the Reject message to provide additional details about the MAP failure.

- **gmm-cause-code** replaces the cause code. For options see below.
- **map-diag-info** instructs the SGSN to include one of two types of MAP diagnostic information in the Reject message *AND* specifies the replacement GMM cause code to use in the Reject message.
  - **gprs-subscription-unknown**
  - **imsi-unknown**

gmm-cause-code *gmm-cause*

Specifies the GPRS mobility management (GMM) cause code to return to a UE in access request Reject messages. Replacement cause code options include:

- **gprs-serv-and-non-gprs-serv-not-allowed**
- **gprs-serv-not-allowed**
- **gprs-serv-not-in-this-plmn**
- **location-area-not-allowed**
- **network-failure**
- **no-suitable-cell-in-this-la**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-la**

Usage Guidelines

This command enables the operator to configure a preferred GMM cause code to return to the UE when a UE access request is rejected due to map-cause 'roaming-not-allowed' or 'unknown-subscriber'.

As well, the operator can send additional MAP failure details in the reject message when the map-cause being replaced is 'unknown-subscriber'.

It is possible to map replacement cause codes for both 'roaming-not-allowed' and 'unknown-subscriber, but additional configurations for either would overwrite.

Example

The following command maps *network-failure* as the GMM cause code to be included in an Access Reject sent to the UE when the UE is denied due to map-cause 'roaming-not-allowed':

```
local-cause-code-mapping map-cause-code roaming-not-allowed gmm-cause-code
 network-failure
```

Use the following to change a mapping configuration of 'unknown-subscriber' replaced by 'roaming-not-allowed-in-this-la' to 'unknown-subscriber' replaced by cause code 'gprs-serv-not-in-this-plmn' and include MAP diagnostic information in the Reject message:

```
local-cause-code-mapping map-cause-code unknown-subscriber map-diag-info
 gprs-subscription-unknown gmm-cause-code gprs-serv-not-in-this-plmn
```

local-cause-code-mapping no-active-bearers

Configures the reject cause code to send to a UE when the context received from a peer SGSN (during a TAU procedure) does not contain any active PDP contexts.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
local-cause-code-mapping no-active-bearers emm-cause-code {
eps-service-not-allowed-in-this-plmn | network-failure | no-bearers-active
 | no-suitable-cell-in-tracking-area | plmn-not-allowed |
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }
remove local-cause-code-mapping no-active-bearers
```

remove local-cause-code-mapping no-active-bearers

Removes the configured cause code mapping.

no-active-bearers emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-bearers-active | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when no active PDP context exists.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure**

- **no-bearers-active**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Usage Guidelines Use this command to configure the cause code returned to a UE when the context received from a peer SGSN (during a TAU procedure) does not contain any active PDP contexts. By default, the MME sends the UE the **#40 - No PDP context activated** cause code when encountering this condition.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

The following command maps the "plmn-not-allowed" cause code to the no active bearer condition:

```
local-cause-code-mapping no-active-bearers emm-cause-code plmn-not-allowed
```

local-cause-code-mapping odb packet-services

Configures the ESM and EMM cause codes to send to a UE depending on the Operator Determined Barring (ODB) condition.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
local-cause-code-mapping odb packet-services emm-cause-code cc_value [
esm-cause-code cc_value ]
remove local-cause-code-mapping odb packet-services
```

remove local-cause-code-mapping odb packet-services

Removes the configured cause code mapping.

packet-services emm-cause-code *cc_value* [esm-cause-code *cc_value*]

Specifies the EPS Mobility Management (EMM) cause code to return when ODB condition is hit.

emm-cause-code *cc_value* : Specifies the EMM cause code for ODB all packet services. The EMM cause code value is an integer from 0 to 255.

esm-cause-code *cc_value* : This is an optional keyword used to specify the ESM cause code as an integer from 0 to 255.

Usage Guidelines

Use this command to configure the cause code returned to a UE when ODB condition is hit, such as when the subscriber does not have an LTE/EPS subscription.

Related Commands:

If a condition is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signaled to the UE. See also the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

The following command maps the EMM cause code #15 (NO_SUITABLE_CELL_IN_TRACKING_AREA) to the ODB condition:

```
local-cause-code-mapping odb packet-services emm-cause-code 15
```

local-cause-code-mapping odb roamer-to-vplmn

Configures the ESM and EMM cause codes to send to a UE depending on the Operator Determined Barring (ODB) condition.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
local-cause-code-mapping odb roamer-to-vplmn emm-cause-code cc_value [
esm-cause-code cc_value ]
remove local-cause-code-mapping odb roamer-to-vplmn
```

remove local-cause-code-mapping odb roamer-to-vplmn

Removes the configured cause code mapping.

roamer-to-vplmn emm-cause-code *cc_value* [esm-cause-code *cc_value*]

Specifies the EPS Mobility Management (EMM) cause code to return when ODB condition is hit.

emm-cause-code *cc_value* : Specifies the EMM cause code for ODB roamer to visited PLMN. The EMM cause code value is an integer from 0 to 255.

esm-cause-code *cc_value* : This is an optional keyword used to specify the ESM cause code as an integer from 0 to 255.

Usage Guidelines

Use this command to configure the cause code returned to a UE when ODB condition is hit, such as when the subscriber does not have an LTE/EPS subscription.

Related Commands:

If a condition is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signaled to the UE. See also the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

The following command maps the EMM cause code #15 (NO_SUITABLE_CELL_IN_TRACKING_AREA) to the ODB condition:

```
local-cause-code-mapping odb roamer-to-vplmn emm-cause-code 15
```

local-cause-code-mapping path-failure

Configures SM cause codes for SGSN to send in Deactivate PDP Request.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
local-cause-code-mapping path-failure sm-cause-code {
insufficient-resources | network-failure | reactivation-requested |
regular-deactivation }
remove local-cause-code-mapping path-failure
```

remove

Erases defined cause code configuration.

sm-cause-code

Defines the SM cause code to replace the default cause code sent in a Deactivate PDP Request message when a GTP-C path failure occurs. Options include:

- insufficient-resources
- network-failure
- reactivation-requested
- regular-deactivation

Usage Guidelines

This command is part of the Cause Code Mapping feature, documented in the *SGSN Administration Guide*, that provides the operator with the option to configure preferred cause codes to be sent in error or failure messages to the UE.

Example

Use the following command to replace the default cause code with SM cause *network-failure*:

```
local-cause-code-mapping path-failure sm-cause-code network-failure
```

local-cause-code-mapping peer-node-unknown

Configures the reject cause code to send to a UE when peer node resolution is not successful.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
local-cause-code-mapping peer-node-unknown emm-cause-code {
eps-service-not-allowed-in-this-plmn | network-failure |
no-suitable-cell-in-tracking-area | plmn-not-allowed |
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }
remove local-cause-code-mapping peer-node-unknown
```

remove local-cause-code-mapping peer-node-unknown

Removes the configured cause code mapping.

peer-node-unknown emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when the peer node resolution is not successful.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Usage Guidelines

Use this command to configure the cause code returned to a UE when peer node resolution is not successful. By default, the MME sends the UE the **#9 - MS identity cannot be derived by the network** cause code when encountering this condition.

During processing of a TAU REQUEST, the resolution of a peer MME that had allocated the temporary identity that is signaled to the UE takes several steps in the MME. This resolution can be done based on DNS or based on local configuration. This condition occurs when all mechanisms for peer node resolution are done with no success.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

The following command maps the "plmn-not-allowed" cause code to the peer node unknown condition:

```
local-cause-code-mapping peer-node-unknown emm-cause-code plmn-not-allowed
```

local-cause-code-mapping pgw-selection-failure

Configures the reject cause code to send to a UE when a failure occurs during P-GW selection.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
local-cause-code-mapping pgw-selection-failure emm-cause-code { {
esm-failure esm-cause-code unknown-apn }|
eps-service-not-allowed-in-this-plmn | network-failure |
no-suitable-cell-in-tracking-area | plmn-not-allowed |
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }
remove local-cause-code-mapping pgw-selection-failure
```

remove local-cause-code-mapping pgw-selection-failure

Removes the configured cause code mapping.

pgw-selection-failure emm-cause-code { { esm-failure esm-cause-code unknown-apn } |eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when a failure occurs during P-GW selection.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**
- **esm-failure**
- **esm-cause-code**
- **unknown-apn**

Usage Guidelines

Use this command to configure the cause code returned to a UE when a failure occurs during P-GW selection. By default, the MME sends the UE the **#17 - Network failure** cause code when encountering this condition. To overcome the impact in MME 4G attach SR calculations, the MME sends the UE the **#19 - ESM failure #27 - Unknown APN**cause code when encountering this condition.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

The following command maps the "plmn-not-allowed" cause code to the P-GW selection failure condition:

```
local-cause-code-mapping pgw-selection-failure emm-cause-code
plmn-not-allowed
```

Example

The following command maps the "esm-failure" "esm-cause-code" and "unknown-apn" cause code to the P-GW selection failure condition:

```
local-cause-code-mapping pgw-selection-failure emm-cause-code { esm-failure
 esm-cause-code unknown-apn }
```

local-cause-code-mapping restricted-zone-code

Configures the reject cause code to send to a UE when a UE requests access to a restricted zone.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
local-cause-code-mapping restricted-zone-code emm-cause-code {
eps-service-not-allowed-in-this-plmn | no-suitable-cell-in-tracking-area
 | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area |
tracking-area-not-allowed }
remove local-cause-code-mapping restricted-zone-code
```

remove local-cause-code-mapping restricted-zone-code

Removes the configured cause code mapping.

restricted-zone-code emm-cause-code *emm_cause_code*

Specifies the EPS Mobility Management (EMM) cause code to return when a UE requests access to a restricted zone.

emm_cause_code must be one of the following options:

- **eps-service-not-allowed-in-this-plmn**
- **no-suitable-cell-in-tracking-area** - Default.
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Usage Guidelines

Use this command to configure the cause code returned to a UE when a UE requests access to a restricted zone.

To set the cause codes for situations where a call control profile cannot be attached to a call (for example new-call restrictions, congestion during new call attempt, etc.), use the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

The following command maps the "PLMN not allowed" cause code to the restricted zone code event:

```
local-cause-code-mapping restricted-zone-code emm-cause-code
plmn-not-allowed
```

local-cause-code-mapping sgw-selection-failure

Configures the reject cause code to send to a UE when a failure occurs during S-GW selection.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
local-cause-code-mapping sgw-selection-failure emm-cause-code {
eps-service-not-allowed-in-this-plmn | network-failure |
no-suitable-cell-in-tracking-area | plmn-not-allowed |
roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }
remove local-cause-code-mapping sgw-selection-failure
```

remove local-cause-code-mapping sgw-selection-failure

Removes the configured cause code mapping.

sgw-selection-failure emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when a failure occurs during S-GW selection.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Usage Guidelines

Use this command to configure the cause code returned to a UE when a failure occurs during S-GW selection. By default, the MME sends the UE the **#17 - Network failure** cause code when encountering this condition.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

The following command maps the "plmn-not-allowed" cause code to the S-GW selection failure condition:

```
local-cause-code-mapping sgw-selection-failure emm-cause-code
plmn-not-allowed
```

local-cause-code-mapping vlr-down

Configures the cause code to send in a ATTACH ACCEPT or TAU ACCEPT to a UE that attachment to the VLR has failed because a VLR down condition is present.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`local-cause-code-mapping vlr-down emm-cause-code { congestion | cs-domain-unavailable | imsi-unknown-in-hlr | msc-temp-unreachable | network-failure }`
`remove local-cause-code-mapping vlr-down`

remove local-cause-code-mapping vlr-down

Removes the configured cause code mapping.

vlr-down emm-cause-code *emm_cause_code*

Specifies the EPS Mobility Management (EMM) cause code to return when a VLR down condition is present.

emm_cause_code must be one of the following options:

- **congestion**
- **cs-domain-unavailable**
- **imsi-unknown-in-hlr**
- **msc-temp-unreachable**- Default.
- **network-failure**

Usage Guidelines

Use this command to configure the cause code returned to a UE when a VLR down condition is present.

To set the cause codes for situations where a call control profile cannot be attached to a call (for example new-call restrictions, congestion during new call attempt, etc.), use the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode* Commands chapter.

Example

The following command maps the "network failure" EMM cause code to the VLR down condition:

`local-cause-code-mapping vlr-down emm-cause-code network-failure`

local-cause-code-mapping vlr-unreachable

Configures the cause code to send in a ATTACH ACCEPT or TAU ACCEPT to a UE that attachment to the VLR has failed because a VLR unreachable condition is present.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`local-cause-code-mapping vlr-unreachable emm-cause-code { congestion | cs-domain-unavailable | imsi-unknown-in-hlr | msc-temp-unreachable | network-failure }`
`remove local-cause-code-mapping vlr-unreachable`

remove local-cause-code-mapping vlr-unreachable

Removes the configured cause code mapping.

vlr-down emm-cause-code *emm_cause_code*

Specifies the EPS Mobility Management (EMM) cause code to return when a VLR unreachable condition is present.

emm_cause_code must be one of the following options:

- **congestion**
- **cs-domain-unavailable**
- **imsi-unknown-in-hlr**
- **msc-temp-unreachable** - Default.
- **network-failure**

Usage Guidelines

Use this command to configure the cause code returned to a UE when a VLR unreachable condition is present.

To set the cause codes for situations where a call control profile cannot be attached to a call (for example new-call restrictions, congestion during new call attempt, etc.), use the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode* Commands chapter.

Example

The following command maps the "network failure" EMM cause code to the VLR unreachable condition:

`local-cause-code-mapping vlr-unreachable emm-cause-code network-failure`

location-area-list

Defines the location area list to allow or restrict services in the specified location areas identified by location area code (LAC).

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`location-area-list instance` *`instance`* **`area-code`** *`area_code`* **`[`** *`area_code *`* **`]`**
`no location-area-list instance` *`instance`* **`[ area-code`** *`area_code`* **`]`**

no

If the **area-code** keyword is included in the command, then only the specified area code is removed from the identified list. If the **area-code** keyword is not included with the command, the entire list of LACs is removed from this call control profile.

instance *instance*

Specifies an identification for the specific location area list.

instance must be an integer between 1 and 5.

area-code *area_code **

This keyword defines the location area codes (LACs) to be used by this call control profile as a determining factor in the handling of incoming calls. Multiple LACs can be defined in a single location-area-list.

area_code: Enter an integer between 1 and 65535.

* If desired, enter multiple LACs separated by a single blank space.

Usage Guidelines

Use the command multiple times to configure multiple LAC lists or to modify the a list.

Example

The following command creates a location area list for a single area code:

```
location-area-list instance 1 area-code 514
```

This command creates a second location area list for with multiple area codes - all separated by a single blank space:

```
location-area-list instance 2 area-code 514 62552 32 1513
```

The next command corrects an area code mistake (327 not 32) made in the previous configuration:

```
location-area-list instance 1 area-code 514 62552 327 1513
```

location-reporting

Enable 3G/2G Location Change Reporting feature on the SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ remove ] location-reporting access-type { gprs | umts }`

remove

If the **remove** keyword is included in the command, then the location change reporting feature is disabled.

access-type *type*

Defines the type of subscriber access which is to reported for location changes.

- **gprs** - 2G
- **umts** - 3G

Usage Guidelines

Use the command multiple times to configure both types of access types.

This command enables the 3G/2G Location Change Reporting feature which notifies the GGSN whenever one of the following changes for a UE:

- the serving cell global identity (CGI), or
- the service area identity (SAI), or
- the routing area identity (RAI).

Example

The following command enables location change reporting to a GGSN for 3G subscribers:

`location-reporting access-type umts`

This command disables location change reporting that has been enabled for 2G subscribers:

`remove location-reporting access-type gprs`

lte-zone-code

Configures the enforcement of allowed or restricted zone code lists and associates an EPS Mobility Management (EMM) cause code to rejected attach attempts.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
lte-zone-code [ allow | restrict } { emm-cause-code {
eps-service-not-allowed-in-this-plmn | no-suitable-cell-in-tracking-area
 | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area |
tracking-area-not-allowed ] zone-code-list zc_id +
remove lte-zone-code zone-code-list
```

remove

Removes the zone code list from the call control profile.

[allow | restrict]

Specifies whether the zone code list is allowed or restricted.

Important You can only create an allowed or restricted list, not both.

emm-cause-code [eps-service-not-allowed-in-this-plmn | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed]

Optionally, specify one of the following EMM cause codes to apply when a UE request is rejected:

eps-service-not-allowed-in-this-plmn

no-suitable-cell-in-tracking-area

plmn-not-allowed

roaming-not-allowed-in-this-tracking-area

tracking-area-not-allowed

zone-code-list *zc_id* +

Specifies the zone code in the allowed or restricted list of zone codes. *zone_code* must be an integer value from 0 to 65535.

Usage Guidelines

Use this command to create zone code lists that allow or restrict access to UEs managed by this call control profile.

Example

The following command restricts access to zone codes 234 and 456 and returns an EMM cause code of "tracking area not allowed":

```
lte-zone-code restrict emm-cause-code tracking-area-not-allowed
zone-code-list 234 456
```

lte-m-rat

Enables configuration for LTE-M-RAT Access type.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*` )`**`lte-m-ratflag-LTEMPI`**`#`

Syntax Description

`[ no | default | remove ]lte-m-rat flag-LTEMPI`

no

Diables the configuration from call-control profile and fallback to the mme-service configuration.

default

Resets the configuration from call-control profile and fallback to the mme-service configuration.

remove

Removes the configuration from call-control profile and fallback to the mme-service configuration.

lte-m-rat

Enables configuration for LTE-M Access Type.

flag-LTEMPI

Configures the LTE-M RAT Indication to S-GW to pass the LTE-M RAT type to the P-GW.

Usage Guidelines

Use this command to enable or disable LTE-M-RAT Access type.

Example

The following command enables the LTE-M-RAT Access type.

`lte-m-rat flag-LTEMPI { 1 | 0 }`

map

Configures the optional extensions to Mobile Application Part (MAP) messages.Using this command the operator can control GPRS/EPS Subscription data requests in UGL messages to the HLR.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ remove ] map message { mo-fwd-sm imsi | update-gprs-location { eps-subscription-not-needed [ always | non- epc-ue ] | exclude-gmlc | gprs-subscription-not-needed [ always | epc-ue ] | imeisv | private-extension access-type } }`
`remove map message update-gprs-location gprs-subscription-not-needed`
`remove map message update-gprs-location eps-subscription-not-needed`

remove

IMEI-SV is not included in the GLU request -- this is the default behavior. The remove option is also used to remove the configuration of GPRS subscription data or EPS subscription data requests in UGL messages to the HLR.

message mo-fwd-sm imsi

Configures the SGSN to include the IMSI of the originating subscriber in the mobile-originated SM transfer. This parameter shall be included when the sending entity (MSC or SGSN) supports mobile number portability (MNP). This IMSI IE is required in the in MAP-MO-FORWARD-SHORT-MESSAGE in countries where MNP is deployed.This keyword-set is required. The default is disabled.

update-gprs-location

Includes a GLU message.

eps-subscription-not-needed

The operator can use this keyword to control the request for EPS Subscription Data in addition to GPRS Subscription Data from the HLR. By default, EPS Subscription Data is always requested from the HLR.

Optionally include:

- **always** - Include this keyword to specify that EPS Subscription Data should never be requested from the HLR.
- **non-epc-ue** - Include this keyword to specify that EPS Subscription Data should never be requested from the HLR when the UE is not an EPC capable device.

exclude-gmlc

This keyword configures the SGSN to exclude the GMLC address in the Update-GPRS-Location (UGL) messages sent to the HLR.

gprs-subscription-not-needed

The operator can use this keyword to control the request for GPRS Subscription Data in addition to EPS Subscription Data from the HLR. By default, GPRS Subscription Data is always requested from the HLR.

Optionally include:

- **always** - Include this keyword to specify that GPRS Subscription Data should never be requested from the HLR.
- **non-epc-ue** - Include this keyword to specify that GRPS Subscription Data should never be requested from the HLR when the UE is an EPC capable device.

imeisv

Specifies the International Mobile equipment Identity-Software Version (IMEI-SV) information to include in the GPRS Location Update (GLU) request message. SGSN will include IMEI-SV in the message, if available. Default: disabled

private-extension access-type

Includes a specific access-type private extension in the message.

Usage Guidelines

This command configures optional extensions to MAP messages. The HLR should ignore these extensions if not supported by the HLR. This command allows operator control over the GPRS Subscription Data or EPS Subscription Data requests in UGL messages to the HLR.

Example

Use the following command to have the SGSN add GLU extension information to the MAP messages sent to the HLR.

```
map message update-gprs-location private-extension access-type
```

Use the following command to ensure the SGSN (or MME/ IWF) will not request GPRS Subscription Data in addition to EPS Subscription Data from the HLR.

```
map message update-gprs-location gprs-subscription-not-needed always
```

Use the following command to ensure the SGSN (or MME/ IWF) will not request GPRS Subscription Data in addition to EPS Subscription Data from the HLR for EPC capable UEs.

```
map message update-gprs-location gprs-subscription-not-needed epc-ue
```

Use the following command to ensure the SGSN will not request EPS Subscription Data in addition to GPRS Subscription Data from the HLR.

```
map message update-gprs-location eps-subscription-not-needed always
```

Use the following command to ensure the SGSN will not request EPS Subscription Data in addition to GPRS Subscription Data from the HLR for Non-EPC capable UEs.

```
map message update-gprs-location eps-subscription-not-needed non-epc-ue
```

map-service

Identifies a Mobile Application Part (MAP) service and the context which contains it and associates both with the call control profile.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`map-service context` *`ctxt_name`* **`service`** *`map_srvc_name`*
`no map-service context`

no

Disables use of MAP service with this call control profile.

context *ctxt_name*

Specifies the name of the context for the MAP service as an alphanumeric string of 1 through 64 characters.

service *map_srvc_name*

Specifies the MAP service name as an alphanumeric string of 1 through 64 characters.

Usage Guidelines

Use this command to enable or disable MAP service with this call control profile.

Example

```
no map-service context
```

max-bearers-per-subscriber

Defines the maximum number of bearers allowed per subscriber.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

max-bearers-per-subscriber *number*
remove max-bearers-per-subscriber

remove

Deletes the definition from the call control profile.

number

Identifies the maximum number of bearers allowed per subscriber as an integer from 1 to 11.

Usage Guidelines

Use this command to set the maximum number of bearers allowed per subscriber.

Example

Set the maximum to 3:

```
max-bearers-per-subscriber 3
```

max-pdns-per-subscriber

Defines the maximum number of PDNs allowed per subscriber.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

max-pdns-per-subscriber *number*
remove max-pdns-per-subscriber

remove

Deletes the definition from the call control profile.

number

Identifies the maximum number of PDNs allowed per subscriber as an integer from 1 to 11.

Usage Guidelines

Use this command to set the maximum number of PDNs allowed per subscriber.

Example

Set the maximum to 4:

```
max-pdns-per-subscriber 4
```

min-unused-auth-vectors

Configures a specific minimum number of unused vectors to be maintained by the SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

min-unused-auth-vectors *min#_vectors*
remove min-unused-auth-vectors

remove

Removes the definition from the configuration file and restores the default behavior, which does not use the threshold.

min#_vectors

Enables and defines a threshold for the minimum number of unused vectors that the SGSN retains to trigger the initation of a service area identity request (SAI) .

min#_vectors: Enter a digit betwen 1 and 4.

Usage Guidelines

Vectors are used by the SGSN for authentication. Use this command to enable a minimum threshold for unused vector for this call control profile. When the unused vector count falls below this configured threshold, then an SAI is initiated to fill the buffer back to 5 or to the most appropriate number based on the MAP service configuration.

Example

Enter a command similar to the following to set a threshold of *3*:

```
min-unused-auth-vectors 3
```

Use the following command to disable this function and restore the default behavior, which does not use a threshold to trigger an SAI:

```
remove min-unused-auth-vectors
```

mme s6a

This command is used to control sending the Notify Request (NOR) on the S6a interface.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

`[ no ] mme s6a send message nor trigger mnrf`

no

Disables sending the NOR on the S6a interface.

mme

Configures MME capability.

s6a

Configures MME capability on the S6a interface.

send

Configures MME capability to send on the S6a interface.

message

Configures MME capability to send message on the S6a interface.

nor

Configures MME capability to send NOR on the S6a interface.

trigger

Configures trigger to send the message.

mnrf

Sends message to trigger MNRF flag on the S6a interface (SMS in MME).

Usage Guidelines

Use this command to control sending the NOR on the S6a interface. This command is disabled by default.

The user sends the NOR on the S6a interface to HSS in the event of user availability to received SMS (if the user moved to active state from idle or the user's memory is available).

mme sgd

This command is used to control sending the Alert SC Request (ALR) on the SGd interface.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

`[ no ] mme sgd send message alr trigger mnrf`

no

Disables sending the ALR on the SGd interface.

mme

Configures MME capability.

sgd

Configures MME capability on the SGd interface.

send

Configures MME capability to send on the SGd interface.

message

Configures MME capability to send message on the SGd interface.

alr

Configures MME capability to send ALR on the SGd interface.

trigger

Configures trigger to send the message.

mnrf

Sends message to trigger MNRF flag on the SGd interface (SMS in MME).

Usage Guidelines

Use this command to control sending the ALR on the SGd interface. This command is disabled by default.

The user sends the ALR on the SGd interface to SMSC in the event of user availability to received SMS (if the user moved to active state from idle or the user's memory is available). It is also sent if the user did a handover to the new MME/SGSN and any MT SMS was pending for the user.

mobility-protocol

This command allows you to configure the default mobility protocol type to be used for setting up a call when the AAA server forwards an IP address directly.

Product

SaMOG

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

`mobility-protocol { GTPv1 | GTPv2 | pmip }`
`default mobility-protocol`

default

Sets the mobility-protocol configuration to its default values.

Default (SaMOG 3G license): GTPv1

Default (SaMOG Mixed Mode license): GTPv2

Usage Guidelines

Use this command to configure the default mobility protocol type to be used for setting up a call when the AAA server forwards an IP address directly. If the mobility protocol is also configured in the APN Profile Configuration Mode, the value configured here will be overridden with the configured value in the APN profile.

Example

The following command configures mobility protocol to GTPv2:

`mobility-protocol GTPv2`

monitoring-events

This command allows you to configure monitoring events for a call control profile for all users.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ no | remove ] monitoring-events`

monitoring-events

The **monitoring-events** keyword is used to Enables the monitoring events under the call control profile mode.

no

The **no** keyword is used to disable CLI monitoring events in a call-control-profile for an MME service.

remove

The keyword **remove** Removes the event configuration from the call-control-profile.

Usage Guidelines

Use this command to configure monitoring events for MME service for users.

Example

The following command configures cli Monitoring Events in a call control profile:

`monitoring-events`

mps

This command under the Call Control profile configuration mode is configured to support Multimedia Priority Service (MPS) in the CS/EPS domain.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ remove ] mps [ cs-priority | eps-priority ] { subscribed | none }`

remove

The **remove** keyword deletes the existing configuration.

cs-priority

The keyword **cs-priority** configures support for priority service in the CS domain.

eps-priority

The keyword eps-priority configures support for MPS in the EPS domain.

subscribed

The keyword **subscribed** configures support for priority service in the CS/EPS domain.

none

The keyword **none** configures disables support for priority service in the CS/EPS domain.

Usage Guidelines

This CLI helps operator to override the MPS CS/EPS Subscription received from HSS. It allows the operator to prioritize the Mobile originating voice calls of a set of subscribers irrespective of them subscribed for MPS services or not. By default MME sets the value of "CS fallback indicator IE" as "CSFB High Priority" in the S1AP UE Context Setup/Modification if the MPS-CS-Priority bit is set in MPS-Priority AVP received from HSS.

Example

The following command is issued to set "CSFB High Priority" for "CS Fallback Indicator IE", in the S1AP UE Context Setup/Modification message:

```
[local]asr5x00(config-call-control-profile-call1)# mps cs-priority
subscribed
```

The following command is issued to set "CSFB Required" for "CS Fallback Indicator IE", in the S1AP UE Context Setup/Modification message:

```
[local]asr5000(config-call-control-profile-call1)# mps cs-priority none
```

msc-fallback-disable

Define all SRVCC causes for which the MME does not try sending PS-CS Request to a next available MSC, during an SRVCC handover, if the MME received one of the configured SRVCC causes in the PS-CS Response received from the first MSC.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description **[remove] msc-fallback-disable srvcc-cause** *cause*

remove

When added to the command, this command filter causes the MME to delete the specified SRVCC cause code definition.

srvcc-cause *cause*

This keyword configures an SRVCC cause code. If the MME receives this SRVCC cause code in a negative PS-CS Response from the first MSC tried in an SRVCC handover, then the MME sends SRVCC HO Failure and no other MSCs are tried. The *cause* must be any integer from 0 to 255, as defined in 3GPP TS 29.280.

Usage Guidelines This command can be repeated to configure more than one SRVCC cause.

This command is only applicable for PS-CS Requests and not for PS to CS complete messages.

This command is applicable for both statically configured MSC addresses (in an MSC Pool) and for MSC addresses returned by DNS.

If this command is not used to define SRVCC causes, then the MME will use default behavior to select the next MSC to retry PS-CS Request.

To confirm the MME's current configuration of SRVCC causes, use the **show call-control-profile full** command to generate output with a list of the 'MSC fallback disabled SRVCC causes'.

Example

Use a command similar to the following to configure one or more SRVCC cause codes. The following set of commands configures three SRVCC cause codes:

```
msc-fallback-disable srvcc-cause 8
msc-fallback-disable srvcc-cause 9
msc-fallback-disable srvcc-cause 10
```

nb-iot

This command enables Extended Discontinuous Reception (eDRX) and configures the respective parameters for NB-IoT subscribers on the MME.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description **nb-iot ignore-attach-without-pdn { edrx { ptw** *ptw_value* **edrx-cycle** *cycle_length_value* **| ue-requested } [dl-buf-duration [packet-count**

```
packet_count_value ] ] | mo-exception-data reporting-threshold-value
threshold_value  }
remove nb-iot {  edrx  | mo-exception-data }
```

ignore-attach-without-pdn

This keyword allows detach of Attach-Without-PDN UE after last PDN disconnect.

remove

This keyword disables the eDRX configuration on the MME for NB-IoT subscribers.

edrx

This keyword configures extended discontinuous reception parameters.

ptw *ptw_value*

This keyword configures the Paging Time Window (PTW) value. *ptw_value* must be an integer value in seconds. The allowed values are 2.56, 5.12, 7.68, 10.24, 12.80, 15.36, 17.92, 20.48, 23.04, 25.60, 28.16, 30.72, 33.28, 35.84, 38.40 and 40.96 seconds.

ue-requested

This keyword specifies the UE requested values of the Paging Time Window (PTW) and the eDRX cycle length received from the UE in the Attach Request or TAU Request message be accepted.

edrx-cycle *cycle_length_value*

This keyword configures the eDRX cycle length. *cycle_length_value* is an integer value in seconds. The allowed values are 5.12, 7.68, 10.24, 12.80, 15.36, 17.92, 20.48, 40.96, 81.92, 163.84, 327.68, 655.36, 1310.72, 2621.44, 5242.88 and 10485.76 seconds.

dl-buf-duration

This optional keyword sends downlink buffer duration in DDN ACK when unable to page UE.

packet-count *packet_count_value*

This optional keyword sends "DL Buffering Suggested Packet Count" in DDN ACK when unable to page UE. The *packet_count_value* is an integer value from 0 to 65535. If the *packet_count_value* is not configured locally, the subscription provided value for the *packet_count_value* is used. The subscription value can be 0 in which case the packet count IE will not be sent for that subscriber even if it is configured locally.

mo-exception-data

Configures NBIOT RRC Cause MO Exception Data counter.

reporting-threshold-value *value*

Specifies reporting threshold value. *value* Must be an integer from 1 to 50.

Usage Guidelines

Use this command to enable eDRX on the MME for NB-IoT subscribers. The operator can use this command for:

- Accept eDRX parameters: Paging Time Window (PTW) and eDRX cycle length value, from the UE
- Configure PTW and eDRX cycle length value
- Configure downlink buffer duration in DDN ACK when unable to page UE
- Configure "DL Buffering Suggested Packet Count" in DDN ACK when unable to page UE

When the eDRX feature is enabled on the MME, it pages the NB-IoT subscribers only at valid paging occasions. The MME sends the NB-IoT eDRX paging parameters to the eNodeB during paging. The operator can either configure the option to accept the UE requested values or configure the values using this command. This command is not enabled by default.

A similar CLI command is implemented for WB-EUTRAN subscribers. Both WB-UTRAN eDRX and NB-IoT eDRX parameters can be configured on the system for WB-UTRAN and NB-IoT subscribers.

See the *eDRX Support on the MME* feature chapter in the *MME Administration Guide* for more information.

Example

The following command configures the PTW and eDRX cycle length. The command also sends the downlink buffer duration in the DDN ACK along with a suggested packet count:

```
nb-iot edrx ptw 256 edrx-cycle 512 dl-buf-duration packet-count 10
```

network-feature-support-ie

Configures support for the IMS Voice over Packet-Switched indication and Homogenous Support of IMS Voice over PS indication.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
network-feature-support-ie ims-voice-over-ps [ not-supported | supported
 srvcc-ue-with-voice-domain-pref ]
remove network-feature-support-ie
```

remove

Disables support for Voice over PS.

ims-voice-over-ps [not-supported | supported]

Enables support for Voice over PS in all Tracking Areas.

not-supported: Configures the MME to add the "Homogenous Support of IMS Voice over PS Sessions" AVP to the S6a Update-Location-Request and Notify Request messages to the HSS, with the value set to "Not Supported". This indicates that IMS Voice over PS is **not** supported in **any** Tracking Areas.

supported: Configures the MME to add the "Homogenous Support of IMS Voice over PS Sessions" AVP to the S6a Update-Location-Request and Notify Request messages to the HSS, with the value set to "Supported". This indicates that IMS Voice over PS is supported in all Tracking Areas.

srvcc-ue-with-voice-domain-pref: IMS Voice Over PS not Supported for srvcc with cs voice preference UE only.

If the command is entered without either the **supported** or **not-supported** keywords, then MME indicates network feature support in the Attach Accept sent to the UE and includes the "Homogenous Support of IMS Voice over PS Sessions" AVP to the S6a Update-Location-Request and Notify Request messages sent to the HSS, with the value set to "Not Supported". This indicates that IMS Voice over PS is supported in all Tracking Areas.

Usage Guidelines

Use this command to include the "IMS Voice over PS" indication, thereby indicating support for IMS Voice over PS sessions for all Tracking Areas.

This command also configures whether to include the "Homogenous Support of IMS Voice over PS Sessions" indication as well as the included in the indication, either supported or not supported.

Example

The following command enables support for IMS Voice over PS on the MME:

```
network-feature-support-ie ims-voice-over-ps
```

network-initiated-pdp-activation

Configures the call control profile to perform two functions: (1) to enable or disable network-requested PDP context activation (NRPCA) for 3G attachments and (2) to define a failure cause code for inclusion in NRPCA-related reject messages.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
[ remove ] network-initiated-pdp-activation { allow primary | restrict
primary | secondary } access type { gprs | umts } { all |
location-area-list instance <instance> }
network-initiated-pdp-activation primary access type { gprs | umts } {
all | location-area-list instance <instance>  } failure-code code
```

network-initiated-pdp-activation secondary access type { gprs | umts } { all | location-area-list instance *<instance>* **} failure-code** *code*

remove

Including this keyword with the command, removes all configured values for the specified configuration.

allow

Allows network-initiated PDP context activation. This keyword must be followed by other parameters to indicate the limitations for allowing the NRPCA.

Allow is the default for NRPCA.

restrict

Restricts network-initiated PDP context activation. This keyword must be followed by other command parameters to indicate the limitations for restricting the NRPCA.

primary

Specifies that only network-initiated primary PDP context activations are to be allowed.

secondary

Specifies that only network-initiated secondary PDP context activations (NRSPCAs) are to be allowed.



Important The **secondary** keyword is visible and can be selected. However, NRSPCA functionality is only supported for Release 15.0 onwards.

all

Configures the SGSN to allow or to restrict NRPCA for calls within all location areas.

location-area-list instance *instance*

Selects a pre-defined list of location area codes (LACs) and allows/restricts the NRPCA procedure for calls within the listed area codes.

instance: Enter a list ID; an integer between 1 and 5.



Important Before using this keyword, ensure that the appropriate LAC information has been defined with the **location-area-list** command, also in this configuration mode.

failure-codes *code*

Enter an integer from 192 to 226 to identify the GTPP failure cause code (from 3GPP TS29.060, list below) to be included in the reject messages when NRPCA is restricted. If a failure cause code is not defined, the default value is 200 (service not supported).

- 192 - Non-existent
- 193 - Invalid message format
- 194 - IMSI not known
- 195 - MS is GPRS Detached
- 196 - MS is not GPRS Responding
- 197 - MS Refuses
- 198 - Version not supported
- 199 - No resources available
- 200 - Service not supported
- 201 - Mandatory IE incorrect
- 202 - Mandatory IE missing
- 203 - Optional IE incorrect
- 204 - System failure
- 205 - Roaming restriction
- 206 - P-TMSI Signature mismatch
- 207 - GPRS connection suspended
- 208 - Authentication failure
- 209 - User authentication failed
- 210 - Context not found
- 211 - All dynamic PDP addresses are occupied
- 212 - No memory is available
- 213 - Relocation failure
- 214 - Unknown mandatory extension header
- 215 - Semantic error in the TFT operation
- 216 - Syntactic error in the TFT operation
- 217 - Semantic errors in packet filter(s)
- 218 - Syntactic errors in packet filter(s)
- 219 - Missing or unknown APN
- 220 - Unknown PDP address or PDP type
- 221 - PDP context without TFT already activated
- 222 - APN access denied – no subscription
- 223 - APN Restriction type incompatibility with currently active PDP Contexts

- 224 - MS MBMS Capabilities Insufficient
- 225 - Invalid Correlation-ID
- 226 - MBMS Bearer Context Superseded

Usage Guidelines

Use this command to allow or restrict network-requested PDP context activation (NRPCA) based on access-type and location areas. NRPCA is used when there is downlink data at the GGSN for a subscriber, but there is no valid context for the already-established PDP address so the GGSN initiates an NRPCA procedure towards the SGSN.

This command can also be used to define the failure cause code that will be included in activation reject messages.

These commands can be repeated to define a unique set of NRPCA parameters for each access-type and each location area list.

The **T3385-timeout** and the **max-actv-retransmission** timers configure the retransmission timer and the number of retries for PDP context activation requests. Both of these timers are set in the SGSN service configuration mode.

The configuration for NRPCA can be viewed via the **show call-control-profile full name** *profile_name*. Statistics associated with NRPCA can be seen via the **show gmm-sm statistics** output and via the **show sgtpc statistics verbose** output.

Example

The following command changes the failure code for Reject messages from 200 (service not supported) to 205 (roaming restriction) for primary NRPCA for all GRPS access and all LACs:

```
network-initiated-pdp-activation primary access-type gprs all failure-code
 205
```

The following command enables network-initiated primary PDP context activation for UMTS calls from the LACs in location-area-list 1:

```
network-initiated-pdp-activation allow primary access-type umts
location-area-list instance 1
```

The following command restricts network-initiated primary PDP context activation for UMTS calls from the LACs in location-area-list 2:

```
network-initiated-pdp-activation restrict primary access-type umts
location-area-list instance 2
```

n1-mode 5gs-interworking-with-n26

Configures the call control profile to enable 5GS Interworking support using N26 interface.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > **call-control-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
n1-mode 5gs-interworking-with-n26 [ sgw-selection { s5-or-s8 | s11 [
ue-usage-type  ue-usage-type-val [ ue-usage-type-val+ ] ]} ]
      [ no | remove] n1-mode 5gs-interworking-with-n26 sgw-selections
ue-usage-type
      [ no ] n1-mode 5gs-interworking-with-n26 sgw-selection s11
      [ no ] n1-mode 5gs-interworking-with-n26 sgw-selection s11 [
ue-usage-type  ue-usage-type-val [ ue-usage-type-val+ ] ]
```

n1-mode 5gs-interworking-with-n26 [sgw-selection { s5-or-s8 | s11 [ue-usage-type ue-usage-type-val [ue-usage-type-val+]]}]

call-control-profile *profile_name*: Creates an instance of a call control profile. *profile_name* specifies the name of a call control profile entered as an alphanumeric string of 1-64 characters.

n1-mode : Configures interworking with 5GS for UEs supporting N1 mode.

5gs-interworking-with-n26 : Enables 5GS-EPS interworking with N26 interface.

no : Disables 5GS-EPS interworking with N26 interface.

remove: Removes the configuration from the Call Control Profile and the MME service configuration applies.

Usage Guidelines

Use this command to enable 5GS Interworking support using N26 interfac or remove the call control profiles.

Example

The following command indicates that if the N1 mode is configured and sgw-interface is configured with s11 and ue-usage-type in the Call Control Profile, then Ue-usage 130 gets removed using **no** option.

```
no n1-mode 5gs-interworking-with-n26sgw-selections ue-usage-type 130
```

override-arp-with-ggsn-arp

Enables or disables the ability of the SGSN to override an Allocation/Retention Priority (ARP) value with one received from a GGSN. If there is no authorized Evolved ARP received from the GGSN, by default the SGSN continues to use the legacy ARP included in the Quality of Service (QoS) Profile IE.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > **call-control-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description **[remove] override-arp-with-ggsn-arp**

remove

Adding the **remove** keyword to the command disables the override feature.

Usage Guidelines Enabling this function on the SGSN will allow the ARP sent by the GGSN, in CPCR / UPCR / UPCQ, to be applicable as an overriding value.

Example

Use this command to configure the SGSN to negotiate the ARP to be used as an overriding value:

override-arp-with-ggsn-arp

paging-priority

This command is configured to support sending of paging-priority value in S1AP paging-request message to the eNodeB. This command supports both PS and CS traffic types.

Product MME

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description **[remove] paging-priority cs** *cs_value*

From release 20.0 onwards the paging priority command is updated to support PS traffic:

[remove] paging-priority { cs { *cs_value* **| map emlpp-priority** *emlpp_value* **s1-paging-priority** *priority_value* **} | ps map arp** *arp_value* **s1-paging-priority** *priority_value*

remove

The **remove** keyword deletes the configured value of paging-priority to be sent to eNodeB for CS /PSpaging.

cs

This keyword is used to configure the value of paging-priority to be sent to eNodeB for Circuit Switched (CS) traffic. The paging priority value can be configured or it can be used to map the received value to the paging-priority.

cs_value

The paging priority *value* is an integer in the range "0" up to "7". Configuring a value of "0" disables sending of paging priority value to eNodeB.

ps

This keyword is used to configure the value of paging-priority to be sent to eNodeB for Packet Switched (PS) traffic. The paging priority value can be configured or it can be used to map the received value to the paging-priority.

map

This keyword is used to map the received value to paging-priority.

emlpp-priority

This keyword is used to configure priority value of enhanced Multi Level Precedence and Pre-emption service

emlpp_value

The emlpp value is an integer in the range "0" up to "7".

s1-paging-priority

This keyword is used to configure the value of paging-priority to be sent to eNodeB.

priority_value

The priority_value is an integer in the range "0" up to "7". Configuring a value of "0" disables sending of paging priority value to eNodeB.

arp

This keyword is used to configure the value of allocation and retention priority.

arp_value

The arp_value is an integer in the range "1" up to "15".

Usage Guidelines

This command helps operator to map eMLPP Priority / ARP to s1 ap paging priority to be sent to eNB. By default, sending of paging priority-ie in S1AP paging-request message to eNodeBs is enabled. The priority value received from the MSC/VLR is relayed to the eNodeB. A lower value of paging priority indicates a higher priority. Older values of paging priority are overridden by configuring new values. By default no mapping is enabled. From release 20.0 onwards this command is enhanced to emlpp-priority to paging-priority. It is used to configure the priority value of enhanced Multi Level Precedence and Pre-emption service. This command is also used to configure the Allocation Retention priority value for PS paging.

Example

The following command is issued to disable sending of paging priority value to the eNodeB:

```
[local]asr5x00(config-call-control-profile-call1)# paging-priority cs 0
```

The following command enables sending of paging priority value to the eNodeB, a priority value of "5" is configured using this command:

```
[local]asr5000(config-call-control-profile-call1)# paging-priority cs 5
```

pcscf-restoration

This command enables HSS-based P-CSCF Restoration procedure.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

```
[ remove ] pcscf-restoration
```

remove

The remove keyword disables HSS-based P-CSCF Restoration in the MME.

pcscf-restoration

The pcscf-restoration command in the above configuration enables HSS-based P-CSCF restoration. When enabled, MME supports P-CSCF Restoration on the S6a interface towards HSS for IMS PDN.

Usage Guidelines

The command **pcscf-restoration** aids in successful establishment of MT VoLTE calls when the serving P-CSCF is unreachable. By default, the above configuration is disabled. To select the method for P-CSCF Restoration, use the **pcscf-restoration** keyword in **apn-type ims** command under APN Profile Configuration mode.

Example

The following configurations enables HSS-based P-CSCF Restoration:

```
pcscf-restoration
```

pdp-activate access-type

Configures the PDP context activation option based the type of access technology.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
pdp-activate access-type { grps | umts } { all | location-area-list
instance instance } failure-code failure_code
default pdp-activate access-type { grps | umts } { all | location-area-list
 instance instance } failure-code code
```

default

Resets the configuration to system default values for PDP context activation request.

{ grps | umts }

Specifies the access technology type for PDP context activation.

- **gprs**: Enables access type as GPRS.
- **umts**: Enables access type as UMTS.

all

Default: allow

Configures the system to allow the creation of all PDP context activation requests received from MS.

location-area-list instance *instance*

Specifies the location area instance for which to create a PDP context as an integer from 1 through 5. The value must be an already defined instance of a location area code (LAC) list created via the **location-area-list** command.

failure-code *code*

Specifies the failure code for PDP context activation as an integer from 8 through 112. Default: 8

Usage Guidelines

Use this command to configure this call control profile to allow GPRS/UMTS access through PDP context activation request from MS.

Example

The following command configures the system to create the PDP context for requests from MS for GPRS access with location area list instance *2* and failure-code *5*:

```
pdp-activate access-type gprs location-area-list 2 failure-code 5
```

pdp-activate allow

Configures the system to allow the PDP context activation based on the type of access technology.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ no ] pdp-activate allow access-type { grps | umts } location-area-list instance` *`instance`*

no

Removes the configured permission to create PDP context on request of PDP context activation from MS for an access type.

access-type { grps | umts }

Specifies the access technology type for PDP context activation.

- **gprs**: Enables access type as GPRS.
- **umts**: Enables access type as UMTS.

location-area-list instance *instance*

Specifies the location area instance to create PDP context.

instance must be an integer from 1 through 5. The value must be an already defined instance of a location area code (LAC) list created via the **location-area-list** command.

Usage Guidelines

Use this command to configure this call control profile to allow GPRS/UMTS access through PDP context activation request from MS.

Example

The following command configures the system to allow the PDP context activation for GPRS access type with location area list instance *2*:

```
pdp-activate allow access-type gprs location-area-list instance 2
```

pdp-activate restrict

Configures the system to restrict the PDP context activation based on the type of access technology.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

[no | remove] { { access-type { gprs | umts } { all | location-area-list instance *instance* **} } | { pdp-type { all | dual-ipv4v6 | ipv4 | ipv6 | ppp } { access-type { gprs | umts } { all | location-area-list instance** *instance* **} } } | { secondary-activation access-type { gprs | umts } { all | location-area-list instance** *instance* **} } }**

no | remove

Either of these prefixes removes the previously configured restriction on PDP context activation and returns the 'allow' default.

access-type { grps | umts }

Specifies the access technology type for which to restrict PDP context activation.

- **gprs**: Enables access type as GPRS.
- **umts**: Enables access type as UMTS.
- **all**: Configures the system to restrict all PDP context activation requests from the MS.
- **location-area-list instance** *instance*: Specifies the location area instance to restrict PDP context activation, where *list_id* must be an integer from 1 through 5. The value must be an already defined instance of a location area code (LAC) list created with the **location-area-list** command.

pdp-type

Sets the configuration to restrict PDP activation based on the requested PDP type.

To restrict more than one type of PDP, the command must be reissued for each PDP type.

- **all**: restricts activation of all types PDP.
- **dual-ipv4v6**: restricts activation when dual-IPv4v6 PDP contexts are requested.
- **ipv4**: restricts activation when IPv4 PDP contexts are requested.
- **ipv6**: restricts activation when IPv6 PDP contexts are requested.
- **ppp**: restricts activation when PPP PDP contexts are requested.

secondary-activation

Restricts the SGSN, based on the access-type, so that secondary PDP contexts are not created when receiving the PDP Context Activation Request from the MS.

Usage Guidelines

Use this command to configure this call control profile to restrict PDP context activation requests from MS.

Example

The following command configures the system to restrict the PDP context activation for request from 2G MS with location area list instance *2*:

```
pdp-activate restrict access-type gprs location-area-list instance 2
```

The following command configures the SGSN to restrict PDP context activation for requests from 3G MS if their PDP-type is IPv4. The second command restricts based on PDP-type IPv6.

```
pdp-activate restrict pdp-type ipv4 access-type umts all
pdp-activate restrict pdp-type ipv6 access-type umts location-area-list
instance 1
```

pdn-type-override

Configures the MME or the SGSN to override the requested packet data network (PDN) type based on the inbound roamer PLMN, and re-assigns the UE to an IPv4-only or IPv6-only PDN. This override can be applied based on the type of access technology.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
pdn-type-override { ipv4-only | ipv4v6 { ipv4 | ipv6 } [ access-type {
eps | grps | umts } ] }
remove pdn-type-override [ access-type { eps | grps | umts } | ipv4-only
 ]
```

remove

Removes the configured PDN type override.

ipv4-only

Enables MME to allow only IPv4 addresses to a PDN connection.

The default behavior allows PDN to have IPv6 addresses when subscription allows it.

ipv4v6 { ipv4 | ipv6 }

Defines the PDN type (IPv4 or IPv6) to which UEs should be restricted.

access-type { eps | grps | umts }

Specifies the access technology type to which the override is applied.

- **eps**- enables PDN override for EPS access type.
- **gprs** - enables PDN override for GPRS access type.
- **umts** - enables PDN override for UMTS access type.

If this keyword is not included, then all three access types can have the PDN type overridden.

Usage Guidelines

Use this command to configure the call control profile to override the requested packet data network (PDN) type and re-assign the UE to a different PDN type. Optionally, it is possible to filter the override based on access technology.

Important This call control profile becomes valid only when it is associated with an operator policy using the **associate** command in the Operator Policy configuration mode.

Example

The following command configures the system to override the requested PDN type and assign a UE to an IPv4-only PDN if the UE's access technology is GPRS:

```
pdn-type-override ipv4v6 ipv4 access-type gprs
```

peer-mme

Configures a peer MME address. S4-SGSN operators can use this command if they wish to bypass DNS resolution to obtain the MME address.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

peer-mme { mme-groupid *<lac val>* **mme-code** *<rac value>* **| tac** *tac* **} prefer { fallback-for-dns | local } address {** *<ipv4_address>* **|** *<ipv6_address>* **} interface**

```
 { gn [ s3 ] | s3 [ gn ] }
remove peer-mme { mme-groupid <lac val> mme-code <rac value> | tac  tac }
address [ <ipv4_address> | <ipv6_address> [ interface { gn [ s3 ] | s3 [ gn ]
} ]
```

remove

Removes a specified peer MME from the call control profile. The **interface** keyword is optional. If it is not used, the entire interface will be deleted.

mme-groupid *<lac val>*

Specifies the location area code value of the peer MME. The MME group ID of the peer MME maps to the LAC value when GUTI is converted to P-TMSI.

<lac val> must be an integer from 1 to 65535.

mme-code *<rac value>*

Specifies the routing area code value of the peer MME. The MME code of the peer MME maps to the RAC value when GUTI is converted to P-TMSI.

<rac value> must be an integer from 0 to 255.

tac *tac*

Optional. Specifies the Tracking Area Code (TAC) of the target eNodeB that is used for UTRAN to E-UTRAN (SGSN to MME) SRNS relocation across the S3 interface. Valid entries are 1 to 65535. This setting applies only if SRNS relocation first has been configured via the **srns-inter** and/or **srns-intra** commands in *Call Control Profile Configuration Mode*.

prefer { fallback-for-dns | local }

Indicates whether to use a DNS query to obtain the address or to use a locally configured peer MME address:

- **fallback-for-dns** - Instructs the SGSN to perform a DNS query to get the IP address of the peer MME. If the DNS query fails, then the IP address configured with this command is used.
- **local** - Use the locally configured address for the MME address.



Important If the **prefer** command is used to change an existing peer-mme configuration (with the same LAC and RAC) from **fallback-for-dns** to **local**or from **local** to **fallback-for-dns**, the new setting overwrites the previously configured setting for all interfaces.

address { *ipv4_address | ipv6_address* }

Specifies the IP address of the peer MME. Currently, the IPv6 address option is not supported on the S4-SGSN.

ipv4 must be in standard dotted-decimal notation.

interface { gn [s3] | s3 [gn] }

Specifies the interface to use for communication between the SGSN and the peer MME:

- **gn**: Use the Gn interface between the S4-SGSN and the MME in the LTE network.
- **s3**: Use the S3 interface between the S4-SGSN and the MME in the LTE network. This is the default setting.

Usage Guidelines

Use this command to instruct the S4-SGSN how to determine a peer MME address, via DNS or local configuration. For a local address, use this command to configure the peer MME address.

This command also sets the interface type to be used between the peer MME and the SGSN.

Example

The following command configures LAC/RAC *111/22* for the peer MME and instructs the SGSN to use the MME's locally configured IPv4 address of *209.165.200.225*and an S3 interface between the MME and the SGSN.

```
 peer-mme mme-groupid 111 mme-code 22 prefer local address 1.1.1.1
interface s3
```

peer-msc

Enables/disables weight-based selection of a peer MSC during MSC lookup. By default, this functionality is disabled.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

```
peer-msc interface-type sv weight
remove peer-msc interface-type sv weight
```

remove

Deletes the weight-based selection for peer-MSC configuration if it has been enabled using this command and returns to the default of preference-based selection of a peer MSC.

Usage Guidelines

This command enables the operator to override the default behavior and define weight-based selection of a peer-MSC during MSC lookup to facilitate 'weight' based load balancing for the MME's Sv interface.

Example

Disable weight-based MSC selection when it has been configured:

```
remove peer-msc interface-type sv weight
```

peer-nri-length

Enables the SGSN to use NRI-FQDN-based DNS resolution for non-local RAIs when selection of the call control profile is based on the old-RAI and the PLMN Id of the RNC (for 3G subscribers) or BSC (for 2G subscribers) where the subscriber originally attached. The SGSN also supports RAI based query when NRI based query fails.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

peer-nri-length *length* **[rai-fqdn-fallback] [nri-for-inter-pool-address]**
remove peer-nri-length [rai-fqdn-fallback] [nri-for-inter-pool-address]

remove

Deletes the NRI length configuration for the non-local RAIs and the SGSN sends RAI-FQDN-based DNS resolution.

length

This defines the NRI length for the peer SGSN and enables use of NRI-FQDN-based DNS resolution for non-local RAIs. This variable allows for an integer from 1 to 10.

rai-fqdn-fallback

This keyword allows the operator to configure SGSN support for RAI based query when NRI based query fails. By default this keyword is disabled.

nri-for-inter-pool-address

This keyword enables NRI-only based static peer-sgsn address configuration for inter-pool. If this keyword is configured and if the NRI value derived from the PTMSI received in the RAU request matches the NRI value configured in the CLI **sgsn-address nri** *nri-value* **prefer local address ipv4** *addr* **interface** *name*, the static sgsn-address configured in the above CLI will be used to initiate the context request. Otherwise, a DNS query will be initiated to fetch the peer-sgsn address.

Usage Guidelines



Important

- This feature is supported only for 3G subscribers until Release 15.0.
- This feature is also supported for 2G subscribers from Release 16.0 onwards.

Important Fall back to RAI based query when NRI based query fails is not supported in the following scenarios:

- 2G Context Request and Identification Request are not supported.
- S4 support of this extension for all applicable scenarios are not supported.

The command enables the SGSN to perform DNS query with an NRI when RAU comes from an SGSN outside the pool. The SGSN uses NRI-FQDN-based DNS resolution for the non-local RAIs for 3G and 2G subscribers in place of RAI-FQDN-based DNS resolution.

This functionality is applicable in situations for either inter- or intra-PLMN when the SGSN has not chosen a local NRI value (configured with SGSN Service commands) other than local-pool-rai or nb-rai. This means the RAI (outside pool but intra-PLMN) NRI length configured here will be applicable even for intra-PLMN with differently configured NRI lengths (different from the local pool).

This functionality is not applicable to call control profiles with an associated MSIN range as ccprofile selection is not IMSI-based. When this feature is enabled, the selection of the ccprofile is based on the old-RAI and the PLMN Id (if configured) of the RNC (for 3G subscribers) or BSC (for 2G subscribers) where the subscriber originally attached.

When the CLI keyword **nri-for-inter-pool-address** is enabled the static SGSN address configured in the command **sgsn-address** is used for inter-pool Attaches/RAUs if the NRI value configured in the CLI **sgsn-address** matches the NRI value calculated from the PTMSI received in the attach/RAU message. If the keyword **nri-for-inter-pool-address** is not enabled, a DNS query is sent out to fetch the peer-sgsn address. This enhancement is applicable for both 2G and 3G scenarios. The primary advantage of this enhancement is that the DNS query for inter-pool 3G or 2G Attach/RAU scenarios is avoided.

Example

The following command is used to configure a peer-nri-length of *3*, with support for RAI based query when NRI based query fails:

```
peer-nri-length 3 rai-fqdn-fallback
```

plmn-protocol

Configures the protocol supported by the PLMN (Public Land Mobile Network).

Product MME

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

plmn-protocol plmnid mcc *mcc_num* **mnc** *mnc_num* **{ s5-protocol | s8-protocol } { gtp | pmip }**
remove plmn-protocol plmnid mcc *mcc_num* **mnc** *mnc_num*

remove

Deletes the definition from the call control profile configuration.

plmn-id mcc *mcc_num* mnc *mnc_num*

Identifies the PLMN by MCC (mobile country code) and MNC (mobile network code).

mcc_num: Enter a 3-digit integer from 100-999.

mnc_num: Enter a 2- or 3-digit integer from 00 to 999.

s5-protocol | s8-protocol

Select which protocol – S5 or S8 – that controls the identified PLMN.

gtp | pmip

Select the protocol variant - GTP or PMIP - that controls functionality for the identified PLMN.

Usage Guidelines

Use this command to identify a particular PLMN and, at a higher level, its operational characteristics.

Example

The following command instructs the MME to use PLMN MCC423.MNC40.GPRS with PMIP under S8 Protocol:

```
plmn-protocol plmnid mcc 423 mnc 40 s8-protocol pmip
```

prefer subscription-interface

Selects the specified subscription interface (Gr or S6d) if both interface types are associated with a call-control-profile. Use of this command requires an S6d license. The SGSN also allows selection of S6d interface only if the UE is EPC capable. The keyword **epc-ue** supports the selection of HSS interface only for EPC capable subscribers.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
prefer subscription-interface { hlr | hss  [ epc-ue ] }
remove prefer subscription-interface
```

remove

Removes the preferred subscription-interface for the call control profile.

hlr

Selects the HLR Gr interface.

hss

Selects the HSS S6d interface.

epc-ue

Configure this keyword to select the HSS interface for EPC capable subscribers. For other subscribers the MAP interface will be selected. This keyword will be applicable only when both MAP and HSS interfaces are configured in the Call-control profile. If this keyword is not configured then SGSN follows existing logic for interface selection. The interface selection based on UE capability is done only at the time of Attach / new SGSN RAU / SRNS. Once the interface is selected, the subscriber remains in same interface till the UE moves out of the SGSN.

Usage Guidelines

Use of this command requires an S6d license.

The SGSN provides a mechanism to associate a MAP service with call control profile. It is possible that both MAP service and HSS peer service are associated with the call control profile. If the interface preference selected is "hlr", the MAP protocol is used to exchange messages with the HLR. If the interface preference selected is "hss", the Diameter-protocol is used to exchange messages with the HSS.

Example

The following command specifies that "hss" for S6d is selected as the subscription-interface:

```
prefer subscription-interface hss
```

psm

This command is used to configure UE Power Saving Mode parameters.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

[remove] psm {ue-requested [dl-buf-duration [packet-count *packet_value* **]]| t3324-timeout** *t3324_value* **t3412-extended-timeout** *t3412_ext_value* **[dl-buf-duration [packet-count** *packet_value* **]]}**

remove

The **remove** keyword deletes the existing power saving mode configuration.

ue-requested

Use this keyword when UE requested values for Active and Extended Periodic timers are to be accepted.

t3324-timeout *t3324_value*

Use this keyword to configure the T3324 active timer value.

t3324_value

The T3324 active timer is an integer value in the range 0 up to 11160 seconds.

t3412-extended-timeout *t3412_ext_value*

Use this keyword to configure the t3412 Extended timer value.

t3412_ext_value

The T3412 extended timer is an integer value in the range 0 up to 35712000 seconds.

dl-buf-duration

Use this keyword to Send Downlink Buffer Duration in DDN ACK when unable to page UE.

packet-count *packet_value*

Use this keyword to send 'DL Buffering Suggested Packet Count' in DDN ACK when unable to page UE.

packet_value

The *packet_value* is an integer value from 0 up to 65535.

Usage Guidelines

Use this CLI command to configure the T3324 active and T3412 extended timers. The CLI also provides an option to either accept UE requested values or HSS subscribed values or MME configured values for these timers. This command is used to configure either to send or not send the Downlink Buffer Duration in DDN Ack, the DDN Ack Optional IE "Downlink Suggested Packet Count". The CLI option **dl-buf-duration [packet-count** *packet_value* **]** is used to optionally configure either to send or not send the downlink buffer duration in DDN Ack, the DDN Ack Optional IE "Downlink Suggested Packet Count" can also be configured. If this option is not configured and not sent in subscription, MME does not send IE in DDN reject. If the **packet-count** value is not configured locally, the subscription value for **packet-count** is used. The subscription value can be "0", in this case the packet count IE will not be sent for that subscriber even if it is configured locally. If the T3324 active and T3412 extended timers are locally configured these values are always used. If the **psm** command is configured to use the UE requested values for Active and Extended Periodic timers the UE requested values are accepted, but in case if the UE does not request T3412 extended timer, then the value available in subscription data are used for Extended Periodic timer. If the values are not available in the subscription data then the values configured under the MME service are used .

As per latest version of 3GPP TS 24.008, the maximum value of T3412 extended timer can be "320*31" hours that is "35712000" seconds. Due to MME constraints on timer implementation the T3412 extended timer is restricted to 1050 hours that is "3780000" seconds. However, the nearest usable value of this timer as 3GPP TS 24.008 GPRS Timer 3 is 960 hours (320 * 3) that is 3456000 seconds.

Example

Use the following command to enable power saving mode and to accept UE requested values for T3324 and T3412 timers.

psm ue-requested

Use the following command enable UE power saving mode and provide operator desired values for T3324 and T3412 timers:

psm t3324-timeout *100* **t3412-extended-timout** *5000*

Use the following command to enable PSM and accept UE requested values for T3324 and T3412 timers. This command also specifies the 'DL Buffering Suggested Packet Count' in DDN ACK when unable to page UE.

psm ue-requested dl-buf-duration packet-count *100*

In the following example, PSM is enabled and values of T3324 and T3412 timers are specified along with configuring a packet count in DDN ACK:

psm t3324-timeout *1000* **t3412-extended-timeout** *5000* **dl-buf-duration packet-count** *100*

ptmsi-reallocate

Defines P-TMSI reallocation for Attach Requests, RAU Request, and Service Requests.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

ptmsi-reallocate { attach | frequency *frequency* **| interval** *interval* **| routing-area-update [update-type] | service-request [service-type] } [access-type { gprs | umts }]**
ptmsi-reallocate routing-area-update [access-type { gprs | umts } | frequency *frequency* **| update-type { combined-update | imsi-combined-update | periodic | ra-update } [access-type { gprs | umts } | frequency** *frequency* **]]**
ptmsi-reallocate service-request [frequency *frequency* **| service-type { data | page-response | signaling } [frequency** *frequency* **]]**

```
[ no | remove ] ptmsi-reallocate { attach | frequency | interval |
routing-area-update [ update-type { combined-update | imsi-combined-update
 | periodic | ra-update } [ access-type { gprs | umts } ] ] |
service-request [ service-type { data | page-response | signaling } ] }
[ access-type { gprs | umts } ]
```

no

Disables the authentication procedures configured for the specified P-TMSI reallocation configuration in the call control profile.

remove

Deletes the defined authentication procedures for the specified P-TMSI reallocation configuration from the call control profile configuration file.

attach

Enables/disables P-TMSI reallocation for Attach with local P-TMSI.



Important IMSI or inter-SGSN Attach is not configurable and will always be reallocated.

access-type *type*

One of the following must be selected to reallocate on the basis of the type of network access:

- **gprs**
- **umts**

This keyword can be used in combination with other keywords to refine the reallocation configuration.

frequency *frequency*

Defines frequency of the reallocation based on the number of messages skipped. If the frequency is set for 1, then the SGSN skips 1 message and then reallocates on receipt of the 2nd (alternate) request message, essentially reallocating the P-TMSI every time. If the frequency is set for 12, then the SGSN skips reallocation for 12 messages and reallocates on receipt of the 13th request message. This keyword can be used in combination with other keywords to refine the reallocation configuration.

frequency must be an integer from 1 to 50.

By default, frequency is not defined and, therefore, reallocation is done for every request message and none are skipped.

interval *minutes*

Enter an integer between 1 and 1440 to define the time interval (in minutes) for skipping the service/RAU/attach request message procedure.

routing-area-update [update-type]

Enables/disables P-TMSI reallocation for RAU (routing area update) with local P-TMSI. To refine the reallocation configuration, include one of the optional types of updates to limit reallocation:

- **combined-update**
- **imsi-combined-update**
- **periodic**
- **ra-update**



Important Inter-SGSN RAU will always be reallocated.

service-request [service-type]

Enables/disables P-TMSI reallocation for Service Requests. To refine the Service-Request reallocation configuration, include on of the optional service-types to limit the reallocation:

- **data**
- **page-response**
- **signaling**

Usage Guidelines By default, reallocation is not enabled. Use this command to enable P-TMSI reallocation for Attach Requests, RAU Request, and Service Requests. Fine-tune the reallocation configuration according to frequency, interval, or access-type.

Example

The following command configures the SGSN to perform P-TMSI reallocation upon receiving 2G Attach Requests

```
ptmsi-reallocate attach access-type gprs
```

The following command configures the SGSN to disable all previously defined P-TMSI reallocations based on the combined criteria of interval and 3G requests:

```
no ptmsi-reallocate interval access-type umts
```

ptmsi-signature-reallocate

Enables P-TMSI signature reallocation during Attach/RAU procedures.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > **call-control-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
ptmsi-signature-reallocate { attach | frequency frequency | interval interval
  | ptmsi-reallocation-command | routing-area-update [ update-type ] } [
 access-type { gprs | umts } | frequency frequency ]
ptmsi-signature-reallocate routing-area-update [ access-type { gprs |
umts } | frequency frequency | update-type { combined-update |
imsi-combined-update | periodic | ra-update } ] [ access-type { gprs |
umts } | frequency frequency ]
[ no | remove ] ptmsi-signature-reallocate { attach | frequency | interval
 | routing-area-update [ update-type { combined-update |
imsi-combined-update | periodic | ra-update } ] } [ access-type { gprs |
 umts } ]
```

no

Disables the authentication procedures configured for the specified P-TMSI signature reallocation configuration in the call control profile.

remove

Deletes the defined authentication procedures for the specified P-TMSI signature reallocation configuration from the call control profile configuration file.

attach

Enables/disables P-TMSI signature reallocation for Attach with local P-TMSI.

access-type *type*

One of the following must be selected to reallocate on the basis of the type of network access:

- **gprs**
- **umts**

This keyword can be used in combination with other keywords to refine the reallocation configuration.

frequency *frequency*

Defines 1-in-N selective reallocation. If the frequency is set for 12, then the SGSN skips reallocation for the first 11 messages and reallocates on receipt of the twelfth request message.

frequency must be an integer from 1 to 50.

This keyword can be used in combination with other keywords to refine the reallocation configuration.

interval *minutes*

Enter an integer between 1 and 1440 to define the time interval (in minutes) for skipping the service/RAU/attach request message procedure before performing a P-TMSI signature reallocation.

ptmsi-reallocation-command

Includes P-TMSI signature reallocation as a part of the P-TMSI reallocation configuration.

routing-area-update [update-type]

Enables/disables P-TMSI signature reallocation for RAU (routing area update) with local P-TMSI. To refine the reallocation configuration, include one of the optional types of updates to limit reallocation:

- **combined-update**
- **imsi-combined-update**
- **periodic**
- **ra-update**

Usage Guidelines

By default, P-TMSI signature reallocation is disabled. This command allows the operator to configure when the P-TMSI signature is reallocated.

Example

The following command configures the SGSN to reallocate the P-TMSI signature for every third UMTS attach procedure:

```
ptmsi-signature-reallocate attach frequency 3 access-type umts
```

The following command configures the SGSN to reallocate the P-TMSI signature for every seventh GPRS periodic RAU procedure:

```
ptmsi-signature-reallocate routing-area-update uupdate-type periodic
frequency 7 access-type gprs
```

The following command removes all configuration instances for reallocating the P-TMSI signature based on intervals and UMTS access:

```
remove ptmsi-signature-reallocate interval access-type umts
```

qos

Configures the quality of service (QoS) parameters to be applied.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
qos { gn-gp | ue-ambr }
qos gn-gp { arp high-priority priority medium-priority priority | pre-emption
 { capability { may-trigger-pre-emption | shall-not-trigger-pre-emption
} | vulnerability { not-pre-emptable | pre-emptable }
qos ue-ambr { max-ul mbr_up max-dl mbr_dl | prefer-as-cap {
both-hss-and-local  minimum | local } }
qos ue-ambr { max-ul mbr_up max-dl mbr_dl | prefer-as-cap both-hss-and-local
 { local-when-subscription-not-available | minimum |
subscription-exceed-reject [ emm-cause-code [ eps-service-disallowed |
eps-service-not-allowed-in-this-plmn | no-suitable-cell-in-tracking-area
 | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area |
tracking-area-not-allowed ] ] }
remove qos { gn-gp | ue-ambr }
```

remove

Deletes the configuration from the call control profile.

gn-gp

Configures Gn-Gp pre-release 8 ARP and pre-emption parameters.

arp

Maps usage of ARP (allocation/retention policy) high-priority (H) and medium-priority (M):

- **high-priority** *priority*: Enter an integer from 1 to 13.
- **medium-priority** *priority*: Enter an integer from 2 to 14.

pre-emption

Defines the pre-emption/vulnerability criteria for PDP Contexts imported from SGSN on Gn/Gp:

- **capability**
  - **may-trigger-pre-emption**: PDP Contexts imported from Gn/Gp SGSN may preempt existing bearers.
  - **shall-not-trigger-pre-emption**: PDP Contexts imported from Gn/Gp SGSN shall not preempt existing bearers.
- **vulnerability**
  - **not-pre-emptable**: PDP Contexts imported from Gn/Gp SGSN are not vulnerable to pre-emption.
  - **pre-emptable**: PDP Contexts imported from Gn/Gp SGSN are vulnerable to pre-emption.

ue-ambr

This keyword enables the operator to configure either the aggregate maximum bit rate stored on the UE (UE AMBR) or select the preferred uplink and downlink QoS cap values.

Important The SGSN only supports the **ue-ambr** keyword beginning in Release 16.

Configures the aggregate maximum bit rate that will be stored on the UE (user equipment).

- **max-ul** *mbr_up*: Defines the maximum bit rate for uplink traffic.

  mbr_up: Enter a value from 1 to 1410065408 (StarOS release 16.1 and higher), or 0 to 1410065408 (Kbps).

  In StarOS 21.8 and later releases: *mbr_up* must be an integer from 0 to 4000000000000 (4 Tbps).

- **max-dl** *mbr_down*: Defines the maximum bit rate for downlink traffic.

  mbr_down: Enter a value from 1 to 1410065408 (StarOS release 16.1 and higher), or 0 to 1410065408 (Kbps).

  In StarOS 21.8 and later releases: *mbr_down* must be an integer from 0 to 4000000000000 (4 Tbps).

prefer-as-cap both-hss-and-local { local-when-subscription-not-available | minimum | subscription-exceed-reject [emm-cause-code [eps-service-disallowed | eps-service-not-allowed-in-this-plmn | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed]] }

This set of options is only available on the MME.

Specifies the QoS cap value to use.

- **local-when-subscription-not-available**: Use the locally configured values if the Home Subscriber Server (HSS) does not provide QoS bit rate values.
- **minimum**: Use the lower of either the locally configured QoS bit rate or the HSS-provided QoS bit rate. This will override the HSS provided values if it is greater than the locally configured values, or if the HSS does not provide any values.
- **subscription-exceed-reject**: If the requested QoS bit rate exceeds the locally configured value, reject the PDN connection.
- **emm-cause-code**: Specifies the EPS Mobility Management (EMM) cause code to return when the PDN connection is rejected.
  - **eps-service-disallowed** - Default
  - **eps-service-not-allowed-in-this-plmn**
  - **no-suitable-cell-in-tracking-area**
  - **plmn-not-allowed**
  - **roaming-not-allowed-in-this-tracking-area**
  - **tracking-area-not-allowed**

prefer-as-cap { both-hss-and-local minimum | local }

This set of options is only available on the SGSN.

Specifies the QoS cap value to use:

- **both-hss-and-local minimum** Use the lower of either the locally configured QoS bit rate or the Home Subscriber Server (HSS)-provided QoS bit rate.
- **local** Use the locally configured QoS bit rate.

Usage Guidelines

Use this command to configure the QoS parameters for the call control profile for either the MME or the SGSN.

On an S4-SGSN, this command ensures proper QoS parameter mapping between the S4-SGSN and EPC UEs, SGWs and PGWs:

- Map EPC ARP parameters to pre-release 8 ARP (Gn/Gp ARP) used during S4-SGSN-to-Gn SGSN call handovers.
- Map ARP parameters received in a GPRS subscription from the HLR to EPC ARP parameters if:
  - The S4 interface is selected for an EPC capable UE, and
  - The UE has only a GPRS subscription (but no EPS subscription) in the HLR / HSS.

Example

Configure the Gn/Gp interface ARP priority values:

```
qos gn-gp arp high-priority 2 medium-priority 3
```

rau-inter

Defines acceptable parameters for inter-SGSN routing area updates.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
rau-inter { accept use-auth-vector | access-type gprs { all |
location-area-list instance instance_id | routing-area-list instance
instance_id } { failure-code fail_code | user-device-release { before-r99 |
r99-or-later } failure-code fail_code } } | allow accept access-type gprs
location-area-list instance instance_id | avoid-s12-direct-tunnel |
ctxt-xfer-failure | exclude-uteid-in-mbr | ignore-peer-context-id |
peer-sgsn-addr-resolution-failure failure-code fail_code | restrict
access-type { { gprs | umts } { all | location-area-list instance instance_id
 | routing-area-list instance instance_id } }
default rau-inter ( accept use-auth-vector | access-type { { gprs | umts
 } { all | location-area-list instance instance_id | routing-area-list
instance instance_id } user-device-release { before-r99 | r99-or-later }
failure-code fail_code } } | avoid-s12-direct-tunnel |  failure-code fail_code
 | ignore-peer-context-id | peer-sgsn-addr-resolution-failure failure-code
 fail_code }
```

no rau-inter (accept use-auth-vector | allow access-type { gprs | umts } location-area-list instance *instance_id* **| routing-area-list instance** *instance_id* **| ignore-peer-context-id | restrict access-type { gprs | umts } { all | location-area-list instance** *instance_id* **| routing-area-list instance** *instance_id* **} }**
remove rau-inter { avoid-s12-direct-tunnel | exclude-uteid-in-mbr | ctxt-xfer-failure}

no

Including **no** as part of the command structure disables the values already configured for parameters specified in the command.

default

Resets the configuration of specified parameters to system default values.

remove

remove can only be used with the **avoid-s12-direct-tunnel** keyword to erase a configuration instructing the SGSN to avoid establishment of a direct tunnel for S12 interfaces.

accept use-auth-vector

Sets the SGSN to accept using the authorization vector.

allow access-type

Including this keyword with one of the following options, configures the SGSN to allow MS/UE with the identified access-type extension to be part of the intra-RAU procedure.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System

avoid-s12-direct-tunnel

Enables the operator to modify the Call-Control profile default configuration and instructs the SGSN to avoid establishment of a direct tunnel for S12 interfaces.

This keyword is only supported for configuration of S12 interfaces.

ctxt-xfer-failure *fail_code*

Configure or removes a GMM failure cause code to be sent in a RAU Reject to the UE due to context transfer failures.

fail_code For acceptable options, refer to the failure-codes listed below.

remove filter works with this keyword to erase the context transfer failure cause code definition.

exclude-uteid-in-mbr

By default, the SGSN sends user plane fully qualified tunnel end-point identifier (UTEID) in the Modify Bearer Reqeust (MBR). If RABs are not yet established, this keyword disables or enables the sending of the

UTEID in the MBR during a new SGSN RAU over S16/S3. This keyword is in compliance with 3GPP TS 23.401 v11.8.0.

ignore-peer-context-id

Sets the SGSN to ignore the peer's context-ID and replace with PDP context-ID information based on the HLR subscription.

peer-sgsn-addr-resolution-failure *fail_code*

Configure or remove a GMM failure cause code to be sent in a RAU Reject to the UE due to peer address resolution failures at the SGSN.

fail_code Enter either 9 (MSID cannot be derived by the network) or 10 (Implicitly detached) to identify the GMM failure cause code.

remove filter works with this keyword to erase the failure code definition.

restrict access-type

Including this keyword-set with one of the following options, configures the SGSN to restrict MS/UE with the identified access-type extension from the inter-RAU procedure.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System

all

all - adding this option to the keyword determines that the failure cause code will be applicable to all location areas.

location-area-list instance *instance_id*

instance_id must be an integer between 1 and 5. The value must be an already defined instance of a location area code (LAC) list created with the **location-area-list** command.

routing-area-list instance *instance_id*

Instructs the SGSN to apply the command action to a specific routing area list. Routing area lists should already have been created with the **routing-area-list** command.

instance_id must be an integer from 1 to 5.

failure-code *fail-code*

Specify a GSM Mobility Management (GMM) failure cause code to identify the reason an inter SGSN RAU does not occur. This GMM cause code will be sent in the reject message to the MS.

fail-code must be an integer from 2 to 111. Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME

- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 -MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

user-device-release { before-r99 | r99-or-later } failure-code *code*

Default: Disabled

Enables the SGSN to reject an Inter-RAU procedure based on the detected 3GPP release version of the MS equipment and selectively send a failure cause code in the reject message. The SGSN uses the following procedure to implement this configuration:

1. When Attach Request is received, the SGSN checks the subscriber's IMSI and current location information.
2. Based on the IMSI, an operator policy and call control profile is found that relates to this Attach Request.

3. call control profile is checked for access limitations.
4. Attach Request is checked to see if the revision indicator bit is set
   - if not, then the configured common failure code for reject is sent;
   - if set, then the 3GPP release level is verified and action is taken based on the configuration of this parameter

One of the following options must be selected and completed:

- **before-r99**: Indicates the MS would be a 3GPP release prior to R99 and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

- **r99-or-later**: Indicates the MS would be a 3GPP Release 99 or later and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

Usage Guidelines Use this command to configure the restrictions and function of the inter-RAU procedure.

Example

Configure default inter-RAU settings for Edge calls from subscribers on location-area-list no. *1*:

```
default rau-inter allow access-type gprs location-area-list instance 1
```

rau-inter-plmn

Enables or disables restriction of all Routing Area Updates (RAUs) occurring between different PLMNs.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
rau-inter-plmn access-type { all | location-area-list instance instance }
{ failure-code fail_code | user-device-release { before-r99 } failure-code
 fail_code | r99-or-later } { failure-code fail_code } }
default rau-inter-plmn access-type { all | location-area-list instance
instance} user-device-release { before-r99 failure-code | r99-or-later
failure-code }
[ no ] rau-inter-plmn { restrict | allow } access-type { gprs | umts } {
 all | location-area-list instance instance }
```

```
[ no ] rau-inter-plmn { allow access-type | restrict access-type } { [
all ] failure-code fail_code | location-area-list instance instance }
default rau-inter { allow access-type | restrict access-type } { [ all ]
 failure-code fail_code | location-area-list instance instance } }
```

no

Including "no" as part of the command structure disables the values already configured for parameters specified in the command.

default

Resets the configuration of specified parameters to system default values.

allow access-type

Including this keyword-set with one of the following options, configures the SGSN to allow MS/UE with the identified access-type extension to be part of the intra-RAU procedure.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System

restrict access-type

Including this keyword-set with one of the following options, configures the SGSN to restrict MS/UE with the identified access-type extension from the inter-RAU procedure.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System

all

all - adding this option to the keyword determines that the failure cause code will be applicable to all location areas.

location-area-list instance *instance*

list_id must be an integer between 1 and 5. The value must be an already defined instance of a LAC list created with the **location-area-list** command.

failure-code *fail-code*

Specify a GSM Mobility Management (GMM) failure cause code to identify the reason an inter SGSN RAU does not occur. This GMM cause code will be sent in the reject message to the MS.

fail-code must be an integer from 2 to 111. Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME

- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 -MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

user-device-release { before-r99 | r99-or-later } failure-code *code*

Default: Disabled

Enables the SGSN to reject an Inter-RAU procedure based on the detected 3GPP release version of the MS equipment and selectively send a failure cause code in the reject message. The SGSN uses the following procedure to implement this configuration:

1. When Attach Request is received, the SGSN checks the subscriber's IMSI and current location information.
2. Based on the IMSI, an operator policy and call control profile are found that relate to this Attach Request.

3. The call control profile is checked for access limitations.
4. Attach Request is checked to see if the revision indicator bit is set
   - if not, then the configured common failure code for reject is sent;
   - if set, then the 3GPP release level is verified and action is taken based on the configuration of this parameter

One of the following options must be selected and completed:

- **before-r99**: Indicates the MS would be a 3GPP release prior to R99 and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

- **r99-or-later**: Indicates the MS would be a 3GPP Release 99 or later and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

Usage Guidelines

Use this command to configure the restrictions and function of the inter-RAU procedure occurring across RNCs or BSSs where the PLMN changes. For example:

- inter-IuPS RAU, where the two IuPSs have different PLMNs
- inter-GPRS RAU, where the two GPRSs have different PLMNs
- inter-RAT RAU (2G > 3G), where the IuPS/GPRS services have different PLMNs
- inter-RAT-RAU (3G > 2G), where the IuPS/GPRS services have different PLMNs

Example

```
default rau-inter allow access-type gprs location-area-list instance 1
```

rau-intra

Defines an acceptable procedure for intra-SGSN Routing Area Updates (RAUs).

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

rau-intra access-type { all | location-area-list instance *instance_id* **| routing-area-list instance** *instance_id* **} { failure-code** *fail_code* **|**

user-device-release { before-r99 } { failure-code *fail_code* **| r99-or-later } { failure-code** *fail_code* **} }**
default rau-intra access-type { all | location-area-list instance *instance_id* **| routing-area-list instance** *instance_id***} user-device-release { before-r99 failure-code | r99-or-later failure-code }**
rau-intra { allow access-type | restrict access-type } { [all] failure-code *fail_code* **| location-area-list instance** *instance_id* **| routing-area-list instance** *instance_id* **} }**
no rau-intra { allow access-type | restrict access-type } { [all] failure-code *fail_code* **| location-area-list instance** *instance_id* **| routing-area-list instance** *instance_id* **}**
default rau-intra { allow access-type | restrict access-type } { [all] failure-code *fail_code* | location-area-list instance *instance_id* **| routing-area-list instance** *instance_id***} }**

no

Including "no" as part of the command structure disables the values already configured for parameters specified in the command.

default

Resets the configuration of specified parameters to system default values.

allow access-type

Including this keyword-set with one of the following options, configures the SGSN to allow an MS/UE with the identified access-type extension to be part of the intra-RAU procedure.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System

restrict access-type

Including this keyword-set with one of the following options, configures the SGSN to restrict an MS/UE with the identified access-type extension from the intra-RAU procedure.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System

all

all - adding this option to the keyword determines that the failure cause code will be applicable to all location areas.

location-area-list instance *instance_id*

instance_id must be an integer from 1 to 5. The value must be an already defined instance of a location area code (LAC) list created via the **location-area-list** command.

routing-area-list instance *instance_id*

Instructs the SGSN to apply the command action to a specific routing area list. Routing area lists should already have been created with the **routing-area-list** command.

instance_id must be an integer from 1 to 5.

failure-code *fail-code*

Specify a GSM Mobility Management (GMM) failure cause code to identify the reason an inter SGSN RAU does not occur. This GMM cause code will be sent in the reject message to the MS.

fail-code must be an integer from 2 to 111. Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 -MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state

- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

user-device-release { before-r99 | r99-or-later } failure-code *code*

Default: Disabled

Enables the SGSN to reject an Intra-RAU procedure based on the detected 3GPP release version of the MS equipment and selectively send a failure cause code in the reject message. The SGSN uses the following procedure to implement this configuration:

1. When Attach Request is received, the SGSN checks the subscriber's IMSI and current location information.
2. Based on the IMSI, an operator policy and call control profile are found that relate to this Attach Request.
3. Call control profile is checked for access limitations.
4. Attach Request is checked to see if the revision indicator bit is set
   - if not, then the configured common failure code for reject is sent;
   - if set, then the 3GPP release level is verified and action is taken based on the configuration of this parameter

One of the following options must be selected and completed:

- **before-r99**: Indicates the MS would be a 3GPP release prior to R99 and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

- **r99-or-later**: Indicates the MS would be a 3GPP Release 99 or later and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

Usage Guidelines Use this command to configure the restrictions and function of the intra-RAU procedure.

Example

```
default rau-intra allow access-type gprs location-area-list instance 1
```

re-authenticate

Enables or disables the re-authentication feature. This command is available in releases 8.1 and higher.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
re-authenticate [ access-type { gprs | umts } ]
remove re-authenticate
```

remove

Including this keyword with the command disables the feature. The feature is disabled by default.

access-type

Defines the type of access to be allowed or restricted.

- **gprs**
- **umts**

If this keyword is not included, then both access types are allowed by default.

Usage Guidelines

Use this command to enable or disable the re-authentication feature, which instructs the SGSN to retry authentication with another RAND in situations where failure of the first authentication has occurred. To address the introduction of new SIM cards, for security reasons a systematic "last chance" authentication retry with a fresh Authentication Vector is needed, particularly in cases where there is an SRES mismatch at authentication.

Example

```
re-authenticate
```

regional-subscription-restriction

Allows the operator to define the cause code for subscriber rejection when it is due to regional subscription information failure.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

[remove] regional-subscription-restriction [failure-code *code* **| user-device-release { before-r99 failure-code** *code* **| r99-or-later failure-code** *code* **}]**

remove

This keyword causes the configuration to be deleted from the call control profile configuration.

failure-code *cause_code*

cause_code: Enter an integer from 2 to 111; default code is 13 (roaming not allowed in this location area [LA]).

Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 - MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented

- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

user-device-release { before-r99 | r99-or-later } failure-code *code*

Enables the SGSN to assign a reject cause code based on the detected 3GPP release version of the MS equipment.

One of the following options must be selected and completed:

- **before-r99**: Indicates the MS would be a 3GPP release prior to R99 and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111. Refer to the list above.

- **r99-or-later**: Indicates the MS would be a 3GPP Release 99 or later and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111. Refer to the list above.

Usage Guidelines

Use this command to define GMM reject cause codes when rejection is due to regional subscription information failure.

Example

The following command sets a location area rejection message, code 12 for regional restriction rejections:

```
regional-subscription-restriction failure-code 12
```

release-access-bearer

Enables sending of Release Access Bearer and configures the S4-SGSN to send Release Access Bearer Request on Iu-Release for non-DT and non-ISR subscribers in 3G and on Ready-to-Standby or Radio-Status-Bad for non-ISR subscribers in 2G.

Product



Important We recommend that Release Access Bearer be enabled (with this command) prior to enabling Subscriber Overcharing Protection for S4-SGSN. This will ensure that the S4-SGSN sends Release Access Bearer with the ARRL bit set if LORC (loss of radio coverage) is detected.

SGSN.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
release-access-bearer [ on-iu-release | on-ready-to-standby ]
remove release-access-bearer [ on-iu-release | on-ready-to-standby ]
```

remove

When included with the command, **remove** disables sending Release Access Bearer in either the selected (with optional keyword) 2G or 3G environment or both environments (with no keyword included).

on-iu-release

This optional keyword instructs the SGSN to send Release Access Bearer upon Iu-Release in a 3G network so that Release Access Bearer will be initiated for non-ISR and non-DT subscribers upon Iu-Release. For ISR and DT subscribers, Release Access Bearer will be initiated unconditionally.

on-ready-to-standby

This optional keyword instructs the SGSN to send Release Access Bearer on Ready-to-Standby transition in a 2G network so that Release Access Bearer will be initiated for non-ISR subscribers on Ready-to-Standby transition. For ISR subscribers, Release Access Bearer will be initiated unconditionally.

Usage Guidelines

If no optional keywords are included with the **release-access-bearer** command, then the S4-SGSN applies Release Access Bearer for both 2G and 3G networks.

By default, Release Access Bearer initiation on Iu-Release or Ready-to-Standby transition is not enabled. When disabled or prior to being enabled, either/both remove release-access-bearer on-iu-release or/and remove release-access-bearer on-ready-to-standby will display in the output generated by the **show configuration [verbose]** command.

This command, in compliance with 3GPP TS 23.060 v11.7.0, provides the operator with the option to have the S4-SGSN send Release Access Bearer Request to the S-GW to remove the downlink user plane on the S4 interface for non-DT and non-ISR scenarios.

In accordance with 3GPP TS 23.401 v11.8.0, if the SGSN and the S-GW are configured to release S4 U-Plane when the EPS bearer contexts associated with the released RABs are to be preserved, then the SGSN should not send SGSN address and TEID for U-Plane in the Modify Bearer Request (MBR). The operator can now use the **rau-inter exclude-uteid-in-mbr** command (under Call-Control Profile configuration mode) to configure the SGSN not to send the UTEID in the MBR.

Example

To enable release access bearer in both 2G and 3G networks, use a command similar to the following:

```
release-access-bearer
```

To disable release access bearer in 3G networks, use a command similar to the following:

```
remove release-access-bearer on-iu-release
```

reporting-action

This command enables event logging in the MME.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

`[ remove ] reporting-action { event-stream event-report-conn` *`gmpc_event_report_name`* **`| mme-event-record}`**

remove

This command disables the reporting action configuration.

event-stream event-report-conn

Provides event logs for both MME and SGSN procedures using packet streaming.

mme-event-record

Provides event logs for MME procedures in the form of event records using CDRMOD.

Usage Guidelines

The **reporting-action** command is configured in the Call Control Profile Configuration mode. This command enables procedure reports (Event Data Records). However, the Event Data Records (EDRs) are configured in the Context Configuration mode under the **edr-module active-charging-service** command. Along with EDR configuration, the file parmeters can also be confgured in the Context Configuration mode under the **session-event-module** command. Finally, to enable the Event Logging, the EDR configuration profile must be associated to an MME-Service available under Operator Policy and LTE Policy configuration.

Example

The following configuration enables Event Logging in the MME:

```
reporting-action event-stream
reporting-action mme-event-record
```

reuse-authentication-triplets

Creates a configuration entry to enable or disable the reuse of authentication triplets in the event of a failure.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

`[ no | remove ] reuse-authentication-triplets no-limit`

no

Disables this configuration entry and disables reuse of authentication triplets.

remove

This keyword causes the reuse configuration to be deleted from the call control profile configuration.

This is the default behavior. Triplets are reused.

no-limit

This keyword enables reuse triplets as needed.

Usage Guidelines

Use this command to enable reuse of authentication triplets.

Example

`reuse-authentication-triplets no limit`

rfsp-override

Configures RAT frequency selection priority override parameters for this call control profile.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

rfsp-override { default *value* **| eutran-ho-restricted** *value* **| ue-val** *value* **new-val** *value* **+ }**
remove rfsp-override { default | eutran-ho-restricted | ue-val *value* **}**

remove

Deletes the rfsp-override configuration from the call control profile.

default

Restores the default value assigned.

eutran-ho-restricted *value*

This keyword is used to configure the value for RAT frequency selection priority when Handover to EUTRAN is restricted. This value overrides the RFSP ID value sent by the HLR/HSS in an EPS subscription.

value: Enter an integer from 1 to 256.

ue-val *value*

Assign the UE value for the RAT frequency selection priority.

value: Enter an integer from 1 to 256.

new-val *value*

Assign a new RFSP Index value.

value: Enter an integer from 1 to 256.

Multiple UE value/new value combinations can be configured in a single command.

Usage Guidelines

Use this command to configure the RAT frequency selection priority override parameter.

Multiple UE value/new value combinations can be configured.

Example

The following command resets the specified RFSP Index value (1) to its default value, thereby removing the RFSP Index override value previously configured:

```
rfsp-override default 1
```

rfsp-override ue-settings

Configures the override of the RAT Frequency Selection Priority (RFSP) of matching subscribers.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
[ remove ] rfsp-override ue-settings { data-centric
ue-voice-domain-preference { cs-voice-only |
cs-voice-preferred-ims-ps-voice-secondary | ims-ps-voice-only |
ims-ps-voice-preferred-cs-voice-secondary } | voice-centric
ue-voice-domain-preference { cs-voice-only |
cs-voice-preferred-ims-ps-voice-secondary | ims-ps-voice-only |
ims-ps-voice-preferred-cs-voice-secondary } new-val value }
```

remove

Deletes the rfsp-override configuration from the call control profile.

ue-settings *value*

Assign the UE value for the RAT frequency selection priority.

data-centric ue-voice-domain-preference

Assign the UE value for the RAT frequency selection priority for data-centric calls.

- **cs-voice-only**: Circuit switched voice only.
- **cs-voice-preferred-ims-ps-voice-secondary**: Circuit switched voice preferred.
- **ims-ps-voice-only**: IMS Packet switched voice only.
- **ims-ps-voice-preferred-cs-voice-secondary**: IMS Packet switched voice preferred.

voice-centric ue-voice-domain-preference

Assign the UE value for the RAT frequency selection priority for voice-centric calls.

- **cs-voice-only**: Circuit switched voice only.
- **cs-voice-preferred-ims-ps-voice-secondary**: Circuit switched voice preferred.
- **ims-ps-voice-only**: IMS Packet switched voice only.
- **ims-ps-voice-preferred-cs-voice-secondary**: IMS Packet switched voice preferred.

new-val *value*

Assign a new RFSP Index value.

value: Enter an integer from 1 to 256.

Multiple UE value/new value combinations can be configured in a single command.

Usage Guidelines

Use this command to assign an RFSP Index for a UE based on the following factors:

- Operator policy (where IMSI range or PLMN can influence the selected RFSP)
- UE usage setting (voice centric, data centric)

- Voice domain preference (CS voice only, CS voice preferred, IMS PS voice preferred, IMS PS voice only).

To support Radio Resource Management (RRM) in E-UTRAN, the MME provides the parameter RFSP Index to an eNodeB across S1. The RFSP Index is used by the eNodeB to apply specific RRM strategies.

The MME receives the subscribed RFSP Index from the HSS, then overrides the RFSP Index for the UE based on the settings defined in this command.

Multiple UE value/new value combinations can be configured.

Example

The following command overrides the RFSP Index value for voice-centric circuit switched calls to an RFSP Index of 10:

```
rfsp-override ue-setting voice-centric voice-domain-pref cs-voice_only
new-val 10
```

routing-area-list

Defines the routing area list to allow or restrict services in the specified routing areas identified by routing area code (RAC).

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
routing-area-list instance instance_id lac lac rac rac
no routing-area-list instance instance_id
```

no

Deletes the specified routing area list configurations.

instance *instance_id*

Specifies an identification for the specific routing area list.

instance must be an integer between 1 and 5. Instance number will be valid only if the area code is configured for this instance.

lac *lac*

This keyword defines the location area codes (LACs) to be used by this call control profile as a determining factor in the handling of incoming calls.

lac must be an integer from 1 to 65535.

rac *rac*

This keyword defines the routing area codes (RACs) to be used by this call control profile as a determining factor in the handling of incoming calls.

rac must be an integer from 0 to 255.

Usage Guidelines Use the command multiple times to configure multiple RAC lists or to modify the list.

Example

The following command creates a routing area list:

```
routing-area-list instance 1 lac 514 rac 10
```

s1-reset

Configures the behavior of user equipment (UE) on S1-reset.

Product MME

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
s1-reset { detach-ue | idle-mode-entry }
default s1-reset
```

default

Reset the profile configuration to the system default of **idle-mode-entry**.

detach-ue

Upon S1-reset the MME will detach the UE.

idle-mode-entry

Upon S1-reset the MME will move the UE to idle-mode. This is the default setting for this command.

Usage Guidelines Use this command to set the MME's reactions to an S1-reset.

Example

Configure the MME to put the UE into idle-mode upon receipt of S1-reset:

```
s1-reset idle-mode-entry
```

samog-cdr

Enables the SaMOG Gateway to send the AP Group Name in the SSID field of tWANUserLocationInformation in the S-GW CDR.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

samog-cdr twanuli ap-group-name

no samog-cdr twanuli ap-group-name

no

If configured, disables SaMOG from sending the AP Group Name in the SSID field of tWANUserLocationInformation in the S-GW CDR, and reverts the configuration to its default behavior. By default, the SaMOG Gateway sends the SSID information in the tWANUserLocationInformation attribute.

Usage Guidelines

Use this command to enable the SaMOG Gateway to send the AP Group Name in the SSID field of tWANUserLocationInformation (TWAN ULI) in the S-GW CDR.

To enable the SaMOG Gateway to send the TWAN ULI attribute in the GTPP requests, use the **gtpp attribute twanuli** command under the GTPP Group Configuration Mode.



Important SaMOG services and standalone S-GW services must not share a GTTP group that has the **gtpp attribute twanuli** command configured. Instead, configure the command under different GTPP groups for each service.

Example

Configure SaMOG Gateway to send the AP Group Name in the SSID field of tWANUserLocationInformation in the S-GW CDR:

```
samog-cdr twanuli ap-group-name
```

samog-gtpv1

Enables SaMOG to forward the User Equipment's (UE) Identity, and/or the Access Point's (AP) Location information over the GTPv1 interface.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

samog-gtpv1 send { imeisv value ue-mac [decimal | filler *filler_value* **] | uli value cgi }**
no samog-gtpv1 send { imeisv | uli }

no

If configured, disables SaMOG from forwarding the UE Identity and/or AP Location information over the GTPv1 interface.

imeisv value ue-mac

Specifies to forward the UE Identity. By default this configuration is disabled.

decimal

Specifies to encode the UE's MAC address for the IMEIsV IE value in decimal format. By default, the UE's MAC address in the IMEIsV IE value is encoded in Hexa-decimal format.

filler *filler_value*

Specifies the 2 bytes of padding to be used with the UE's MAC address for the IMEIsV IE value.

filler_value must be a hexadecimal number from 0x0 through 0xFFFE. The default filler value is 0xFFFF.

uli value cgi

Specifies to forward the AP's User Location Information (ULI) IE during the PDP context setup.

Usage Guidelines

Use this command to enable SaMOG to forward the User Equipment's (UE) Identity, and/or the Access Point's (AP) Location information over the GTPv1 interface.

Example

Configure SaMOG to forward the AP location information :

samog-gtpv1 uli value cgi

samog-s2a-gtpv2

Enables SaMOG to forward S2a GTPv2 Information Element (IE) related parameters.



Important This command is available only when the SaMOG General license (supporting both 3G and 4G) is configured. Contact your Cisco account representative for more information on license requirements.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

samog-s2a-gtpv2 send { imeisv value ue-mac [decimal | filler *filler_value* **] | pco pap value mn-nai | serving-network value uli | twan-identifier { civic-addr-fld ca-type name value ap-group-name | ssid-fld value ap-group-name } | uli }**

no samog-s2a-gtpv2 send { imeisv | pco pap value mn-nai | serving-network value uli | twan-identifier { civic-addr-fld | ssid-fld value ap-group-name } | uli }

no

Disables a previously enabled configuration.

imeisv value ue-mac [decimal | filler *filler_value*]

Specifies to forward the UE Identity in the IMEIsV IE value. By default this configuration is disabled.

decimal: Specifies to encode the UE's MAC address for the IMEIsV IE value in decimal format. By default, the UE's MAC address in the IMEIsV IE value is encoded in Hexa-decimal format.

filler: Specifies the 2 bytes of padding to be used with the UE's MAC address for the IMEIsV IE value.

filler_value must be a hexadecimal number from 0x0 through 0xFFFE.

pco pap value mn-nai

Specifies to forward the UE's MN-NAI value in the PAP container within the PCO IE in the CSR message to P-GW.

This configuration is disabled by default.

serving-network value uli

Specifies to populate the Serving-Network Information Element (IE) with the PLMN ID (MCC and MNC values) from the 3GPP-User-Location-Information AVP sent by the AAA Server (STa interface).

This configuration is disabled by default.

twan-identifier ssid-fld value ap-group-name

Specifies to forward the AP group name in the SSID sub-field of TWAN-Identifier.

By default, the SSID value is forwarded in the SSID sub-field of TWAN-Identifier.

twan-identifier civic-addr-fld ca-type name value ap-group-name

Specifies to the AP group name value in the Civic Address Information sub-field of the TWAN-Identifier IE over the S2a interface.

This configuration is disabled by default.

uli

Specifies to forward the User-Location-Information (ULI) Information Element (IE) in the CSR message over the S2a interface. SaMOG populates the ULI IE from the 3GPP-User-Location-Information AVP received from the AAA Server over the STa interface.

This configuration is disabled by default.

Usage Guidelines

Use this command to enable SaMOG to forward:

- The User Equipment's (UE) Identity information over the GTPv2 interface in decimal or hexa-decimal format
- The UE's MN-NAI value in the PAP container within the PCO IE in the CSR message.
- The Serving-Network IE information in the Create Session Request message over the S2a interface.
- The AP group name in the SSID sub-field of the TWAN-Identifier.
- The AP group name in the Civic Address Information sub-field of the TWAN-Identifier .
- The ULI IE information in the Create Session Request message over the S2a interface.

Example

Configure SaMOG to forward the UE identity with a padding value of **0xFEFE**:

```
samog-s2a-gtpv2 send imeisv value ue-mac filler 0xFEFE
```

Configure SaMOG to forward the UE's MN-NAI value in the PAP container within the PCO IE in the CSR message:

```
samog-s2a-gtpv2 send pco pap value mn-nai
```

sctp-down

Configures the behavior towards UE (user equipment) when Stream Control Transmission Protocol (SCTP) goes down.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

`sctp-down { detach-ue | idle-mode-entry }`
`default sctp-down`

default

Reset the profile configuration to the system default when SCTP layer goes down. The default for this command is **idle-mode-entry**.

detach-ue

When SCTP goes down, the MME will detach the UE.

idle-mode-entry

When the SCTP goes down, the MME will move the UE to idle-mode. This is the default for this command.

Usage Guidelines

Use this command to set the MME's reactions when the SCTP goes down.

Example

Configure the MME to put the UE into idle-mode when the SCTP layer goes down:

`sctp-down idle-mode-entry`

secondary-rat

Enables the Secondary RAT Data Usage Report to support 5G NSA.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > **call-control-profile** *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
secondary-rat data-usage-report { pgw [ sgw ]  | sgw [ pgw ] }
[ no | remove ] secondary-rat data-usage-report
```

no

Disables the Secondary RAT Usage Report at call-control-profile.

remove

Removes the Secondary-RAT Usage Report configuration from call-control-profile. It fall-back to MME service level configuration.

secondary-rat data-usage-report { pgw [sgw] | sgw [pgw] }

MME sets IR-SGW and IR-PGW flags based on the available options configured for Secondary-RAT data usage report. By default, MME disables the Secondary-RAT data usage reporting towards both SGW and PGW. If the configuration is removed from call-control-profile, then it fall-back to MME-SERVICE level configuration for Secondary-RAT-Data-Usage-Report functionality.

- **secondary-rat data-usage-report pgw**: Disables the Secondary-RAT Usage Report option for S-GW and enables only for PGW.
- **secondary-rat data-usage-report sgw**: Disables the Secondary-RAT Usage Report option for P-GW and enables only for S-GW.
- **secondary-rat data-usage-report pgw sgw**: Enables Secondary-RAT Usage Report option for both SGW and PGW.
- **secondary-rat data-usage-report sgw pgw**: Enables Secondary-RAT Usage Report option for both SGW and PGW.

Usage Guidelines

Use this command to enable the Secondary RAT Data Usage Report to support 5G NSA.

Example

Configures the Secondary-RAT Usage Report option for both SGW and PGW:

```
secondary-rat data-usage-report pgw sgw
```

serving-plmn

Configures a static serving node PLMN Identifier (MCC and MNC) for this Call Control Profile.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`serving-plmn id mcc` *`mcc_value`* **`mnc`** *`mnc_value`*
`remove serving-plmn id`

remove

Removes the static serving node PLMN ID configuration from this Call Control Profile.

mcc *mcc_value*

Specifies the Mobile Country Code (MCC) of the serving PLMN Identifier for this Call Control Profile.

mcc_value must be an integer between 100 and 999.

mnc *mnc_value*

Specifies the Mobile Network Code (MNC) of the serving PLMN Identifier for this Call Control Profile.

mnc_value must be an integer between 0 and 999.

Usage Guidelines

Use this command to configure a static serving node PLMN Identifier (MCC and MNC) for this Call Control Profile.

Example

Configure a static serving PLMN ID with a value of 777 for MCC and 109 for MNC using the following example:

`serving-plmn id mcc 777 mnc 109`

serving-plmn-rate-control

This command is used to configure the serving PLMN rate control for control plane CIoT optimization. The serving PLMN rate control limits the rate at which UE or PGW/SCEF can send data over the control plane when CP optimization is enabled.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

serving-plmn-rate-control ul-rate *ul_rate_value* **dl-rate** *dl_rate_value*
remove serving-plmn-rate-control

remove

The keyword remove deletes the existing configuration.

ul-rate *ul_rate_value*

The maximum number of data NAS PDUs the UE can send in uplink path per deci-hour (6 minutes). The uplink rate is an integer from 10 up to 65535. A value of 65535 in this case implies no limit on the number of PDUs the UE can send in the uplink path per deci-hour.

dl-rate *dl_rate_value*

The maximum number of data NAS PDUs the PGW/SCEF can send in the downlink path to the UE per deci-hour (6 minutes). The downlink rate is an integer from 10 up to 65535. A value of 65535 in this case implies no limit on the number of PDUs the PGW/SCEF can send in the downlink path per deci-hour.

Usage Guidelines

This command configures serving PLMN rate for data over NAS. It limits the rate for data exchange between UE and the PGW/SCEF while using control plane CIoT optimization. This command is not enabled by default.

Example

Use the following command to configure the serving PLMN rate for data over NAS, with uplink rate as 35 and downlink rate as 45:

serving-plmn-rate-control ul-rate *35* **dl-rate** *45*

sgs-cause-code-mapping

Configures the EMM reject cause code to send to a UE when an SGs cause code is received.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

sgs-cause-code-mapping *sgs-cause* **emm-cause-code** *emm_cause_code*
remove sgs-cause-code-mapping *sgs-cause*

remove sgs-cause-code-mapping *sgs-cause*

Removes the configured cause code mapping and returns it to its default value.

sgs-cause-code

Specifies the SGs cause code received on the SGs interface to which the new cause code should be mapped.

- **congestion** - Default mapped EMM cause code: #22 Congestion.
- **illegal-me** - Default mapped EMM cause code: #16 MSC temporarily unreachable.
- **illegal-ms** - Default mapped EMM cause code: #16 MSC temporarily unreachable.
- **imei-not-accepted** - Default mapped EMM cause code: #16 MSC temporarily unreachable.
- **imsi-unknown-in-hss** - Default mapped EMM cause code: #2 IMSI unknown in HSS.
- **imsi-unknown-in-vlr** - Default mapped EMM cause code: #16 MSC temporarily unreachable.
- **la-not-allowed** - Default mapped EMM cause code: #16 MSC temporarily unreachable.
- **network-failure** - Default mapped EMM cause code: #17 Network failure.
- **no-suitable-cells-in-la** - Default mapped EMM cause code: #16 MSC temporarily unreachable.
- **plmn-not-allowed** - Default mapped EMM cause code: #16 MSC temporarily unreachable.
- **protocol-error** - Default mapped EMM cause code: #16 MSC temporarily unreachable.
- **roaming-not-allowed-in-la** - Default mapped EMM cause code: #16 MSC temporarily unreachable.
- **service-not-subscribed** - Default mapped EMM cause code: #16 MSC temporarily unreachable.
- **service-not-supported** - Default mapped EMM cause code: #16 MSC temporarily unreachable.
- **service-out-of-order** - Default mapped EMM cause code: #16 MSC temporarily unreachable.

emm-cause-code *emm_cause_code*

Specifies the EPS Mobility Management (EMM) cause code to return to the UE for the given SGs cause code.

- **congestion**
- **cs-domain-unavailable**
- **imsi-unknown-in-hss**
- **msc-temp-unreachable**
- **network-failure**

Usage Guidelines

Use this command to configure the EMM cause code returned to a UE when an error is reported via the SGs inteface when attachment to the VLR has failed.

If a condition is specified in both the call control profile associated with a call and also the MME service, the cause configured on the call control profile is signalled to the UE.



Important EMM cause code #18 "CS Domain not available" is not mapped to any SGs code but is returned when SGs service is disallowed by a policy or on unexpected behavior such as when the MME is unable to send an SGs message to a VLR.

Related Commands

To set the cause codes for situations where a call control profile cannot be attached to a call (for example new-call restrictions, congestion during new call attempt, etc.), use the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

The following command maps the "congestion" EMM cause code to the "network-failure" SGs cause code:

```
sgs-cause-code-mapping network-failure emm-cause-code congestion
```

sgsn-address

Defines the IP addresses for peer SGSNs in a static SGSN address table. These configured addresses can be used if operators wish to bypass DNS.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
sgsn-address { nri nri | rac rac-id lac lac_id | rnc_id rnc_id } [ nri nri ]
prefer { fallback-for-dns | local } address { ipv4 ip_address | ipv6 ip_address
 } interface { gn | s16 }
no sgsn-address { ipv4 ip_address | ipv6 ip_address } { nri nri | rac rac_id
lac lac_id [ nri nri | rnc_id rnc_id } [ interface { gn | s16 } ]
```

no

Disables the specified peer-SGSN address configuration.

rac *rac_id*

Identifies the foreign routing area code (RAC) of the peer-SGSN address to be configured in the static peer-SGSN address table. *rac_id* must be an integer from 1 to 255.

lac *lac_id*

Identifies the foreign location area code (LAC) ID of the peer-SGSN address to be configured in the static peer-SGSN address table. *lac_id* must be an integer from 1 to 65535.

rnc_id *rnc_id*

Optional. Specifies the target RNC ID that maps to the address of the peer SGSN via the S16 interface. The RNC ID is used by the S4-SGSN for inter-SGSN SRNS relocations. Valid entries are 1 to 65535. This setting only applies if SRNS relocation has been configured via the **srns-inter** and/or **srns-intra** commands in *Call Control Profile Configuration Mode*.

nri *nri*

Identifies the network resource identifier stored in the P-TMSI (bit 17 to bit 23). *nri* must be an integer from 0 to 63.

Important Typically, use of this keyword is optional. However, it must be included in the command when Flex (SGSN-Pooling) is implemented.

Important Look up for peer SGSN in the local pool can be performed by configuring only the NRI value, as the NRI value is unique in a pool.

prefer { fallback-for-dns | local }

Indicates the preferred source of the address to be used.

- **fallback-for-dns** - Instructs the SGSN to perform a DNS query to get the IP address of the peer-SGSN. If the DNS query fails, then the IP address configured with this command is used.
- **local** - instructs the system to use the local IP address configured with this command.

Important If the **prefer** command is used to change an existing sgsn-address configuration (with the same LAC and RAC) from **fallback-for-dns** to **local** or from **local** to **fallback-for-dns**, the new setting overwrites the previously configured setting for all interfaces.

address { ipv4 *ip_address* | ipv6 *ip_address* }

Specifies the IP address of the peer SGSN. Currently, the IPv6 address option is not supported on the S4-SGSN.

- **ipv4** *ip_address* - specifies a valid address in IPv4 dotted-decimal notation.
- **ipv6** *ip_address* -

Important The **ipv6** option is under development for future use and is not supported in this release.

interface { gn | s16 }

interface - optional. Specifies the interface type used for communicating with the peer SGSN. Must be one of the following:

- **gn** specifies that communication will occur over the Gn interface with a peer SGSN configured for 2.5G, 3G, or dual access SGSN services.
- **s16** specifies that communication will occur over the S16 interface with a peer S4-SGSN.

Usage Guidelines

Use this command to save time by avoiding DNS. This command enables a local mapping by setting the peer-SGSN IP address to be used for inter-SGSN Attach and inter-SGSN-RAU. When configured, if the SGSN receives a RAU or an Attach Request with a P-TMSI and an old-RAI that is not local, the SGSN consults this table and uses the configured IP address instead of resolving via DNS. If this table is not configured, then IP address resolution is done using DNS.

The MCC and MNC of the RAI are taken from the IMSI range configured in the operator policy and the LAC and RAC are configured here in the call control profile configuration mode.

The **sgsn-address** command differs from other Call Control Profile configuration mode commands in the following ways:

- Within the SGSN's call logic, all other configuration elements defined with the other commands in this mode are used ***after*** the IMSI is learnt. The configuration defined with this command is part of the decision logic ***prior*** to the IMSI being known.
- With the peer-SGSN address configured using this **sgsn-address** command, the peer-SGSN-RAI's MCC/MNC is used as a 5 or 6-digit IMSI and the operator policy and call control profile selection are completed.

Important Typically, use of this command is optional. However, it must be included in the configuration when Flex (SGSN-Pooling) is implemented if (1) the SGSN functions as a default SGSN, then configure the local-NRI of other SGSN with this command; or if (2) another SGSN is offloading, then configure the NB-RAI/null-NRI of the peer-SGSN with this command.

Important It is recommended to execute the S4 SGSN configuration commands during the maintenance window. After configuring the node, re-start the node to activate the configuration commands. This will ensure that the node is in a consistent state and S4 SGSN service instability scenarios are avoided.

Example

Create a local peer-SGSN address mapping of an RAI with RAC of *192* and LAC of *4444* and an *IPv4* address of *192.0.2.0* for the peer-SGSN:

```
sgsn-address rac 192 lac 4444 local address ipv4 192.0.2.0
```

sgsn-core-nw-interface

This command enables operators to select the Gn interface or the S4 interface for EPC capable UEs and Non-EPC capable UEs on the S4-SGSN.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
sgsn-core-nw-interface { gn | s4 [ epc-ue { always | eps-subscribed }
non-epc-ue { never | always | eps-subscribed } ] }
```

sgsn-core-nw-interface { gn | s4 }

Specifies the interface that EPC-capable UEs will use to communicate wit the packet core gateways (GGSN/SGW). Selection must be one of:

- **gn**: Forces the SGSN to forcefully select the Gn interface for EPC-capable UEs.
- **s4**: Specifies that the SGSN will use the S4 interface between the S4-SGSN and packet core gateways (GGSN/SGW). This is the default setting for EPC-capable UEs.

The S4-SGSN uses GTPv2 by default and allows new Inter SGSN RAUs over GTPv2 for all subscribers. The S4-SGSN allows ISRAUs over GTPv2 even if the subscriber's call-control-profile is configured explicitly with Gn interface as the S4-SGSN does not check for core network interface configured for a specific subscriber before allowing GTPv2. The inbound ISRAUs over GTPv2 interface has to be restricted for roaming subscribers. Access to S4 interface or GTPv2 should be limited only to home subscribers.

In release 19.3.10 the configuration of the CLI command **sgsn-core-nw-interface** was used to decide whether to reject/honor the RAU request upon context response received via GTPv2.

The configuration of the CLI command **sgsn-core-nw-interface** is used to impose restriction on roaming subscribers for ISRAU over GTPv2. The command **sgsn-core-nw-interface gn** has to be configured in the roaming subscribers call-control-profile to implement the restriction on ISRAU over GTPv2 for roaming subscribers. When the EGTP context response is received from the peer during inbound ISRAU over GTPv2, a new check is introduced where the **sgsn-core-nw-interface gn** command configuration is verified. If the subscriber's call-control profile is configured to use Gn interface alone, then EGTP Context ACK with failure cause will be sent to peer and RAU will fall back to GTPv1. The failure cause value sent in EGTP context Ack message to peer is EGTP_CAUSE_USER_AUTHENTICATION_FAILED. This is applicable for both 2G and 3G scenarios. The following table displays the actions based on the configuration:

Interface	sgsn-core-nw-interface gn	sgsn-core-nw-interface s4
GTPv1 protocol	Proceed with call	Proceed with call
GTPv2 protocol	RAU fall back to GTPv1 and proceed with call	Proceed with call

epc-ue

Configures the S4 Interface Selection Option for EPC Capable UE.

non-epc-ue

Configures the S4 Interface Selection Option for Non-EPC Capable UE.

always

Instructs the SGSN to always choose a S4 Interface.

never

Instructs the SGSN to not choose a S4 Interface.

eps-subscribed

Instructs the SGSN to choose a S4 Interface if EPS Subscription is available.

Important

- When keywords or options are not selected with the selection of the S4 interface option, it implies that the SGSN will apply S4 interface always for both EPC and Non- EPC devices. This is also synonymous to the CLI command configured as **sgsn-core-nw-interface s4 epc-ue always non-epc-ue always**.
- To configure SGSN behavior supported in previous releases, the CLI is configured as **sgsn-core-nw-interface s4 epc-ue always non-epc-ue eps-subscribed**. This is also the default behavior when the CLI is not configured.

Important It is recommended to execute the S4 SGSN configuration commands during the maintenance window. After configuring the node, re-start the node to activate the configuration commands. This will ensure that the node is in a consistent state and S4 SGSN service instability scenarios are avoided.

Usage Guidelines

Use this command to forcefully select the interface that the SGSN will use for EPC-capable UEs.

This command is available only if the *SGSN S4 Interface* license is enabled on the SGSN.

Example

sgsn-core-nw-interface gn

sgsn-number

Defines the SGSN's E.164 number to be used for interactions via the Mobile Application Part (MAP) protocol. E.164 is an ITU-T recommendation that defines the international public telecommunication numbering plan used in public switched telephone networks (PSTN) and some other data networks.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

sgsn-number *E164_number*
no sgsn-number

no

Disables the use of this configuration definition.

E164_number

Specifies a string of 1 to 16 digits that serve as the SGSN's E.164 identification.

Usage Guidelines

This command configures the current SGSN E164 contact number.

The SGSN number configured for a call control profile is related to the SGSN number configured in the SGSN service configuration and/or in the GPRS service configuration. If the SGSN number is not configured as part of the call control profile configuration, then the SGSN number defined as part of the SGSN service or GPRS service configuration is used.

When the 3G SGSN supports multiple PLMNs configured through different IuPS services or when network sharing is implemented, then it may be required to use different SGSN numbers for each PLMN. In such cases, configure the per-PLMN SGSN number in a call control profile. SGSN number definition for a call control profile allows emulation of a different SGSN to each HLR per PLMN. SGSN number definitions in the call control profile also enable the SGSN to use a different SGSN number per operator when network sharing is implemented.

Example

Map the E.164 number *198765432123456* for the SGSN to this call control profile configuration:

```
sgsn-number 198765432123456
```

sgtp-service

Identifies the SGTP service configuration to be used according to this call control profile.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
sgtp-service context ctxt_name service sgtp_service_name
no sgtp-service context
```

context *ctxt_name*

Specifies the SGTP context as an alphanumeric string of 1 through 64 characters.

service *sgtp_service_name*

Specifies the SGTP service name as an alphanumeric string of 1 through 64 characters.

no

Disables use of SGTP service.

Usage Guidelines Use this command to configure enabling or disabling of SGTP service for this call control profile.

Example

```
sgtp-service context sgtp1 service sgtp-srvc1
```

sgw-retry-max

Sets the maximum number of SGW selection retries to be attempted during Attach/HO/TAU. By default, this functionality is not enabled.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

sgw-retry-max *max_number*

no sgw-retry-max

no

Disables the configuration for the maximum number of retries.

max_number

Sets the maximum number of retries possible. Enter an integer from 0 to 5. If 0 (zero) is configured, then the MME sends Create-Session-Request to the 1st SGW and if that SGW does not reply, the MME does not select any further SGW to retry. The MME then rejects the ongoing procedure (Attach/HO/TAU) and sends a Reject message.

Usage Guidelines Using the this command sets a limit to the maximum number of SGW selection retries to be attempted during Attach/HO/TAU. This means, the total number of tries would be 1 (the initial try) + the sgw-retry-max value (the maximum number of retries). This command is applicable only to scenarios, where SGW is selected from the DNS pool (i.e. not taken from static configuration of MME). For statically configured SGW nodes the SGW selection takes place only once.

Entering a value with this command overrides the default behavior. If no value is configured, then the MME uses or falls back to the default behavior which is in compliance with 3GPP TS 29.274, Section 7.6. The MME sends Create-Session-Request message to one SGW in the pool. If the SGW node is not available, the MME picks the next SGW from the pool and again sends a Create-Session-Request message. The MME repeats this process. For an Attach procedure, the MME tries up to five (1 + 4 retries) different SGWs from the pool. In

the case of a HO procedure, the MME will try every SGW in the entire pool of SGWs sent by the DNS. If there are no further SGW nodes available in the DNS pool or if the guard timer expires, then MME stops trying and sends a Reject with cause "Network-Failure" towards the UE and the UE must restart the Attach/Handover procedure.

Benefits of this configuration -- The amount of signaling at Attach or Handover can be reduced and the amount of time to find an available SGW can be reduced.

If the **sgw-retry-max** command is configured under both the MME service and the Call-Control Profile, then the configuration under Call-Control Profile takes precedence.

Example

Use this command to enable the functionality for limiting the number of SGWs tried during Attach/HO/TAU to 2 retries:

```
sgw-retry-max 2
```

sms-in-mme

Configures the MME preference for SMS and SMSC address.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
sms-in-mme { preferred [ smsc-address smsc_address ] | smsc-address smsc_address
 | subscribe { eps-only-attach } [ notify ue ] }
default sms-in-mme { subscribe { eps-only-attach } [ notify ue ] }
no sms-in-mme { preferred [ smsc-address ] | smsc-address | subscribe {
eps-only-attach } [ notify ue ] }
```

default

Restores the default configuration, which is to enable the Subscription Request for SMS services (via SGd) to HSS for all users.

no

Deletes the specified configuration.

sms-in-mme { preferred [smsc-address *smsc_address*] | smsc-address *smsc_address* }

Configures the SMS capability (SGd interface for SMS) in MME.

- **preferred**: Configures the SMS preference in MME.
- **smsc-address** *smsc_address*: Configures the SMSC address (ISDN identity) for the MME to send SMS on the SGd interface. *smsc_address* must be an integer from 1 to 15.

subscribe { eps-only-attach } [notify ue]

Enables the Subscription Request for SMS services (via SGd) to HSS for all users.

- **eps-only-attach**: Configures support for SMS over SGd for EPS only Attach.
- **notify**: Configures the notification to be sent to the users.
- **ue**: Sends SMS-Only indication to UE in Attach/TAU Accept message (only if HSS accepts SMS Registration for SGd).

Usage Guidelines

Use this command to configure SGd as the preferred SMS service and to configure the SMSC address.

Example

The following command configures the preferred SGd SMS option with SMSC address *91984599136* for a subscriber:

```
sms-in-mme preferred smsc-address 91984599136
```

sms-mo

Configures how mobile-originated (MO) short message service (SMS) messages are handled.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
[ remove ] sms-mo { { access-type { gprs | umts } { all-location-areas |
 location-area-list } | allow access-type { gprs | umts } | restrict
access-type { gprs | umts } }
```

remove

Deletes the specified configuration.

access-type *type*

Access by SMS will be limited to SMS coming from this network type:

- **gprs**
- **umts**

allow

Allow either GPRS or UMTS type access for SMS.

restrict

Restrict either GPRS or UMTS type access for SMS.

location-area-list instance *instance*

instance must be an integer between 1 and 5. The value must identify an already defined location area code (LAC) list created with the **location-area-list** command.

failure-code *code*

code: Must be an integer from 2 to 111.

Usage Guidelines

Configure filtering for SMS-MO messaging.

Example

```
sms-mo access-type gprs all-location-areas failure-code 100
```

sms-mt

This command configures how mobile-terminated (MT) short message service (SMS) messages are handled.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
[ remove ] sms-mt { { access-type { gprs | umts } { all-location-areas |
 location-area-list } | allow access-type { gprs | umts } | restrict
access-type { gprs | umts } }
```

remove

Deletes the specified configuration.

access-type *type*

Access by SMS will be limited to SMS coming from this network type:

- **gprs**
- **umts**

allow

Allow either GPRS or UMTS type access for SMS.

restrict

Restrict either GPRS or UMTS type access for SMS.

location-area-list instance *instance*

instance must be an integer between 1 and 5. The value must identify an already defined LAC list created with the **location-area-list** command.

failure-code *code*

code: Must be an integer from 2 to 111.

Usage Guidelines

Configure filtering for SMS-MT messaging.

Example

```
sms-mt access-type gprs all-location-areas failure-code 100
```

srns-inter

Defines handling parameters for Inter-SRNS (Serving Radio Network Subsystem) relocation.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
srns-inter ( all failure-code | allow { routing-area-list instance
instance_id | location-area-list instance instance_id | location-area-list
instance instance failure-code code| routing-area-list instance instance_id
failure-code code | restrict location-area-list instance instance_id|
routing-area-list instance instance_id }
no srns-inter { allow location-area-list instance instance_id |
```

routing-area-list instance *instance_id* **| restrict location-area-list instance** *instance_id* **}**
default srns-inter { all | location-area-list-instance *instance_id* **| routing-area-list instance** *instance_id* **}**

no

Deletes the inter-SRNS relocation configuration.

default

Resets the configuration to default values.

all failure-code *code*

Define the failure code that will apply to all inter-SRNS relocations.

code must be an integer from 2 to 111.

allow { location-area-list instance *instance_id* | routing-area-list instance *instance_id* }

Identifies the location area list Id (LAC Id) or routing area list Id (RAC Id) that will allow services in the defined area.

location-area-list instance *instance*

instance: Must be an integer between 1 and 5 that identifies the previously defined location area list created with the **location-area-list** command.

routing-area-list instance *instance_id*

Instructs the SGSN to apply the command action to a specific routing area list. Routing area lists should already have been created with the **routing-area-list** command.

instance_id must be an integer from 1 to 5.

restrict { location-area-list instance *instance_id* **| routing-area-list instance** *instance_id* **}**

Identifies the location area list Id (LAC Id) or routing area list Id (RAC Id) that indicates the areas where services will be restricted.

Usage Guidelines

This command defines the operational parameters for inter-SRNS relocation.

Example

The following command allows services in areas listed in LAC list #3:

```
srns-inter allow location-area-list instance 3
```

srns-intra

Defines handling parameters for intra-SRNS (Serving Radio Network Subsystem) relocation.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

srns-intra (all failure-code | allow { routing-area-list instance *instance_id* **| location-area-list instance** *instance_id* **| location-area-list instance** *instance* **failure-code** *code*| **routing-area-list instance** *instance_id* **failure-code** *code* **| restrict location-area-list instance** *instance_id*| **routing-area-list instance** *instance_id* **}**
no srns-intra { allow location-area-list instance *instance_id* **| routing-area-list instance** *instance_id* **| restrict location-area-list instance** *instance_id* **}**
default srns-intra { all | location-area-list-instance *instance_id* **| routing-area-list instance** *instance_id* **}**

no

Deletes the intra-SRNS relocation configuration.

default

Resets the configuration to default values.

all failure-code *code*

Define the failure code that will apply to all intra-SRNS relocations.

code: Must be an integer from 2 to 111.

allow { location-area-list instance *instance_id* | routing-area-list instance *instance_id* }

Identifies the location area list Id (LAC Id) or routing area list Id (RAC Id) that will allow services in the defined area.

location-area-list instance *instance*

instance: Must be an integer between 1 and 5 that identifies the previously defined location area list created with the **location-area-list** command.

routing-area-list instance *instance_id*

Instructs the SGSN to apply the command action to a specific routing area list. Routing area lists should already have been created with the **routing-area-list** command.

instance_id must be an integer from 1 to 5.

restrict { location-area-list instance *instance_id* **| routing-area-list instance** *instance_id* **}**

Identifies the location area list Id (LAC Id) or routing area list Id (RAC Id) that indicates the areas where services will be restricted.

Usage Guidelines This command defines the operational parameters for intra-SRNS relocation.

Example

The following command restricts service in areas listed in the LAC list 1:

```
srns-intra restrict location-area-list instance 1
```

srvcc exclude-stnsr-nanpi

Configures the MME to **not** include the Nature of Address and Numbering Plan Indicator (NANPI) in the Session Transfer Number for Single Radio Voice Call Continuity (STN-SR) IE on Sv interface in PS to CS requests to the MSC server and Forward Relocation requests to the peer-SGSN/peer-MME.

Product MME

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description **`[ remove ] srvcc exclude-stnsr-nanpi`**

remove

Deletes this configuration from the call control profile. This returns the MME to its default configuration where the NANPI is not included in the STN-SR IE.

Usage Guidelines This command applies to Release 15.0 MR3 and higher.

In Release 15.0 MR3 and later releases, the encoding of the STN-SR IE on Sv interface now includes the NANPI from the HSS in PS to CS requests to the MSC server and Forward Relocation requests to the peer-SGSN/peer-MME. The value of NANPI sent by the MME is 0x11. This change in behavior is provided in support of TS 29.280 V10.1.0.

This command provides an option to maintain backward compatibility. When this command is issued, the MME excludes the NANPI from these requests, as was the default in releases prior to 15.0 MR3.

srvcc

This command configures the basic SRVCC support on the MME.

Product MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ remove ] srvcc unauthorized`

remove

Deletes this configuration from the call control profile. This returns the MME to its default configuration where the SRVCC handovers are allowed.

unauthorized

Restricts the SRVCC handovers for a set of subscribers.

Usage Guidelines

This command is not enabled by default. The operator must enable **unauthorized** to restrict SRVCC handovers for a set of subscribers.

subscriber multi-device

Enable or disable the operator policy from allowing multiple PDN connections. When enabled, a maximum of 11 PDN connections are allowed for a subscriber.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ no ] subscriber multi-device`

no

If previously enabled, disables multiple PDN device connections for a subscriber.

Usage Guidelines

Use this command to enable or disable the operator policy from allowing multiple PDN connections for a subscriber. If this optional configuration is not enabled, only one PDN connection is allowed for a subscriber.



Important The SaMOG Web Authorization feature is license dependent. Contact your Cisco account representative for more information on license requirements.

Example

The following command enables mutiple device connections for a subscriber:

```
subscriber multi-device
```

subscriber-control-inactivity

Configures \the subscriber-control inactivity timer. The system detects inactivity when no PDP context is activated and starts the timer.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

subscriber-control-inactivity timeout minutes *time* **detach { immediate | next-connection | reattach-time-period }**
{ no | default } subscriber-control-inactivity

no

Deletes the timer configuration.

default

Resets the timer configuration to the default value of 7 days (10080 minutes).

timeout minutes *time* [detach]

Sets the number of minutes the SGSN monitors the connection after inactivity has been detected. When the timer expires, the subscribe will be detached.

time: Enter an integer from 1 to 20160 (two weeks).

detach [immediate | next-connection | reattach-time-period]

Instructs the SGSN to detach and can be configured to specify when the detach will occur after inactivity is detected. To fine-tune the detach instruction, include one of the following with the command:

- **immediate** - Instructs the SGSN to detach immediately after inactivity is detected. May combine with **reattach-time-period**.
- **next-connection** - Instructs the SGSN to wait for the next Iu connection after inactivity is detected and then detach. Any message except Attach on the next Iu is unconditionally rejected with cause code “GPRS services not allowed”.

Important Supported for 3G SGSNs only.

- **reattach-time-period** *period* **[action]** - Specify the number of seconds the SGSN will monitor a new re-attach after the previous detach was due to inactivity. Also, you can define the action to be taken regarding new attaches.

  period: Enter an integer from 60 to 3600.

  action - Select an action:

  - **deny**
  - **permit-and-stop-monitoring**

Usage Guidelines Use this command to configure the timeout timer. After this timer times out the subscriber is detached from the SGSN.

Example

The following command instructs the SGSN to monitor the connection for up to *360* minutes after inactivity is detected, or detach immediately after inactivity is detected:

```
subscriber-control-inactivity timeout minutes 360 detach immediate
```

super-charger

Enables or disables the SGSN to work with a super-charged network.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
[ remove ] super-charger
```

remove

Disables the super-charger functionality.

Usage Guidelines By enabling the super charger functionality for 2G or 3G connections controlled by an operator policy, the SGSN changes the hand-off and location update procedures to reduce signalling traffic management.

Example

The following command enables the super charger feature:

```
super-charger
```

tau

Configure parameters for the tracking area update (TAU) procedure.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
tau { imei-query-type { imei | imei-sv | none } [ verify-equipment-identity
 [ allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency
 ] ] | inter-rat { notify-request | security-ctxt { allow-mapped | native
 } }{ send-emm-info }}[ access-type{ all | nb-iot |
wb-eutran }] }
remove tau { imei-query-type | inter-rat { notify-request | security-ctxt
 }| { send-emm-info } }
```

remove

Deletes this TAU configuration from the call control profile.

send-emm-info

Sends EMM information to UE in case of Periodic TAU with Active Flag not set.

access-type { all | nb-iot | wb-eutran }:

access-type Enables the access type extension.

- **all**: Enables the configuration for NB-IOT and WB-EUTRAN access type.
- **nb-iot**: Enables the configuration for NB-IoT access type.
- **wb-eutran**: Enables configuration for WB-EUTRAN access types.

imei-query-type { imei | imei-sv | none }

This keyword set is specific to the MME.

Sets the IMEI query-type if an IMEI (International Mobile Equipment Identity) is not already present.

- **imei**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity (IMEI).
- **imei-sv**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity - Software Version (IMEI-SV).
- **none**: Specifies that the MME does not need to query for IMEI or IMEI-SV.

verify-equipment-identity [allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency]

Specifies that the identification (IMEI or IMEI-SV) of the UE is to be performed by the Equipment Identity Register (EIR) over the S13 interface.

- **allow-on-eca-timeout**: Configures the MME to allow equipment that has timed-out on ECA during the attach procedure.
- **deny-greylisted**: Configures the MME to deny grey-listed equipment during the attach procedure.
- **deny-unknown**: Configures the MME to deny unknown equipment during the attach procedure.
- **verify-emergency**: Configures the MME to ignore the IMEI validation of the equipment during the attach procedure in emergency cases. This keyword is only supported in release 12.2 and higher.

inter-rat notify-request

Configure inter-RAT parameters for TAU. This keyword provides the operator with the option of sending Notify-Request to HSS from MME during 3G to 4G TAU/HO.

inter-rat security-ctxt { allow-mapped | native }

Configure inter-RAT parameters for TAU. This keyword provides the operator with the option of continuing with the mapped context or creating a new native context after an inter-RAT handover.

- **allow-mapped**: Configures inter-RAT security-context type as mapped. Mapped security context is allowed after inter-RAT handover. This is the default value.
- **native**: Configures inter-RAT security-context type as native only. Inter-RAT handover will always result in a native security context.

Usage Guidelines

Use this command to define tracking area update procedures such as inter-RAT security context and IMEI query-type.

Example

The following command sets the IMEI query type to IMEI-SV:

```
tau imei-query-type imei-sv verify-equipment- identity
```

tcp-maximum-segment-size

This command enables the operator to define a maximum segment size (MSS), that will be used to overwrite received TCP MSS values in uplink/downlink packets between UE and the server.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`tcp-maximum-segment-size` *`size`*
`remove tcp-maximum-segment-size`

remove

Instructs the SGSN to forward the user data without changing the TCP MSS value.

size

This entry specifies the maximum number of octets for a segment. Valid range is 1 to 1460.

Usage Guidelines When configuring with this command, an additional Yes/No prompt is included due to the high impact of the MSS configuration.

Configure the MSS, helps the operator to avoid fragmentation. This command enables the operator to modify or overwrite the TCP MSS value exchanged between the UE and the server (for both 2G and 3G uplink/downlink traffic) if the requested value is more than the SGSN's locally configured value.

Example

Use a command similar to the following to define 1200 octets as the maximum segment size:

`tcp-maximum-segment-size 1200`

timeout

Configure the duration after which the cached MAC to IMSI mapping entry maintained by the IPSG manager during the SaMOG web authorization pre-authentication phase is removed.

Product SaMOG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

timeout imsi cache *timer_value*
{ default | no } timeout imsi cache

default

Sets the timeout duration to its default value.

Default: 1440 minutes

no

If previously configured, removes the timeout duration.

timer_value

timer_value must be an integer between 1 to 20160 minutes.

Usage Guidelines

Use this command to configure the duration after which the cached MAC to IMSI mapping entry of a subscriber device maintained by the IPSG manager during the SaMOG web authorization pre-authentication phase is removed.

Important The SaMOG Web Authorization feature is license dependent. Contact your Cisco account representative for more information on license requirements.

Example

The following command sets a timeout value for clearing the MAC to IMSI mapping entry to 2000 minutes:

timeout imsi cache 2000

treat-as-hplmn

Enables or disables the SGSN to treat an IMSI series as coming from the home PLMN.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*host_name*`(config-call-control-profile-`*profile_name*`)#`

Syntax Description

[remove] treat-as-hplmn

remove

Deletes this configuration from the profile. This would disable this function and is the default.

Usage Guidelines

Use this command to enable or disable the SGSN to treat an IMSI series as coming from the home PLMN.

Example

The following command disables previously configured feature:

```
remove treat-as-hplmn
```

vplmn-address

Enables/disables the SGSN, MME, and ePDG to override the VPLMN address-allowed flag.

Product

ePDG

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
vplmn-address { allowed | not-allowed }
remove vplmn-address
```

remove

Using **remove** disables the override behavior and the VPLMN-Address-Allowed flag is interpreted as it is in the subscription data.

allowed

Using **allowed** instructs the SGSN/MME/ePDG to set the VPLMN-Address-Allowed flag during GGSN/P-GW seletion - even if the flag was not received in the subscription data from the HLR/HSS/AAA.

not-allowed

Using **not-allowed** instructs the SGSN/MME/ePDG not to set the VPLMN-Address-Allowed flag during GGSN/P-GW seletion - even if the flag is received in the subscription data from the HLR/HSS/AAA.

Usage Guidelines

Use this command to override the VPLMN-Address-Allowed flag/AVP received in subscription data from HLR/HSS during GGSN/P-GW selection. This flag is used to decide whether to use the VPLMN-OI received from a roaming subscriber to form the full-APN. The full-APN is then used in a DNS query to select a

GGSN/P-GW. This override enables the operator to control selection of a different GGSN/P-GW for a roaming subscriber by using/not-using VPLMN-OI in full-APN.

Example

The following command instructs the SGSN/MME/ePDG to set the VPLMN-Address-Allowed flag during GGSN/P-GW selection, even if the flag was not received in subscription data from the HLR/HSS/AAA:

vplmn-address allowed

The following command instructs the SGSN/MME/ePDG not to set the VPLMN-Address-Allowed flag during GGSN/P-GW selection, even if the flag was received in subscription data from the HLR/HSS/AAA:

vplmn-address not-allowed

The following command instructs the SGSN/MME/ePDG not to override standard behavior regarding the VPLMN-Address-Allowed flag/AVP:

remove vplmn-address

zone-code

Configures a zone code listing of one or more location area code (LACs) included in the zone.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

zone-code *zc_id* **location-area-code** *lac*
no zone-code *zc_id* **[location-area-code** *lac* **]**

no

Removes either a specific LAC from the zone code list. If the **location-area-code** parameter is not included in the command, then the entire zone code list definition is removed from configuration.

zc_id

Identifies an instance of a zone code list as an integer from 1 to 65535.

An unlimited number of zone code lists can be configured per Call Control Profile as the zone code lists are allocated dynamically.

location-area-code *lac*

Prompts for the location area-code(s), where the subscribers can roam, that are part of the zone. *lac* is an integer from 1 to 65535.

Repeat the **zone-code** command with this keyword to include up to 100 LACs in each zone code list.

Usage Guidelines



Important While there is no limit to the number of zone codes that can be created, only 100 LACs per zone code can be defined.

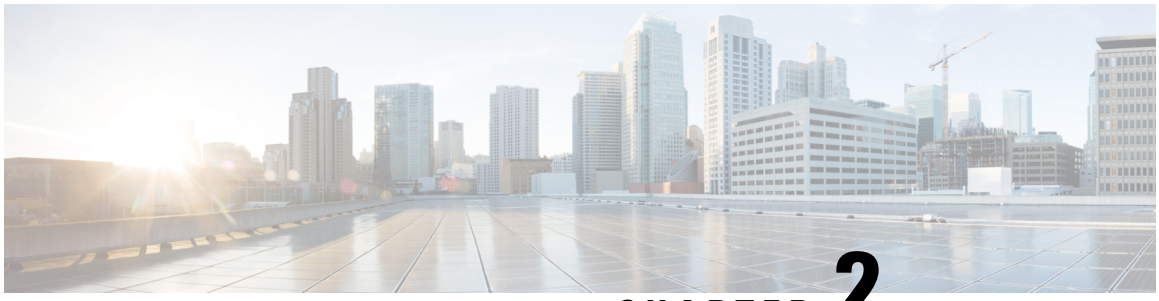
Use this command to define zone code restrictions. Regional subscription data at the home location register (HLR) is used to determine the regional subscription area in which the subscriber is allowed to roam. The regional subscription data consists of a list of zone codes. A zone code is comprised of one or more location areas (identified by a LAC) into which the subscriber is allowed to roam. Regional subscription data, if present in the insert subscriber data (ISD) request from the HLR, defines the subscriber's subscription area for the addressed SGSN. It contains the complete list (up to 10 zone codes) that apply to a subscriber in the currently visited PLMN.

During the GPRS Location Update procedure, the zone code list is received in the ISD request from the HLR. The zone code list from the HLR is validated against the configured values in the operator policy. If matched, then the ISD is allowed to proceed. If not matched, then the ISD response is that the Network Node Area is Restricted and the GPRS Location Update procedure fails. If no zone codes are included in the ISD (whether or not the zone codes are defined in the SGSN configuration), then checking is not done.

Example

The following command defines multiple LACs for zone code 1:

```
zone-code 1 lac 413 212 113
```



CHAPTER 2

Call-Home Configuration Mode

Command Modes

The Call-Home Configuration Mode sets parameters for the Smart Call Home feature. Smart Call Home is a contracted service that sends real-time alerts, remediation, and personalized web-based reports to the Cisco Technical Assistance Center (TAC) and other configured receivers.

Exec > Global Configuration > Call-Home Configuration

configure > call-home

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-home)#
```

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

- activate, on page 223
- alert-group, on page 224
- contact-email-addr, on page 225
- contract-id, on page 226
- customer-id, on page 227
- end, on page 228
- exit, on page 228
- mail-server, on page 228
- phone-number, on page 229
- profile, on page 230
- rate-limit, on page 231
- sender, on page 231
- site-id, on page 232
- street-address, on page 233

activate

Activates the Cisco Smart Call Home service.

Product All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call-Home Configuration

configure > call-home

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-home)#
```

Syntax Description

activate
[default | no] activate

default

Configures the call-home service.

no

Disables the call-home services.

activate

Enables the call-home services.

Usage Guidelines

Use this command to enable the call-home services.

Example

The following command disables the call-home service:

no activate

alert-group

Enables or disables the Smart Call Home alert-group.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call-Home Configuration

configure > call-home

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-home)#
```

Syntax Description

[default | no] alert-group { all | configuration | crashinfo | diagnostic | environment | inventory | syslog }

default

Configures the alert-group back to default settings. The default is enabled.

no

Disables the alert-groups.

alert-group all

Enables an alert group for all categories.

alert-group configuration

Enables an alert group related to configuration.

alert-group crashinfo

Enables an alert group related to crashes.

alert-group diagnostics

Enables an alert group related to diagnostics.

alert-group environment

Enables an alert group related to environment. These typically include events related to power, fan, and temperature alarms.

alert-group inventory

Enables an alert group related to inventory. This is a non-critical event that could include notifications when cards are inserted or removed, or when the system is cold-booted.

alert-group syslog

Enables an alert group related to syslog. This includes events generated by the syslog PORT facility.

Usage Guidelines

An alert group is a predefined subset of Smart Call Home alerts that are supported on this device. Alert groups allow you to select the set of Smart Call Home alerts that you want to send to a predefined or custom destination profile.

Example

The following command enables alerts for all of the preconfigured Smart Call Home alerts:

```
alert-group all
```

contact-email-addr

Sets the e-mail address of the person identified as the prime contact for this system.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call-Home Configuration

configure > call-home

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-home)#
```

Syntax Description **`[ no ] contact-email-addr`** *email_addr*

no

Removes the contact e-mail address.

contact-email-addr *email_addr*

Specifies the information for prime contact as an alphanumeric string in the format *local-part@domain*, where domain can be made up of a number of labels, each separated by a period and between 1 and 63 characters in length. The local-part can be 1-64 characters. The domain-label can be 1-63 characters. The domain can be 1 through 135 characters. The entire alphanumeric string can be a no larger than 200 characters.

Usage Guidelines Use this command to set up the e-mail address for the person identified as the contact person for this device.

Important You can enter any valid e-mail address. You cannot use spaces.

Example

The following command specifies e-mail address for the entity *notity.TAC@NOCservices.net*:

`contact-email-addr notity.TAC@NOCservices.net`

contract-id

Configures the system's contract-identifier for Cisco AutoNotify.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call-Home Configuration

configure > call-home

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-home)#
```

Syntax Description **`[ default | no ] contract-id`** *`contractID`*

default

Configures the call-home contract-id back to default settings.

no

Removes the call-home contract-id.

contract-id *contractID*

Specifies the call-home contract-id as an alphanumeric string of 1 through 64 characters that is case sensitive. If you include spaces in this string, you must enclose it in double quotation marks.

Usage Guidelines Use this command to enter this system's AutoNotify contract ID.

Example

The following command specifies the contract-id as *Contract1234_ID*:

`contract-id Contract1234_ID`

customer-id

Configures the system's customer-identifier for Cisco AutoNotify.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call-Home Configuration

configure > call-home

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-home)#`

Syntax Description **`[ default | no ] customer-id`** *`customerID`*

default

Configures the call-home customer-id back to default settings.

no

Removes the call-home customer-id.

customer-id *customerID*

Specifies the call-home customer-id as an alphanumeric string of 1 through 64 characters that is case sensitive. If you include spaces in the string, you must enclose it in double quotation marks.

Usage Guidelines Use this command to set up the system's customer ID for Cisco's AutoNotify.

Example

The following command specifies the customer-id as *CustID_1234*:

```
customer-id CustID_1234
```

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.

mail-server

Configures the Smart Call Home mail-server.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call-Home Configuration

configure > call-home

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-home)#
```

Syntax Description **`[ no ] mail-server`** *`server_name`* **`priority`** *`priority_num`*

no

Removes the call-home mail-server.

mail-server *server_name*

Identifies the mail server as an alphanumeric string of 1 through 64 characters. The server ID can take the form of a host name (DNS) or an IPv4 address in dotted-decimal notation.

priority

Sets the mail server priority order as an integer from 1 (highest) to 100 (lowest).

Usage Guidelines Use this command to set up the mail server for Smart Call Home. This configuration is mandatory when the user profile is configured to only send out e-mail messages.

Example

The following command specifies the mail-server as *10.2.3.4* with a priority of *1*:

```
mail-server 10.2.3.4 priority 1
```

phone-number

Enables or disables the phone-number for the Smart Call Home contact person.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call-Home Configuration

configure > call-home

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-home)#
```

Syntax Description **`[ no | default ] phone-number`** *`phone-number-string`*

default

Configures the phone number back to default settings. The default is enabled.

no

Removes the call-home phone number.

phone-number *phone-number-string*

Specifies the phone number for the contact person for this system as an alphanumeric string that can only contain: + (plus sign), - (dash) and numbers. The total length of the string is 12 to 16 characters. If you include spaces, you must enclose the string in double quotation marks.

Usage Guidelines

Use this command to set up the phone number for Smart Call Home contact.

Example

The following command specifies the phone number as *+866-111-2234*:

```
phone-number 866-111-2234
```

profile

Creates the Smart Call Home profile.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call-Home Configuration

configure > call-home

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-home)#
```

Syntax Description

`[ no ] profile` *`profile_name`*

no

Removes the call-home profile.

profile *profile_name*

Creates or modifies the profile name for this system as an alphanumeric string of 1 through 31 characters.

Usage Guidelines

Use this command to create a new profile or modify an existing profile. This command moves you to the Call-Home Profile Configuration mode.

Example

The following command creates a profile named *Profile_1*:

```
profile Profile_1
```

rate-limit

Enables or disables the message rate-limit for Smart Call Home features.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call-Home Configuration

configure > call-home

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-home)#
```

Syntax Description

[no | default] rate-limit *message_count*

default

Sets the rate limit back to the default of 20 messages per minute.

no

Removes the call-home rate-limit.

rate-limit *message_count*

Sets the rate limit in messages per minute. *message_count* is an integer from 1 to 60. Default: 20

Usage Guidelines

Use this command to configure the call-home message rate limit per minute. The default is 20 messages per minute.

Example

The following command sets the call-home rate limit to *10*:

```
rate-limit 10
```

sender

Specifies the Smart Call Home e-mail settings for the "from" address and "reply-to" address.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call-Home Configuration

configure > call-home

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-home)#
```

Syntax Description

`[ no | default ] sender { from email_address | to email_address }`

default

Sets the sender back to the default.

from *email_address*

Sets the sender's reply from address.

no

Removes the call-home sender.

to *email_address*

Sets the sender's reply-to address.

email_address

This is an alphanumeric string in the format *local-part@domain*, where domain can be made up of a number of labels, each separated by a period and between 1 and 63 characters in length. The local-part can be 1-64 characters. The domain-label can be 1-63 characters. The domain can be 1 through 135 characters. The entire alphanumeric string can be a no larger than 200 characters.

Usage Guidelines

Use this command to specify the e-mail settings for the sender. This command sets the "to" and "from" fields in the e-mail.

Example

The following command sets the from address to *notity.TAC@NOCservices.net* and the reply-to address to *support@cisco.com*:

`semder from notity.TAC@NOCservices.net to support@cisco.com`

site-id

Specifies the Smart Call Home site identifier for this system.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call-Home Configuration

configure > call-home

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-home)#
```

Syntax Description **`[ default | no ] site-id`** *`siteID`*

default

Sets the site-id back to the default.

no

Removes the call-home site-id.

site-id *siteID*

Specifies the site ID as an alphanumeric string of 1 through 200 characters. If you include spaces, then you must enclose your entry in quotes.

Usage Guidelines Use this command to specify the Smart Call Home site identifier for this system.

Example

The following command sets the site-id to *NOC_Services_site_1011*:

```
site id NOC_Services_site_1011
```

street-address

Specifies the Smart Call Home street address for the system.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call-Home Configuration

configure > call-home

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-home)#
```

Syntax Description **`[ default | no ] street-address`** *`streetADR`*

default

Sets the street-address back to the default.

no

Removes the call-home street-address.

street-address *streetADR*

Specifies e Smart Call Home street-address as an alphanumeric string of 1 through 200 characters. You can include the street address, City, State, and ZIP Code. If you include spaces, then you must enclose the string in double quotation marks.

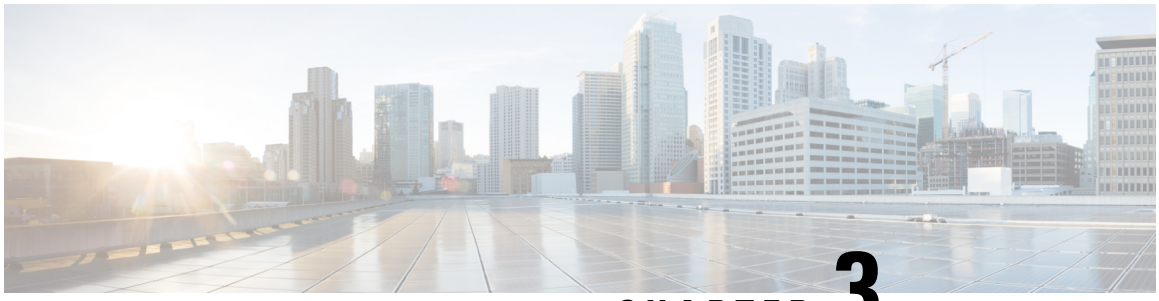
Usage Guidelines

Use this command to set up the street address for the system.

Example

The following command sets the street address to *123 Main St., Chicago, IL 60000*:

```
street-address "123 Main St., Chicago, IL 60000"
```



CHAPTER 3

Call-Home Profile Configuration Mode

Command Modes

The Call-Home Profile Configuration Mode is used to create groups of users that will receive alerts when events occur. The Smart Call Home service sends real-time alerts, remediation, and personalized web-based reports to the Cisco Technical Assistance Center (TAC) and other configured receivers.

Exec > Global Configuration > Call-Home Configuration > Call-Home Profile Configuration

configure > call-home > profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-home-profile)#
```

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

- active, on page 235
- destination, on page 236
- end, on page 238
- exit, on page 238
- subscribe-to-alert-group, on page 238

active

Activates this Smart Call Home profile.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call-Home Configuration > Call-Home Profile Configuration

configure > call-home > profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-home-profile)#
```

Syntax Description

```
active
default active
no active
```

default

Configures the call-home profile back to default settings. By default, the profile is enabled.

no

Deletes the call-home profile.

activate

Activates this Smart Call Home profile.

Usage Guidelines

Use this command to activate or deactivate this call-home profile. By default, the profile is enabled.

Example

The following command disables the call-home profile:

```
no active
```

destination

Configures the message destinations for this Smart Call Home profile.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call-Home Configuration > Call-Home Profile Configuration

configure > call-home > profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-home-profile)#
```

Syntax Description

```
destination [ address [ email email_address | http http_url ] |
message-size-limit size | preferred-msg-format [ long-text | short-text |
 xml ] | transport-method [ email email_address | http http_url] ]
default destination [ message-size-limit | preferred-msg-format |
transport-method ]
no destination [ address [ email email_address | http http_url ] |
message-size-limit size | preferred-msg-format [ long-text |short-text |
xml ] | transport-method [ email email_address | http http_url ] ]
```

address [email *email_address* | http *http_url*]

Configures an destination e-mail address or HTTP URL where short-text/long-text call-home message and XML-based call-home messages will be sent.

- **email**: Use this option to add an e-mail address to this profile. *email_addr* is an alphanumeric string of the form *local-part@domain* where domain can be made up of a number of labels, each separated by a period and between 1 and 63 characters in length. The local-part can be 1-64 characters. The domain-label can be 1-63 characters. The domain can be 1-135 characters. The entire alphanumeric string can be a no larger than 200 characters.
- **http**: Use this option to add an HTTP URL to this profile. *http_url* is an alphanumeric string of 1 through 200 characters.

default

Configures the call-home profile back to default settings. By default, the profile is enabled.

message-size-limit *size*

Specifies the message size (in bytes) for this profile as an integer from 50 to 3145728. The default is 3145728.

no

Deletes the call-home profile.

preferred-msg-format [long-text | short-text | xml]

Specifies the message format for the profile. The default is xml.

- **long-text**: Use this option to set long-text messages as the preferred message format. The long message format has all the details related to the event, including information related to chassis, card, and outputs of show commands for the alert group.
- **short-text**: Use this option to set short-text messages as the preferred message format. The short message has information on the severity of event, a short description of the event, the event time, and the device ID.
- **xml**: Use this option to set XML as the preferred message format. (Default)

transport-method [email *email_address* | http *http_url*]]

Specifies the transport-method for the messages. The default is e-mail. For the user profile, both e-mail and http can be enabled. If all are options are disabled, e-mail will be set for the profile.

For the Cisco TAC profile, only one transport method can be enabled. If the user enables a second transport method, the first one will be automatically disabled.

- **email**: Enables an e-mail address for this profile. This is the default.
- **http**: Enables an HTTP URL for this profile.

Usage Guidelines

Use this command to activate the current call-home profile. By default, the profile is enabled.

Example

The following command disables the call-home profile:

```
no destination
```

The following command sets the preferred message format for the profile to the call-home profile to short text:

```
destination preferred-msg-format short-text
```

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.

subscribe-to-alert-group

Subscribes this profile to the alert group for the call-home profile.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call-Home Configuration > Call-Home Profile Configuration

configure > call-home > profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-home-profile)#
```

Syntax Description

subscribe-to-alert-group [all {severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] } | configuration { periodic [daily | monthly | weekly] } | crashinfo | diagnostic { severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] } | environment { severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] } | inventory { periodic [daily | monthly | weekly] } | syslog {severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] }]
default subscribe-to-alert-group
no subscribe-to-alert-group [all {severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] } | configuration { periodic [daily | monthly | weekly] } | crashinfo | diagnostic {severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] } | environment {severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] } | inventory { periodic [daily | monthly | weekly] } | syslog {severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] [pattern *pattern_to_match*] }]

all {severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] }

Enables call-home messages based for all group-types and severity for the profile. The following severities are supported:

- **catastrophic**– Level 1: catastrophic event, matches platform logging level critical.
- **disaster** – Level 2: disaster event, matches platform logging level critical.
- **fatal** – Level 3: fatal event, matches platform logging level critical.
- **critical** – Level 4: critical event, matches platform logging level critical.
- **major** – Level 5: major event, matches platform logging level error.
- **minor** – Level 6: minor event, matches platform logging level warning.
- **warning** – Level 7: warning event, matches platform logging level warning.
- **notification** – Level 8: notification event, matches platform logging level unusual.
- **normal** – Level 9: normal event, matches platform logging level info.

configuration { periodic [daily | monthly | weekly] }

Enables call-home messages based for configuration alert groups. The messages are sent at periodic intervals such as:

- **daily**: Sends a daily call-home message.
- **monthly**: Sends a monthly call-home message.
- **weekly**: Sends a weekly call-home message.

crashinfo

Configures the call-home profile back to default settings. By default, the profile is enabled.

default

Restores the parameter back to the default value.

diagnostic { severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] }

Enables call-home messages based for diagnostic group-types and severity for the profile. The following severities are supported:

- **catastrophic**– Level 1: catastrophic event, matches platform logging level critical.
- **disaster** – Level 2: disaster event, matches platform logging level critical.
- **fatal** – Level 3: fatal event, matches platform logging level critical.
- **critical** – Level 4: critical event, matches platform logging level critical.
- **major** – Level 5: major event, matches platform logging level error.
- **minor** – Level 6: minor event, matches platform logging level warning.
- **warning** – Level 7: warning event, matches platform logging level warning.
- **notification** – Level 8: notification event, matches platform logging level unusual.
- **normal** – Level 9: normal event, matches platform logging level info.

environment {severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] }

Enables call-home messages based for environment group-types and severity for the profile. The following severities are supported:

- **catastrophic**– Level 1: catastrophic event, matches platform logging level critical.
- **disaster** – Level 2: disaster event, matches platform logging level critical.
- **fatal** – Level 3: fatal event, matches platform logging level critical.
- **critical** – Level 4: critical event, matches platform logging level critical.
- **major** – Level 5: major event, matches platform logging level error.
- **minor** – Level 6: minor event, matches platform logging level warning.
- **warning** – Level 7: warning event, matches platform logging level warning.
- **notification** – Level 8: notification event, matches platform logging level unusual.
- **normal** – Level 9: normal event, matches platform logging level info.

inventory { periodic [daily | monthly | weekly] }

Enables call-home messages based for inventory alert groups. The messages are sent at periodic intervals such as:

- **daily**: Sends a daily call-home message.
- **monthly**: Sends a monthly call-home message.
- **weekly**: Sends a weekly call-home message.

no

Deletes the alert groups.

syslog { severity [catastrophic | diasaster | fatal | critical | major | minor | warning | notification | normal] [pattern *pattern_to_match*] }]

Enables and disables call-home messages based on severity and syslog string pattern match for the profile. The following severities are supported:

- **catastrophic**– Level 1: catastrophic event, matches platform logging level critical.
- **disaster** – Level 2: disaster event, matches platform logging level critical.
- **fatal** – Level 3: fatal event, matches platform logging level critical.
- **critical** – Level 4: critical event, matches platform logging level critical.
- **major** – Level 5: major event, matches platform logging level error.
- **minor** – Level 6: minor event, matches platform logging level warning.
- **warning** – Level 7: warning event, matches platform logging level warning.
- **notification** – Level 8: notification event, matches platform logging level unusual.
- **normal** – Level 9: normal event, matches platform logging level info.

pattern_to_match is an alphanumeric string of 1 through 80 characters.



Note If no *pattern_to_match* is specified, the system will use a ".*" (dot asterisk) pattern.

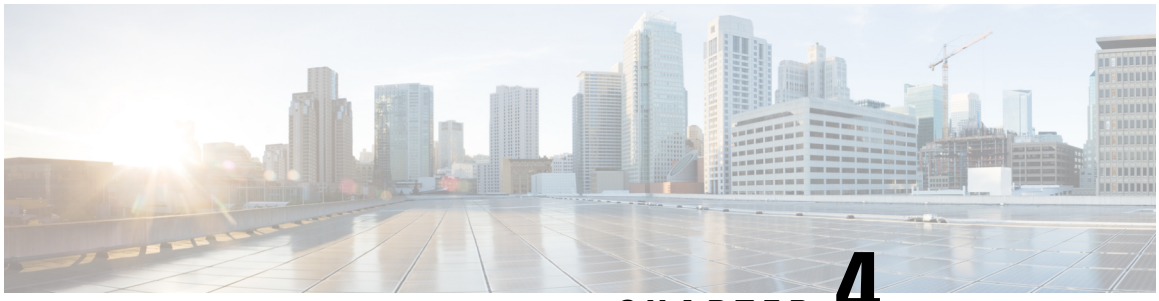
Usage Guidelines

Use this command to enable or disable the call-home messages based on specified alert-groups and severities for the profile.

Example

The following command sets an alert group for the profile to send a daily inventory message:

```
subscribe-to-alert-group inventory periodic daily
```



CHAPTER 4

CAMEL Service Configuration Mode Commands

CAMEL service enables operators of 2.5G/3G networks to provide operator-specific services (such as prepaid GPRS service and prepaid SMS service) to subscribers, even when the subscribers are roaming outside their home public land mobile network (HPLMN).

Command Modes

The CAMEL Service configuration mode provides a set of commands to define the parameters for the Customized Applications for Mobile networks Enhanced Logic (CAMEL) service functionality and the CAMEL interface - the Ge interface.

Exec > Global Configuration > Context Configuration > CAMEL Service Configuration

configure > context *context_name* **> camel-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-camel-service)#
```



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

- associate-sccp-network, on page 243
- end, on page 244
- exit, on page 244
- tcap destination-address, on page 245
- timeout, on page 245

associate-sccp-network

Configure an association between this CAMEL service and a specified SCCP network.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > CAMEL Service Configuration

configure > context *context_name* **> camel-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-camel-service)#
```

Syntax Description

associate-sccp-network *sccp_network_id*
no associate-sccp-network

no

Removes the association with the CAMEL service configuration.

sccp_network_id

Identifies an already defined SCCP network.

sccp_network_id: Enter an integer from 1 to 12.

Usage Guidelines

The SCCP network must be configured prior to use this command.

CAMEL service will not function unless an SCCP network is associated.

Example

Associate this CAMEL service with SCCP network configuration ID 2:

associate-sccp-network2

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.

tcap destination-address

Configure the gsmSCF address to be used to open TC dialogues.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CAMEL Service Configuration

configure > context *context_name* **> camel-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-camel-service)#
```

Syntax Description

tcap destination-address { configured-address | received-address }
default tcap destination-address

configured-address

Default.

Instructs the SGSN to use the SCF address from the GPRS-CSI.

received-address

Instructs the SGSN to overwrite the gsmSCF address with the memorised gsmSCF address that was in the first response message to the InitialDPGPRS and then to use that gsmSCF address.

Usage Guidelines

This command enables the operator to determine which gsmSCF address is to be used to open new TC dialogues. In accordance with 3GPP 29.078, section 14.1.4.1.3, this command enables the SGSN to establish new TC dialogues within the context of a current GPRS dialogue, based on the operators choice:

- to use a 'received-address' where the gprsSSF learns the gsmSCF address used in the first response message to the InitialDPGPRS and uses it to open new TC dialogues, or
- to use a 'configured-address' where the gprsSSF uses the gsmSCF address from the GPRS-CSI to open new TC dialogues.

Example

Configure the SGSN to overwrite the SCF address and to use the gsmSCF address received in the response message:

tcap destination-address received-address

timeout

Configure a range of timers needed to support CAMEL service.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CAMEL Service Configuration

configure > context *context_name* **> camel-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-camel-service)#
```

Syntax Description

```
timeout { gprs-apply-charging-report-ack-timer seconds |
gprs-entity-release-ack-timer seconds | gprs-event-report-ack-timer seconds
 | gprs-tssf-timer seconds | sms-event-report-ack-timer seconds |
sms-tssf-timer seconds | tc-guard-timer seconds }
default timeout { gprs-apply-charging-report-ack-timer |
gprs-entity-release-ack-timer | gprs-event-report-ack-timer |
gprs-tssf-timer | sms-event-report-ack-timer | sms-tssf-timer |
tc-guard-timer }
```

default

Resets the timers to default values.

gprs-apply-charging-report-ack-timer *seconds*

Configure the TCAP invoke timer to set the length of time the SGSN waits for an acknowledgement after sending an ApplyChargingReportGPRS to the SCF.

seconds: Enter an integer from 1 to 20. Default: 4

Important This timer value should be less than the value configured for the tc-guard-timer.

gprs-entity-release-ack-timer *seconds*

Configure the TCAP invoke timer to set the length of time the SGSN waits for an acknowledgement from the SCF after sending Entity Release information.

seconds: Enter an integer from 1 to 20. Default: 4

gprs-event-report-ack-timer *seconds*

Configure the TCAP invoke timer to set the length of time the SGSN waits for an acknowledgement from the SCF after the SGSN sends an event report.

seconds: Enter an integer from 1 to 20. Default: 4

gprs-tssf-timer *seconds*

Configure the GPRS TSSF timer to set the length of time the SGSN waits for an instructions from the SCF. On expiry the SGSN handles the transaction through the default handling specified in the corresponding CSI.

seconds: Enter an integer from 1 to 10. Default: 5

sms-event-report-ack-timer *seconds*

Configure the TCAP invoke timer to set the length of time the SGSN waits for an acknowledgement from the SCF after the SGSN sends an event report for SMS.

seconds: Enter an integer from 1 to 20. Default: 4

sms-tssf-timer *seconds*

Configure the SMS TSSF timer to set the length of time the SGSN waits for an instructions from the SCF. On expiry the SGSN handles the transaction through the default handling specified in the corresponding CSI.

seconds: Enter an integer from 1 to 10. Default: 5

tc-guard-timer *seconds*

Configure the guard tier to start when the SGSN sends ApplyChargingReportGPRS to the SCF. On expiry the SGSN closes the TCAP dialogue if the GPRS Dialogue state is "monitoring". Default handling complies with 3GPP 23.078.

seconds: Enter an integer from 1 to 10. Default: 5

Important This timer value should be greater than the value configured for the gprs-apply-charging-report-ack-timer.

Usage Guidelines

The SCCP network must be configured prior to use this command.

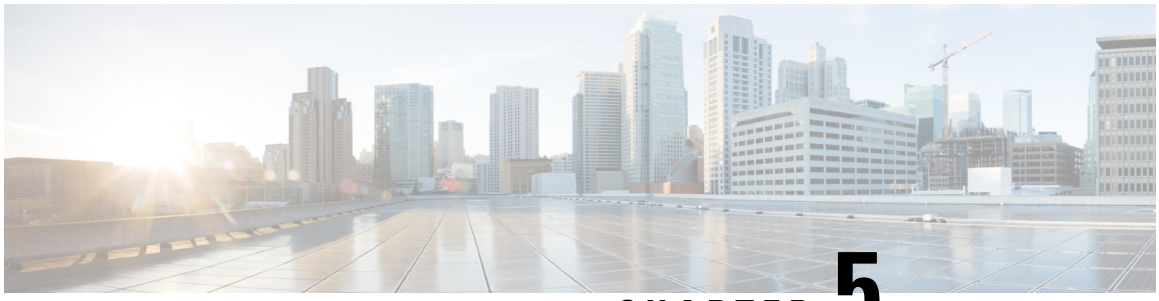
CAMEL service will not function unless an SCCP network is associated.

Repeat the command to configure multiple timers.

Example

Set the tc-guard timer for 4:

```
tc-guard-timer 4
```



CHAPTER 5

Card Configuration Mode Commands

Command Modes

Use the Card configuration mode to create and manage the physical cards in the chassis.

Exec > Global Configuration > Card Configuration

configure > card *card_number*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-card- slot_number)#
```

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

- end, on page 249
- exit, on page 249
- link-aggregation, on page 250
- mode, on page 251
- shutdown, on page 252

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.

link-aggregation

Configures system priority and toggle link settings for Link Aggregation. These parameters are usually changed to match the feature requirements of the remote Ethernet switch.

Product WiMAX

PDSN

HA

FA

GGSN

SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Card Configuration

configure > **card** *card_number*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-card-` *`slot_number`*`)#`

Syntax Description **`link-aggregation { system-priority`** *`priority`* **`| toggle-link } [-noconfirm ] { default | no } link-aggregation { system-priority | toggle-link } [-noconfirm ]`**

default

Resets the configuration to the default.

link-aggregation system-priority *priority*

This command sets the system priority used by Link Aggregation Control Protocol (LACP) to form the system ID.

priority is a hexadecimal value from 0x0000 through 0xFFFF. Default is 0x8000 (32768).

toggle-link

Sets the system to toggle link on port switch.

-noconfirm

Executes the command without additional prompting for command confirmation.

Usage Guidelines

The system MAC address (6 bytes) and system priority (2 bytes) combine to form the system ID. A system consists of a packet processing card and its associated ASR 5500 MIO traffic ports. The highest system ID priority (the lowest number) handles dynamic changes.

For additional usage and configuration information for the link aggregation feature, refer to the *System Administration Guide*.



Important Not supported on all platforms

Example

The following command configures the link aggregation system-priority to 10640 (*0x2990*):

```
link-aggregation system-priority 0x2990
```

mode

Sets the application processor card's current administrative state to active or standby.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Card Configuration

configure > card *card_number*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-card- slot_number)#
```

Syntax Description

```
mode { active | standby } [ -noconfirm ]
default mode [ -noconfirm ]
```

default

Returns the mode to the default value appropriate to the card type.

The default administrative mode for line cards affects a single card and its mated line card. The default state for line cards in the top shelf is active. The default for line cards in the bottom shelf is standby.

The default administrative state for the SPIO in slot 24 is active and the SPIO in slot 25 is standby.

The default administrative mode for packet processing cards is standby.

Important This command results in a migration of processes if the default mode for a card is different than the current state of the card.

active

Defines which card type is to be switched from standby to active state. If a card is present in the slot, the packet processing card is automatically selected depending upon the type of card. If no card is present in the slot, a packet processing card is assumed.

standby

Sets the packet processing card in the slot to standby mode.

Caution Switching an active packet processing card to standby deletes all port configurations, including bindings, for the attached line cards.

-noconfirm

Executes the command without additional prompting for command confirmation.

Usage Guidelines

Set the desired mode of mated cards. The card targeted for maintenance is placed in the standby state first.

The setting of the mode determines which packet processing cards are to be active and which are to be the standby cards for redundancy. Use this command to configure the set of active and standby packet processing cards. The application processor card's standby priority is then used in conjunction with the set of standby packet processing cards to determine the order in which the standby cards are used for redundancy support.

Important Not supported on all platforms

Important This command results in a migration of processes if the mode specified for the card is different than the current state of the card.

Example

The following commands set the state of a card to active and standby, respectively.

```
mode active
mode standby
```

shutdown

Configures a card for active service or terminates all processes on the card.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Card Configuration

configure > card *card_number*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-card- `*`slot_number`*`)#`

Syntax Description

`[ no ] shutdown`

no

no shutdown enables the card.

Enter only the **shutdown** keyword to shut the card down.

Usage Guidelines

Shut down a card to remove it from service or to enable a card to put it into service.

Important Do not use this command to remove a card from service for maintenance. Use the command **card halt** to remove a card for service to avoid changing or deleting the active-mode configuration. See the Exec Mode chapter.

Important Not supported on all platforms

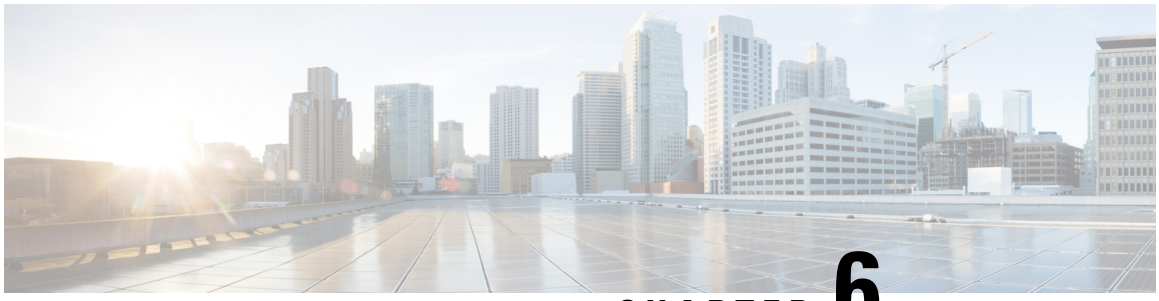
Example

The following command shuts down the card:

`shutdown`

The following command switches the card to online:

`no shutdown`



CHAPTER 6

CBS Service Configuration Mode Commands

Important In Release 20 and later, HNBGW is not supported. Commands in this configuration mode must not be used in Release 20 and later. For more information, contact your Cisco account representative.

The Cell Broadcasting Service (CBS) Configuration Mode is used to create and manage CBS service instances for the current context.

Command Modes Exec > Global Configuration > Context Configuration > Cell Broadcasting Service Configuration

configure > context *context_name* **cbs-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-cbs-service)#`

- bind, on page 255
- cbc-address-validation, on page 256
- cbc-server, on page 257
- end, on page 258
- exit, on page 258
- sabp timer, on page 258
- sabp-class2-aggregation, on page 259
- tcp-keepalive, on page 259
- tcp-mode, on page 260

bind

This command binds the CBS service to the IP address of a logical interface.

Product HNB-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Cell Broadcasting Service Configuration

configure > context *context_name* **cbs-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cbs-service)#
```

Syntax Description

```
bind address ip_address port port_number
no bind address
```

no

Removes a previously configured binding.

ip_address

Specifies the IPv4 type IP address of CBS service. *ip_address* must be expressed in IPv4 dotted-decimal notation.

port

Specifies the TCP port of the CBS service. *port_number* is an integer between 1 and 65535. Standard port used for service area broadcast ptotocol (SABP) is 3452 in case no other port is configured. It is an optional parameter.

Usage Guidelines

Use this command to associate or tie a CBS service to a specific logical IP address previously configured in the current context and bound to a port.

Example

The following command binds the CBS service to the interface with an IP address of *92.168.1.111* having port number 8888:

```
bind address 192.168.1.111 port 8888
```

cbc-address-validation

This command is used for validation of Cell Broadcasting Centre IP address.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax Description

```
[ no ] cbc-address-validation
```

no

Disables the validation of Cell Broadcasting Centre IP address.

Usage Guidelines

Use this command to validate the Cell Broadcasting Centre IP address.

Example

The following command validates the Cell Broadcasting Centre IP address:

cbc-address-validation

cbc-server

This command configures the CBC server for cell broadcasting service.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Cell Broadcasting Service Configuration

configure > context *context_name* **cbs-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-cbs-service)#`

Syntax Description

cbc-server address *ipv4_address* **[port** *port_number* **] [secondary-address** *ipv4_address* **[port** *port_number* **]]**
no cbc-server address

no

Disables the previously configured CBC server.

ip4_address

Specifies the IPv4 type IP address of CBC server. *ip_address* must be expressed in IPv4 dotted-decimal notation.

port

Specifies the TCP port of the CBS service. *port_number* is an integer between 1 and 65535. Standard port used for service area broadcast ptotocol (SABP) is 3452 in case no other port is configured. It is an optional parameter.

secondary-address

Specifies the address of other CBC server.*ipv4_address* is an IPv4 address, using dotted-decimal notation

Usage Guidelines

Use this command to configure the CBC server.

Example

The following command configures a CBC server with an IP address of *92.168.1.112* having default port number 3452::

cbc-server*92.168.1.112*

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.

sabp timer

Configures the Service Area Broadcast Protocol (SABP) procedure timer value.

Product HNB-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Cell Broadcasting Service Configuration

configure > context *context_name* **cbs-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-cbs-service)#`

Syntax Description **`[ default | no ] sabp timer`***`timer_value`*

default

Restores the SABP timer value to the default: 10 seconds.

no

Disables the previouly configured SABP timer value.

sabp timer

Configures the SABP timer which is the wait time for receiving the SABP response from a peer. *timer_value* is an integer value between 1 and 30.

Usage Guidelines

This command is used to set/restore the SABP timer value.

Example

The following command configures the SABP timer value to 25:

```
sabp timer 25
```

sabp-class2-aggregation

This command configures the SABP class-2 aggregation timeout.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax Description

```
sabp-class2-aggregation timeout timeout_value
[ default | no ] sabp-class2-aggregation timeout
```

default

Restores the SABP class-2 aggregation timeout value to the default: 2 seconds.

no

Disables the previouly configured SABP class-2 aggregation timeout value.

sabp-class2-aggregation timeout

Configures the SABP class-2 aggregation timeout value. *timeout_value* is an integer value between 1 and 10.

Usage Guidelines

This command is used to configure the SABP class-2 aggregation timeout.

Example

The following command configures the SABP class-2 aggregation timeout value to 6:

```
sabp-class2-aggregation timeout 6
```

tcp-keepalive

This command is TCP Keepalive timer. It is used to check liveness of Cell Broadcasting Centre. The CBS service must be restarted after setting new values.

Product HNB-GW

Privilege Security Administrator, Administrator

Syntax Description

```
tcp-keepalive idle-timeout idle_timeout_value max-retransmission-count count
  interval value
[ default | no ] tcp-keepalive
```

default

Restores the TCP Keepalive timer related values to default: idle-timeout(600 seconds), max-retransmission-count (3) and interval (30 seconds).

no

Disables the TCP Keepalive timer.

tcp-keepalive idle-timeout

This is the time in seconds to wait before checking the liveness of Cell Broadcasting Centre. *timeout_value* is an integer value between 60 and 7200.

max-retransmission-count

This is the number of attempts to check liveness of Cell Broadcasting Centre after idle time. *count* is an integer value between 2 and 10.

interval

This is the time in seconds between attempts to check liveness of Cell Broadcasting Centre after idle time. *value* is an integer value between 10 and 100.

Usage Guidelines This command is used to check the liveness of Cell Broadcasting Centre.

Example

The following command checks the liveness of Cell Broadcasting Centre with **tcp-keepalive idle-timeout** as 66 seconds, **max-retransmission-count** as 5 and **interval** as 15:

```
tcp-keepalive idle-timeout 66 max-retransmission-count 5 interval 15
```

tcp-mode

This comand configures the mode of TCP connection.

Product HNB-GW

Privilege Security Administrator, Administrator

Syntax Description

```
tcp-mode { client-server | server-only }
```

client-server

This specifies that the HNBGW can act either as client or server.

server-only

This specifies that the HNBGW can act only as server.

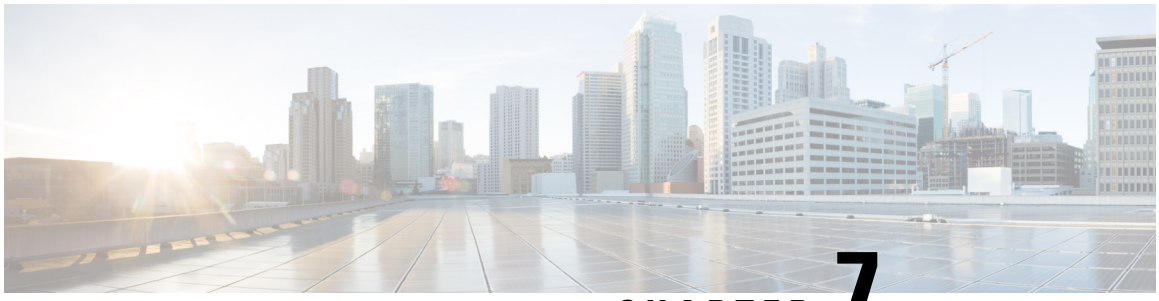
Usage Guidelines

This command is used to configure the mode of TCP connection.

Example

The following command configures the HNBGW as Client and Server.

```
tcp-mode client-server
```



CHAPTER 7

Cell Trace Module Configuration Mode Commands

The Cell Trace Module Configuration Mode provides the commands to configure real time cell traffic trace parameters in a context.

Command Modes

Exec > Global Configuration > Context Configuration > Cell Trace Module Configuration

configure > context *context_name* **> cell-trace-module**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cell-trace)#
```

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

- cell-trace, on page 263
- do show, on page 265
- end, on page 266
- exit, on page 266
- file, on page 266

cell-trace

This command allows you to configure the Cell Traffic Trace transfer parameters.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Cell Trace Module Configuration

configure > context *context_name* **> cell-trace-module**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cell-trace)#
```

Syntax Description

```
cell-trace { purge { { storage-limit storage_limit  | time-limit time_limit
} [ max-files max_files ] } | push-interval interval | push-trigger {
space-usage-percent usage_precent } | remove-file-after-transfer |
transfer-mode { pull [ module-only ] | push primary { encrypted-url enc_url
 | url url [ module-only ] } | use-harddisk }
default cell-trace [ purge | push-interval | push-trigger |
remove-file-after-transfer | transfer-mode | use-harddisk ]
no cell-trace [ purge | remove-file-after-transfer | use-harddisk ]
```

default

Configures this command with its default setting for the specified cell traffic trace parameters.

no

Deletes the specified cell traffic trace parameters.

purge { { storage-limit*storage_limit* | time-limit *time_limit* } [max-files *max_files*] }

Specifies to purge or delete the cell trace records based on "time" or "volume" to restrict hard-disk space usage for cell trace records.

storage-limit *storage_limit*: Specifies the storage space for the record files, in megabytes. *storage_limit* must be an integer from 10 to 143360.

time-limit *time_limit*: Specifies the time to delete record files, in seconds. *time_limit* must be an integer from 600 to 2592000.

max-files *max_files*: Specifies the maximum number of records to purge per iteration. *max_files* must be an integer 0 or ranging from 1000 to 10000. When value is set to 0, it deletes all records until purge limit is reached.

By default, no purge operation is performed by the VPNMGR module.

push-interval *interval*

Specifies the transfer interval in seconds to push cell traffic trace files to an external file server. *interval* must be an integer from 1 to 30.

Default: 1 second

push-trigger { space-usage-percent *usage_precent* }

Configures the disk utilization trigger for cell traffic trace files.

space-usage-percent *usage_precent*: Specifies the disk utilization percentage for triggering PUSH. *usage_precent* must be an integer from 10 to 80.

remove-file-after-transfer

Deletes the files from RAMFS after transfer to an external server. If the **cell-trace use-harddisk** command is not configured, it is recommended to use this command.

transfer-mode { pull [module-only] | push primary { encrypted-url *enc_url* | url *url* } [module-only] }

Configures the transfer mode for cell trace record files. Only one TCE address configuration is required and all files will be sent to this address irrespective of the TCE address received from eNodeB in S1AP cell tracing message. Both the addresses must be the same mostly.

pull [module-only]: Specifies that external storage pulls the cell trace files.

push primary { encrypted-url *enc_url* **| url** *url* **} [module-only]**: Specifies that ST pushes the cell trace files onto the configured external storage server. *enc_url* specifies the location where the cell trace files will be transferred and must be entered in encrypted format. *url* specifies the location where the cell trace files will be transferred and must be entered in the server URL format *scheme://user:password@host:[port]/directory* - string of size 1 to 1024.

If the **module-only** keyword is set, then the given configuration is applied only for the specific record type. The administrator can configure record transfer information for all record types separately or combined using the **module-only** keyword.

pull [module-only]:

Server URL in the format: scheme://user:password@host:[port]/directory - string of size 1 to 1024

If the **module-only** keyword is set, then the given configuration is applied only for the specific record type. The administrator can configure record transfer information for all record types separately or combined using the **module-only** keyword.

use-harddisk

Moves the cell trace files from RAMFS to */hd-raid/* and then transferred to an external server. It is recommended to use this command to prevent space on RAMFS becoming full.

Usage Guidelines

Use this command to configure the Cell Traffic Trace transfer parameters. The user must be in a non-local context when specifying the **cell-trace-module** command.

Example

The following command pushes the cell traffic trace files to an external file server in *20* seconds:

```
cell-trace push-interval 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.

file

This command allows you to configure the file creation properties for cell trace records.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Cell Trace Module Configuration

configure > context *context_name* **> cell-trace-module**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cell-trace)#
```

Syntax Description

```
file [ delete-timeout seconds | directory directory_name | field-separator {
hyphen | omit | underscore } | rotation { num-records num_records | time
rotation_time } | storage-limit storage_limit | trap-on-file-delete ]
default file [ delete-timeout | directory | field-separator | rotation |
 storage-limit | trap-on-file-delete ]
```

default

Configures this command with its default value for the specified parameters.

file delete-timeout *seconds*

Configures the time to delete the completed cell traffic trace files after specified number of seconds. *seconds* must be an integer from 3600 through 31536000.

file directory *directory_name*

Specifies a subdirectory to be generated in the default directory */records/celltrace* in which to store EDR files. *directory_name* must be an alphanumeric string of 1 through 191 characters.

file field-separator { hyphen | omit | underscore }

Specifies the field inclusion/exclusion type of separators between two fields of cell trace files.

- **hyphen**: Specifies to use "-" (hyphen) as the field separator between file format fields.
- **omit**: Excludes the field separator.
- **underscore**: Specifies to use "_" (underscore) as the field separator between file format fields.

file rotation { num-records *num_records* | time *rotation_time* }

Specifies the criteria to rotate the record file. CDRMOD will hold the cell trace records in buffer and write them to the XML file only when the criteria configured by this command are met.

num-records *num_records*: Completes the file when the specified number of records are added. When the number of records in the buffer reaches the specified value, records will be written to the XML file. *num_records* must be an integer from 100 to 2000. Default: 1000.

time *rotation_time*: Completes the file based on file duration, time after which records will be written to XML file. *num_records* must be an integer from 1 to 30. Default: 1 second.

file storage-limit *storage_limit*

Configures the total available storage space on RAMFS for cell trace files. *storage_limit* must be an integer from 10485760 to 134217728. When the storage space is full, the oldest files on RAMFS will be deleted first to create space for new files.

file trap-on-file-delete

Instructs the system to send an SNMP notification (starCDRFileRemoved) when a cell trace file is deleted due to lack of space.

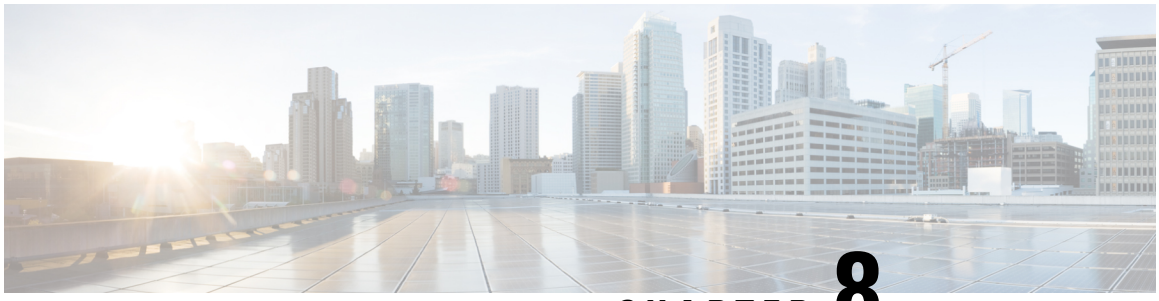
Usage Guidelines

Use this command to configure the file creation properties for cell trace records.

Example

The following command configures the time to delete the cell trace files after *4000* seconds:

```
file delete-timeout 4000
```



CHAPTER 8

Certificate Policy Configuration Mode Commands

Configure the context level name to be used for the IKEv2 Security Association Certificate Policy for the current context.

Command Modes

Exec > Global Configuration > Context Configuration > Certificate Policy Configuration

configure > context *context_name* **Certificate Policy Configuration** *service_name*

Entering the above command sequence results in the following prompt:

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


- do show, on page 269
- end, on page 270
- exit, on page 270
- id, on page 270

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.

id

Configures ID for cert-entry.

Product SecGW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context

configure > context *context_name***ikev2-ikesa** *ikev2_sec_para*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-cert-policy)#`

Syntax Description **epdg-s2b-gtpv2 send** *value* **match-criteria { common-name value***value* **| domain-name value** *value* **}**

id *value*

value: is an integer between 1 and 64.

match-criteria

Configures the match criteria to be configured and used for peer using cert as authorization for given Crypto Template.

common-name value*value*

Configures the entry with match criteria as common-name to be matched with CN in received Certificate.

value: is a string of size 1 through 64.

domain-name value*value*

Configure the entry with match criteria as domain name to be matched with domain in received Certificate.

value: is a string of size 1 through 64.

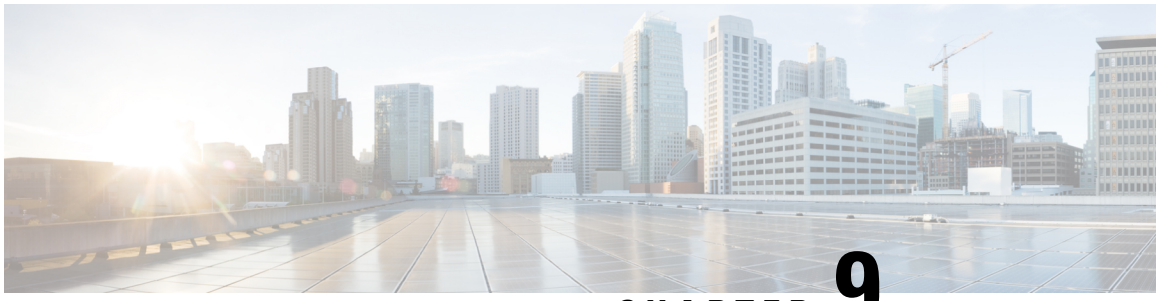
Usage Guidelines

Use this command to Enable/Disable the inclusion of the "UE Local IP Address" and "UE UDP Port" AVPs in the GTPv2 Create Session Request message from ePDG to PGW.

Example

Use the following command to configure ID for certificate entry as 4 with match criteria as domain name dom1.

```
id 4 match-criteria domain-name dom1
```



CHAPTER 9

CGW Service Configuration Mode Commands

Command Modes

Creates Convergence Gateway (CGW) service and enters CGW service configuration mode.

Exec > Global Configuration > Context Configuration > CGW Configuration

configure > **context** *context_name* > **cgw-service** *cgw_service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cgw-service)#
```

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

- associate, on page 273
- bind, on page 275
- enable-bra-failure-handling, on page 277
- end, on page 277
- exit, on page 277
- gre sequence-numbers, on page 278
- reg-lifetime, on page 278
- revocation, on page 279
- session-delete-delay, on page 280
- timestamp-option-validation, on page 281
- timestamp-replay-protection, on page 281

associate

This command associates another service to this CGW service.

Product SaMOG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > CGW Configuration

configure > **context** *context_name* > **cgw-service** *cgw_service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cgw-service)#
```

Syntax Description

associate { egress-egtp-service *egress_egtp_service* **[context** *context_name* **] | ggsn-service** *ggsn_service* **| mag-service** *mag_service* **[context** *context_name* **] | mrme-service** *mrme_service* **| pgw-service** *pgw_service* **| qci-qos-mapping** *qci_qos_mapping* **| sgtp-service** *sgtp_service* **[context** *context_name* **] | subscriber-map** *subscriber_map* **}**
no associate { egress-egtp-service | ggsn-service | pgw-service | ingress-lma-service | mag-service | qci-qos-mapping | sgtp-service | subscriber-map }

Note **associate mrme-service** is not supported in this release.

Note **no ingress-lma-service** is not supported in this release.

no

Disables association to CGW service.

egress-egtp-service *egress_egtp_service* [context *context_name*]

Configures the egtp-service which provides S2A functionality to the CGW service.

egress-egtp-service is a string and the value must be between *1* and *63*.

Use the **context** keyword to associate the egress egtp service from a different context in the CGW service.

context_name must be an alphanumeric string of 1 through 79 characters.

ggsn-service ggsn_service

Configures the association of a GGSN service for this CGW service.

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

mag-service mag_service [context *context_name*]

Configures the association of a MAG service for this CGW service.

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

Important This keyword is available only when the SaMOG General license (supporting both 3G and 4G) is configured. Contact your Cisco account representative for more information on license requirements.

context: Defines the context in which the MAG service was created. If no context is specified, the current context will be used.

context_name must be an alphanumeric string of 1 through 79 characters.

mrme-service *mrme_service*

Configures the association of egress MRME service for this CGW service.

mrme_service is a string and the value must be between *1* and *63*.

pgw-service *pgw_service*

Configures the association of a PGW service for this CGW service.

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

qci-qos-mapping *qci-qos-mapping*

Configuration related QCI to QoS mapping.

qci-qos-mapping is a string and the value must be between *1* and *63*.

sgtp-service *sgtp_service* [context *context_name*]

Specifies the SGTP service instance to associate with this CGW service.

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

context: Defines the context in which the SGTP service was created. If no context is specified, the current context will be used.

context_name must be an alphanumeric string of 1 through 79 characters.

subscriber-map *subscriber_map*

Configures subscriber map association.

subscriber_map is a string and the value must be between *1* and *64*.

ingress-lma-service

Configuration of the ingress LMA for this CGW service.

Usage Guidelines

Use this command to associate another service to this CGW service.

Example

The following command is used to associate the configuration of egress EGTP service *egts* for this CGW service:

```
associate egress-egtp-service egts
```

bind

This command allows you to bind an IPv4 and/or IPv6 address for the LMA driver.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CGW Configuration

configure > context *context_name* **> cgw-service** *cgw_service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cgw-service)#
```

Syntax Description

[no] bind { ipv4-address *ipv4_address* **[ipv6-address** *ipv6_address* **] | ipv6-address** *ipv6_address* **[ipv4-address** *ipv4_address* **] }**

no

Disables binding.

bind ipv6-address *ipv6_address*

Designates an IPv6 address. This must be followed by IPv6 address.

ipv6_address is IPv4 address, using dotted-decimal notation.

ipv4-address *ipv4_address* [ipv6-address *ipv6_address*] | ipv6-address *ipv6_address* [ipv4-address *ipv4_address*]

Important In this release, the configuration of the IPv6 bind address for PMIPv6 access type is supported as lab quality only.

Specifies the IPv4 or IPv6 address to be used as the connection point between the WLC and the SaMOG gateway. You can optionally bind a secondary IPv4 address (if the primary bind address is an IPv6 address) or IPv6 address (if the primary bind address is an IPv4 address) to the CGW service.

The second bind address can be bound in the same command or separate commands. When the second bind address is provided, the CGW service restarts and existing sessions are lost for the other bind address.

Important For PMIPv6 access type, you can either configure an IPv4 address or IPv6 address for binding. Configuring both IPv4 and IPv6 addresses will result in failure of the configuration, and an error message can be seen in the output of the **show config** command.

ipv4_address must be an IPv4 address expressed in dotted-decimal notation.

ipv6_address must be an IPv6 address expressed in colon (or double-colon) notation.

Usage Guidelines

Use this command to bind an IPv4 and/or IPv6 address for the LMA driver.

Example

The following command binds an IPv4 address for lma driver.

bind ipv4-address *192.51.100.1*

enable-bra-failure-handling

This command enables the HAMGR to select the first session incase the Binding Revocation Ack (BRA) does not have required parameters and the session lookup fails.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CGW Configuration

configure > context *context_name* **> cgw-service** *cgw_service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-cgw-service)#`

Syntax Description

`[ no ] enable-bra-failure-handling`

no

Disables Binding Revocation Ack failure handling.

Usage Guidelines

Use this command to enable Binding Revocation Ack failure handling.

Example

The following command enables Binding Revocation Ack failure handling.

`enable-bra-failure-handling`

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.

gre sequence-numbers

This command allows you to enable or disable the inclusion of sequence number bit and sequence number value in the GRE encapsulation header.

Product SaMOG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > CGW Configuration

configure > context *context_name* **> cgw-service** *cgw_service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-cgw-service)#`

Syntax Description **[no] gre sequence-numbers**

no

Disables the inclusion of sequence number bit and sequence number value in the GRE encapsulation header.

Default: Disabled

Usage Guidelines Use this command to enable or disable the inclusion of sequence number bit and sequence number value in the GRE encapsulation header for GRE tunneled packets.

reg-lifetime

Configures Mobile IPV6 session registration lifetime in seconds.

Product SaMOG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > CGW Configuration

configure > context *context_name* **> cgw-service** *cgw_service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-cgw-service)#`

Syntax Description **reg-lifetime** *seconds*
default reg-lifetime

default

Configures Mobile IPV6 session registration lifetime, in seconds to its default value, *600*.

reg-lifetime *seconds*

Configures Mobile IPV6 session registration lifetime.

seconds is the number of seconds, an integer value between *1* and *262140*.

Usage Guidelines

Use this command to configure Mobile IPV6 session registration lifetime, in seconds.

Example

The following command configures Mobile IPV6 session registration lifetime to 500 seconds.

```
reg-lifetime 500
```

revocation

Configures Binding Revocation support for specific CGW service.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CGW Configuration

configure > context *context_name* **> cgw-service** *cgw_service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cgw-service)#
```

Syntax Description

```
revocation { enable |  max-retransmission max_retransmission  |
retransmission-timeout  msecs  }
default revocation { enable |  max-retransmission | retransmission-timeout
 }
no revocation enable
```

default

Resets the revocation to its default value.

no

Disables revocation.

enable

Enables the Binding Revocation Support. Default is disabled.

max-retransmission *max_retransmission*

Configures the maximum number of retransmissions.

max_retransmission must be an integer between *0* and *10*.

retransmission-timeout *msecs*

Configures the retransmission timeout in milli seconds.

msecs must be an integer between *500* and *10000*.

Usage Guidelines Use this command to configure Binding Revocation support for specific CGW service.

Example

The following command configures the retransmission timeout to 1000 milli seconds.

```
revocation retransmission-timeout 1000
```

session-delete-delay

Configures CGW to retain the session on receiving a termination request till configured delay time for session continuity in case of break-before-make scenario.

Product SaMOG

Privilege Security Administrator, Administrator

Syntax Description

```
session-delete-delay timeout delay_msecs
{ default | no } session-delete-delay timeout
```

default

Configures session delate delay to its default value, disabled. Default timeout when enabled is 10000 msecs.

no

Enables / disables session delate delay to its default value.

session-delete-delay timeout *delay_msecs*

timeout : Configuration to retain session till configured time in msecs when enabled.

delay_msecs is the number of milli seconds, an integer value between *1000* and *60000*.

Usage Guidelines Use this command to configure CGW to retain the session on receiving a termination request till configured delay time for session continuity in case of break-before-make scenario.

Example

The following command configures CGW to retain the session timeout to 1500 milli seconds.

```
session-delete-delay timeout 1500
```

timestamp-option-validation

Configures validation of Timestamp Option in Binding Update messages. By default Timestamp option is mandatory.

Product

SaMOG

Privilege

Security Administrator, Administrator

Syntax Description

```
timestamp-option-validation
{ default | no } timestamp-option-validation
```

default

Confiugures validation of Timestamp Option in Binding Update messages to its default value.

no

Disables the Timestamp Option in Binding Update messages.

Usage Guidelines

Use this command to configure validation of Timestamp Option in Binding Update messages.

Example

The following command configures validation of Timestamp Option in Binding Update messages.

```
timestamp-option-validation
```

timestamp-replay-protection

This command designates timestamp replay protection scheme as per RFC 4285.

Product

SaMOG

Privilege

Security Administrator, Administrator

Syntax Description

```
timestamp-replay-protection tolerance seconds
default timestamp-replay-protection tolerance
no timestamp-replay-protection
```

default

Designates default value to timestamp replay protection scheme. The default value of the acceptable difference in timing (between timestamps) before rejecting packet is 7 seconds.

no

Disables the timestamp replay protection scheme.

timestamp-replay-protection tolerance *seconds*

tolerance : Defines the acceptable difference in timing (between timestamps) before rejecting packet, in seconds. *seconds* is the seconds, an integer between *0* and *65535*.

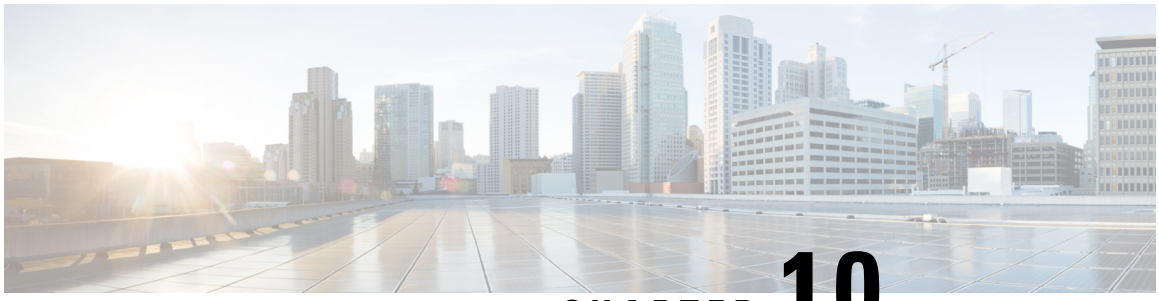
Usage Guidelines

Use this command to designate timestamp replay protection scheme as per RFC 4285.

Example

The following command designates timestamp replay protection for 500 seconds.

```
timestamp-replay-protection  tolerance 500
```



CHAPTER 10

Cipher Suite Configuration Mode Commands

Command Modes

The Cipher Suite Configuration Mode is used to configure the building blocks for SSL cipher suites, including the encryption algorithm, hash function, and key exchange.

Exec > Global Configuration > Context Configuration > Cipher Suite Configuration

configure > context *context_name* **> cipher-suite** *cipher_suite_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-cipher-suite)#
```

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

- encryption, on page 283
- end, on page 284
- exit, on page 284
- hmac, on page 285
- key-exchange, on page 285

encryption

Specifies the encryption algorithm for the SSL cipher suite.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Cipher Suite Configuration

configure > context *context_name* **> cipher-suite** *cipher_suite_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-cipher-suite)#
```

Syntax Description

```
encryption { 3des | aes-128 | null | rc4 }
default encryption
```

default

Sets the encryption option to its default value of RC4.

encryption 3des | aes-128 | null | rc4

Specifies the encryption algorithm.

3des: Encryption algorithm 3DES (Triple Encryption Algorithm). 3DES applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

aes-128: Encryption algorithm AES-128 (Advanced Encryption Standard-128). AES-128 is a symmetric-key encryption standard which has a 128-bit block size, with key size of 128.

null: Encryption algorithm Null.

rc4: Encryption algorithm RC4 (Rivest Cipher 4). RC4 is a stream cipher used with SSL protocol.

Usage Guidelines Use this command to specify encryption for the SSL cipher suite.

Example

The following command sets the encryption option to its default value, which is RC4:

```
encryption rc4
```

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.

hmac

Specifies the HMAC (keyed-Hash Message Authentication Code) for the SSL cipher suite.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Cipher Suite Configuration

configure > context *context_name* **> cipher-suite** *cipher_suite_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-cipher-suite)#
```

Syntax Description

```
hmac { sha1 }
default hmac
```

default

Sets the HMAC option to its default value of SHA-1.

hmac sha1

Specifies the SHA-1 (Secure Hash Algorithm-1) HMAC for the SSL cipher suite.SHA-1 uses a 160-bit secret key and produces a 160-bit digest.

Usage Guidelines

Use this command to specify the SHA-1 HMAC for the SSL cipher suite. The default and only currently available option is SHA-1.

A keyed-Hash Message Authentication Code, or HMAC, is a type of message authentication code (MAC) calculated using a cryptographic hash function in combination with a secret key to verify both data integrity and message authenticity.

Example

The following command sets the HMAC option to its default value, which is SHA-1:

```
hmac sha1
```

key-exchange

Specifies the key exchange algorithm for the SSL cipher suite.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Cipher Suite Configuration

configure > **context** *context_name* > **cipher-suite** *cipher_suite_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-cipher-suite)#
```

Syntax Description

```
key-exchange { rsa }
default key-exchange
```

default

Sets the key exchange option to its default value of RSA.

key-exchange rsa

Specifies the RSA (Rivest, Shamir, and Adleman) key exchange algorithm for the SSL cipher suite. With RSA, the secret key is encrypted with the receiver's public key, and a public-key certificate from the receiver's key must be made available.

Usage Guidelines

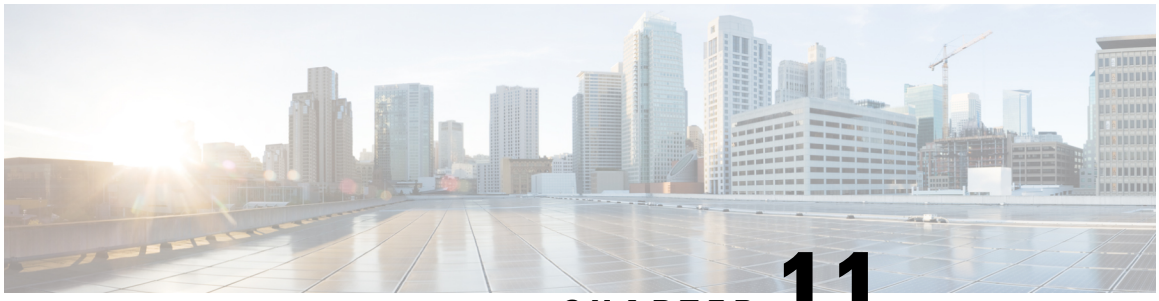
Use this command to specify the RSA key exchange for the SSL cipher suite. The default and only currently available option is RSA.

The key exchange algorithm provides the means by which the cryptographic keys for conventional encryption and MAC calculations are exchanged.

Example

The following command sets the key exchange option to its default value, which is RSA:

```
key-exchange rsa
```



CHAPTER 11

Class-Map Configuration Mode Commands

Class-Map is used to configure a packet classifier for the flow-based Traffic Policing feature within destination context. It filters egress and/or ingress packets of a subscriber session based on rules configured in a subscriber context.

Command Modes

Exec > Global Configuration > Context Configuration > Class-Map Configuration

configure > context *context_name* **> class-map** *class_map_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-class-map)#
```

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

- end, on page 287
- exit, on page 288
- match any, on page 288
- match dst-ip-address, on page 289
- match dst-port-range, on page 289
- match ip-tos, on page 290
- match ipsec-spi, on page 291
- match packet-size, on page 292
- match protocol, on page 293
- match src-ip-address, on page 294
- match src-port-range, on page 295

end

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

Product All

Privilege Security Administrator, Administrator

Syntax Description **`end`**

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

exit

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

Product All

Privilege Security Administrator, Administrator

Syntax Description **`exit`**

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

match any

Allows all traffic types in this class map.

Product PDSN
HA
ASN-GW
HSGW
P-GW
SAEGW
SCM

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Class-Map Configuration

configure > context *context_name* **> class-map** *class_map_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-class-map)#`

Syntax Description **match any**

Usage Guidelines Sets the match rule to allow all traffic flow for specific class map.

Example

The following command allows all packets going to a system with this class map.

`match any`

match dst-ip-address

Specifies a traffic classification rule based on the destination IP address of packets.

Product

PDSN

HA

ASN-GW

HSGW

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Class-Map Configuration

configure > context *context_name* **> class-map** *class_map_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-class-map)#`

Syntax Description

match dst-ip-address *dst_ip_address* **/***subnet_mask*

dst_ip_address/subnet_mask

Specifies the destination IP address of the packets.

dst_ip_address must be entered in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

subnet_mask is an option that is entered in CIDR notation.

Usage Guidelines

Sets the match rule based on the destination IP address of packets for specific Class Map.

Example

The following command specifies the rule for packets going to a system having an IP address *10.1.2.6*.

```
match dst-ip-address 10.1.2.6
```

match dst-port-range

Specifies a traffic classification rule based on the range of destination ports for L4 packets.

Product

PDSN

HA

ASN-GW

HSGW

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Class-Map Configuration

configure > **context** *context_name* > **class-map** *class_map_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-class-map)#
```

Syntax Description

match dst-port-range *initial_port_number* **[to** *last_port_number* **]**

initial_port_number **[to** ***last_port_number*** **]**

Specifies the destination port or range of ports of L4 packets.

initial_port_number is the starting port number and must be an integer 1 to 65535 but less than *last_port_number*, if specified.

last_port_number is the end port number and must be an integer from 1 to 65535 but more than *initial_port_number*.

Usage Guidelines

Sets the match rule based on the destination port number or range of ports of L4 packets for specific Class Map.

Example

The following command specifies the rule for packets having destination port number from *23* to *88*.

```
match dst-port-range 23 to 88
```

match ip-tos

Specifies a traffic classification rule based on the IP Type of Service value in ToS field of packet.

Product

PDSN

HA

ASN-GW

HSGW

P-GW

SAEGW

SCM

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Class-Map Configuration

configure > context *context_name* **> class-map** *class_map_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-class-map)#
```

Syntax Description

match ip-tos { *service_value* **[ip-tos-mask** *mask_value* **] | tos-range** *low_value* **to** *high_value* **}**

service_value

Specifies the IP Type-of-Service value to match inside the ToS field of packets as an integer from 0 to 255.

ip-tos-mask ***mask_value***

Specifies the IP Type-of-Service mask value to match inside the ToS field of packets as an integer from 1 to 255.

tos-range ***low_value*** **to** ***high_value***

Specifies a range that a ToS value in a received packet must fall within to be considered a match. *low_value* and *high_value* must be an integer from 0 to 255.

Usage Guidelines

Sets the match rule based on the IP ToS value in ToS field of packets for specific Class Map.

Example

The following commands specifies the IP ToS value of *3* is the value to match in a ToS field in received packets.

```
match ip-tos 3
```

match ipsec-spi

Specifies a traffic classification rule based on the IPSec Security Parameter Index (SPI) value in the SPI field of packet.

Product

PDSN

HA

ASN-GW

HSGW

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Class-Map Configuration

configure > context *context_name* **> class-map** *class_map_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-class-map)#`

Syntax Description

match ipsec-spi *index_value*

index_value

Specifies the IPSec SPI value to match inside the SPI field of packets as an integer from 1 to 65535.

Usage Guidelines

Sets the match rule based on the IPSec SPI value in SPI field of packets for specific Class Map.

Example

The following command specifies the IPSec SPI value as *1234* for the SPI field in packets.

```
match ipsec-spi 1234
```

match packet-size

Specifies a traffic classification rule based on the size of packet.

Product

PDSN

HA

ASN-GW

HSGW

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Class-Map Configuration

configure > context *context_name* **> class-map** *class_map_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-class-map)#`

Syntax Description

match packet-size [gt | lt] *size*

[gt | lt] ***size***

Specifies the packet length in bytes.

gt: indicates a packet size greater than the specified size.

lt: indicates a packet size less than the specified size.

size must be an integer from 1 to 65535.

Usage Guidelines Sets the match rule based on the size of packets for specific Class Map. This command is only applicable for static policies; it is not available for dynamic policies.

Example

The following command specifies the packet length to be *1024* bytes.

```
match packet-size 1024
```

match protocol

Specifies a traffic classification rule based on the protocol used for session flow.

Product

PDSN

HA

ASN-GW

HSGW

P-GW

SAEGW

SCM

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Class-Map Configuration

configure > context *context_name* **> class-map** *class_map_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-class-map)#
```

Syntax Description **match protocol { gre | ip-in-ip | number | rtp | sip | tcp | udp }**

gre

Sets the match rule for session flow using Generic Routing Encapsulation (GRE) Protocol. It matches the protocol field to GRE inside the packet.

ip-in-ip

Sets the match rule for session flow using IP-in-IP encapsulation protocol. It matches the protocol field to ip-in-ip inside the packet.

number

Sets the match rule for a session flow using Transmission Control Protocol (TCP). It matches the specified protocol field inside the packet.

rtp

Sets the match rule for a session flow using Real Time Protocol (RTP). It matches the specified protocol field inside the packet.

sip

Sets the match rule for a session flow using Session Initiation Protocol (SIP). It matches the specified protocol field inside the packet.

tcp

Sets the match rule for a session flow using Transmission Control Protocol (TCP). It matches the protocol field to TCP inside the packet.

udp

Sets the match rule for a session flow having User Datagram Protocol (UDP). It matches the protocol field to UDP inside the packet.

Usage Guidelines

Sets the match rule based on the protocol of packet flow for a specific Class Map.

Example

The following command specifies the rule for packet flow using IP-in-IP protocol.

```
match protocol ip-in-ip
```

match src-ip-address

Specifies a traffic classification rule based on the source IP address of packets.

Product

PDSN

HA

ASN-GW

HSGW

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Class-Map Configuration

configure > **context** *context_name* > **class-map** *class_map_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-class-map)#
```

Syntax Description

match src-ip-address *src_ip_address* **/***subnet_mask*

src_ip_address/subnet_mask

Specifies the destination IP address of the packets.

src_ip_address must be entered in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

subnet_mask is an option that is entered in CIDR notation.

Usage Guidelines

Sets the match rule based on the source IP address of packets for specific Class Map.

Example

The following command specifies the rule for packets coming from a system having an IP address *10.1.2.3*.

```
match src-ip-address 10.1.2.3
```

match src-port-range

Specifies a traffic classification rule based on the range of source ports of L4 packets.

Product

PDSN

HA

ASN-GW

HSGW

P-GW

SAEGW

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Class-Map Configuration

configure > **context** *context_name* > **class-map** *class_map_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-class-map)#
```

Syntax Description

match src-port-range *initial_port_number* **[to** *last_port_number* **]**

initial_port_number **[to** ***last_port_number*** **]**

Specifies the source port or range of ports of the L4 packets.

initial_port_number is the starting port number and must be an integer from 1 to 65535 but less than *last_port_number*, if specified.

last_port_number is the end port number and must be an integer from 1 to 65535 but more than *initial_port_number*.

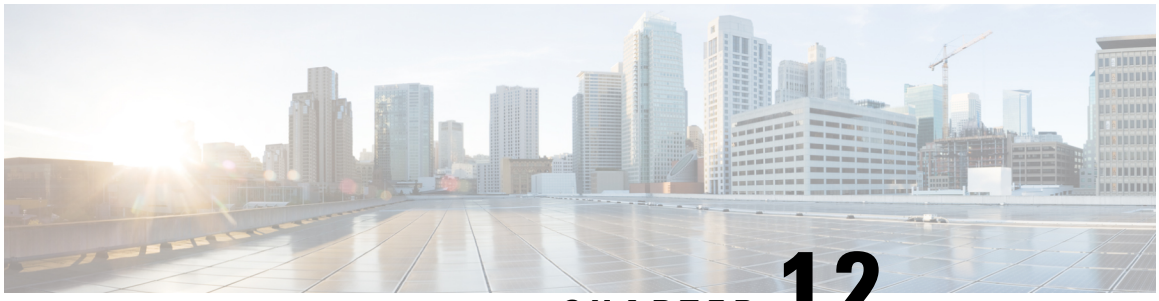
Usage Guidelines

Sets the match rule based on source port number or range of ports of L4 packets for specific Class Map.

Example

The following command specifies the rule for packets having source port number from *23* to *88*.

```
match src-port-range 23 to 88
```



CHAPTER 12

Congestion Action Profile Configuration Mode Commands

The Congestion Policy Configuration Mode is used to create and manage the action profiles to be associated with congestion control policies supporting MME or ePDG configurations on the system.

Command Modes

Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration

configure > lte-policy > congestion-action-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(congestion-action-profile)#
```

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

- ddn, on page 297
- drop, on page 298
- end, on page 300
- exclude-emergency-events, on page 301
- exclude-voice-events, on page 301
- exit, on page 302
- none, on page 302
- reject, on page 304
- report-overload, on page 306

ddn

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration

configure > lte-policy > congestion-action-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(congestion-action-profile)#
```

Syntax Description

ddn sgw-throttling throttle-factor *throttle_factor_value* **delay** *delay_time*
no ddn sgw-throttling

no

Removes the DDN Throttling configuration towards SGW.

ddn

The **ddn** keyword configures the action to be taken for all DDN requests. The operator can reject DDN requests based on ARP or LAPI values or both. Also, there is an option provided to reject all DDN requests without using ARP/LAPI values.

sgw-throttling

Enables DDN throttling towards SGW.

throttle-factor

Specifies the total number of DDN requests to be processed. The number of DDN requests is indicated as a percentage value from 1 to 100.

delay

Specifies the total time for throttling in seconds. The delay value ranges from 2 to 1116000 seconds.

Usage Guidelines

Configures DDN Throttling towards SGW based on the configured throttling factor and throttling delay.

Example

The following example shows DDN throttling with a throttling factor of 30 percent and a throtlling delay of 100 seconds.

```
ddn sgw-throttling throttle-factor 30 delay  100
```

drop

Specifies that incoming packets containing new session requests be dropped when a congestion control threshold has been reached.

Product

MME

ePDG

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration

configure > **lte-policy** > **congestion-action-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(congestion-action-profile)#
```

Syntax Description

drop { addn-brr-requests | addn-pdn-connects | brr-ctxt-mod-requests | combined-attaches | handovers | ps-attaches | s1-setups | service-request | tau-request } [lapi] [apn-based]

addn-brr-requests

Drops packets containing UE initiated bearer resource requests.

This keyword option will be available only if a valid license is installed.

addn-pdn-connects

Drops packets containing additional PDN context connections.

This keyword option will be available only if a valid license is installed.

brr-ctxt-mod-requests

Drops packets containing Bearer Context Modification requests.

This keyword option will be available only if a valid license is installed.

combined-attaches

Drops packets containing combined Attach requests.

handovers

Drops packets containing handover attempts.

ps-attaches

Drops packets containing packet switched Attach requests.

s1-setups

Drops packets containing S1 setup attempts.

This keyword option will be available only if a valid license is installed.

service-request

Drops packets containing all service requests.

This keyword option will be available only if a valid license is installed.

tau-request

Drops packets containing all Tracking Area Update requests.

[lapi] [apn-based]

These keyword options are available only if a valid license is installed.

When a congestion action profile is configured with the **drop <call-event> lapi** option, only requests with Low Access Priority Indication (LAPI) will be dropped for those call-events during congestion. However, if the call-event is configured without the **lapi** option, all LAPI and non-LAPI requests will be dropped.

If the congestion action profile is configured with the **drop <call-event> apn-based** option, only the requests for those APNs configured for congestion control in the Operator Policy will be dropped for those call-events during congestion. However, if the call-event is configured without the **apn-based** option, all requests will be dropped. Refer to the **apn network-identifier** command in the *Operator Policy Configuration Mode* chapter to enable congestion control for a specific APN.

If the congestion action profile is configured with both the **lapi** and **apn-based** options, the call-event will be dropped only if both conditions are matched.

Usage Guidelines

Creates a congestion action profile that drops packets containing a specified request when a threshold is reached.

Some keyword options are available only if a valid license is installed. For more information, contact your Cisco account representative.

Example

The following command drops packets containing Tracking Area Update (TAU) requests when a congestion threshold has been reached:

```
drop tau-request
```

The following command drops Additional PDN Context connetion requests when a congestion threshold has been reached. Only those APNs specified for APN-based congestion in the Operator Policy configuration mode will be dropped. Note that APN-based congestion control functionality supports APN remapping via the APN Remap Table Configuration Mode. The APN to which it is remapped will be checked for the congestion-control configuration.

```
drop addn-pdn-connects apn-based
```

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.

exclude-emergency-events

Excludes emergency events when a congestion control threshold is reached. Emergency events continue to be processed when the threshold has been exceeded.

Product

ePDG

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration

configure > lte-policy > congestion-action-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(congestion-action-profile)#
```

Syntax Description

`[no] exclude-emergency-events`

no

Removes the specified option from the system.

Usage Guidelines

Create a congestion action profile that allows emergency events to be processed when a congestion threshold has been reached.

When exclude-emergency is configured, congestion actions will not be applied for the following messages for emergency attached UEs:

- tau-request
- service-request
- handovers

When exclude-emergency is configured and addn-pdn-requests are configured for reject or drop actions, the reject or drop action on addn-pdn-requests for emergency PDN will not be applied.

Example

The following command allows emergency events to be processed:

`exclude-emergency-events`

exclude-voice-events

Excludes voice calls when a congestion control threshold is reached. Voice calls continue to be processed when the threshold has been exceeded.

Product

MME

ePDG

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration

configure > lte-policy > congestion-action-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(congestion-action-profile)#`

Syntax Description

[no] exclude-voice-events

no

Removes the specified option from the system.

Usage Guidelines

Create a congestion action profile that allows voice calls to be processed when a congestion threshold has been reached.

Example

The following command allows voice calls to be processed:

exclude-voice-events

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.

none

Specifies that no congestion control action be taken on an incoming request when a congestion control threshold has been reached.

Product

MME

ePDG

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration

configure > lte-policy > congestion-action-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(congestion-action-profile)#
```

Syntax Description

none { addn-brr-requests | addn-pdn-connects | combined-attaches | handovers | ps-attaches | s1-setups | service-request | tau-request }

addn-brr-requests

No congestion control action is taken for additional bearer requests when a congestion threshold is reached.

addn-pdn-connects

No congestion control action is taken for additional PDN context connections when a congestion threshold is reached.

brr-ctxt-mod-requests

No congestion control action is taken for Bearer Resource Context Modification Requests when a congestion threshold is reached.

combined-attaches

No congestion control action is taken for combined Attach requests when a congestion threshold is reached.

handovers

No congestion control action is taken for handover attempts when a congestion threshold is reached.

ps-attaches

No congestion control action is taken for packet switched Attach requests when a congestion threshold is reached.

s1-setups

No congestion control action is taken for S1 setup attempts when a congestion threshold is reached.

service-request

No congestion control action is taken for service requests when a congestion threshold is reached.

tau-request

No congestion control action is taken for Tracking Area Update requests when a congestion threshold is reached.

Usage Guidelines

Specifies that no congestion control action be taken for the specified request when a threshold is reached. For all of the above requests, 'none' is the default action; requests are processed normally even when a congestion threshold has been reached.

Example

The following command configures the congestion action profile to take no Congeston Control action for Tracking Area Update (TAU) requests when a congestion threshold is reached, so TAU procedure proceeds normally:

```
none tau-request
```

reject

Processes a specified request when a congestion control threshold has been reached and responds with a reject message.

Product

MME

ePDG

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration

configure > lte-policy > congestion-action-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(congestion-action-profile)#
```

Syntax Description

```
reject { addn-brr-requests | addn-pdn-connects |  brr-ctxt-mod-requests
| combined-attaches | ddn [ arp-watermark arpwatermark_value [ cause cause_value
 ] | cause cause_value | lapi [ cause cause_value ] ] | handovers | ps-attaches
 | s1-setups time-to-wait { 1 | 10 | 2 | 20 | 50 | 60 } | service-request
 | tau-request }[ lapi ] [ apn-based ]
none ddn [ lapi | arp-watermark ]
```

addn-brr-requests

Rejects UE initiated bearer resource requests.

This keyword option will be available only if a valid license is installed.

addn-pdn-connects

Rejects additional PDN context connections.

This keyword option will be available only if a valid license is installed.

brr-ctxt-mod-requests

Rejects packets containing Bearer Context Modification requests.

This keyword option will be available only if a valid license is installed.

combined-attaches

Rejects combined Attach requests.

ddn [arp-watermark | cause | lapi]

The **ddn** keyword configures the action to be taken for all DDN requests. The operator can reject DDN requests based on ARP or LAPI values or both. Also, there is an option provided to reject all DDN requests without using ARP/LAPI values.

The **arp-watermark** keyword specifies that DDN reject is applicable for ARP values greater than or equal to the ARP specified. The ARP value ranges from 1 through 15.

The **cause** keyword rejects DDN with the specified cause value. The valid cause value ranges from 1 through 255. The default value is 90 with the display message "Unable to page ue".

The **lapi** keyword for DDN specifies that DDN rejection is applicable for UEs with LAPI.

This keyword option will be available only if a valid license is installed.

none

Disables DDN configuration.

handovers

Rejects handover attempts.

ps-attaches

Rejects packet switched Attach requests.

s1-setups time-to-wait { 1 | 10 | 2 | 20 | 50 | 60 }

Rejects S1 setup attempts with an eNodeB after 1, 2, 10, 20, 50 or 60 seconds.

This keyword option will be available only if a valid license is installed.

service-request

Rejects all service requests.

This keyword option will be available only if a valid license is installed.

tau-request

Rejects all Tracking Area Update requests.

[lapi] [apn-based]

These keyword options are available only if a valid license is installed.

When a congestion action profile is configured with the **reject <call-event> lapi** option, only requests with Low Access Priority Indication (LAPI) will be rejected for those call-events during congestion. However, if the call-event is configured without the **lapi** option, all LAPI and non-LAPI requests will be rejected.

If the congestion action profile is configured with the **reject <call-event> apn-based** option, only the requests for those APNs configured for congestion control in the Operator Policy will be rejected for those call-events

during congestion. However, if the call-event is configured without the **apn-based** option, all requests will be rejected. Refer to the **apn network-identifier** command in the *Operator Policy Configuration Mode* chapter to enable congestion control for a specific APN.

If the congestion action profile is configured with both the **lapi** and **apn-based** options, the call-event will be rejected only if both conditions are matched.

Usage Guidelines

Creates a congestion action profile that rejects a specified request when a congestion threshold is reached.

Some keyword options are available only if a valid license is installed. For more information, contact your Cisco account representative.

Example

The following command rejects Tracking Area Update (TAU) requests when a congestion threshold has been reached:

```
reject tau-request
```

The following command rejects Additional PDN Context connetion requests when a congestion threshold has been reached. Only those APNs specified for APN-based congestion in the Operator Policy configuration mode will be rejected. Note that APN-based congestion control functionality supports APN remapping via the APN Remap Table Configuration Mode. The APN to which it is remapped will be checked for the congestion-control configuration.

```
reject addn-pdn-connects apn-based
```

report-overload

Enables the MME and ePDG to report overload conditions to eNodeBs to alleviate congestion scenarios.

Product

MME

ePDG

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration

configure > lte-policy > congestion-action-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(congestion-action-profile)#
```

Syntax Description

```
report-overload { permit-emergency-sessions-and-mobile-terminated-services
 | permit-high-priority-sessions-and-mobile-terminated-services |
reject-delay-tolerant-access | reject-new-sessions |
reject-non-emergency-sessions } enodeb-percentage percent
[no] report-overload
```

no

Removes the 'report-overload' action from this congestion action profile.

permit-emergency-sessions-and-mobile-terminated-services

Specifies in the overload message to the eNodeB that only emergency sessions are allowed to access the MME or ePDG during the overload period.

permit-high-priority-sessions-and-mobile-terminated-services

Specifies in the overload message to the eNodeB that only high-priority sessions and mobile-terminated services are allowed to access the MME during the overload period.

reject-delay-tolerant-access

Specifies in the overload message to the eNodeB that delay-tolerant access destined for the MME will be rejected during the overload period.

reject-new-sessions

Specifies in the overload message to the eNodeB that all new connection requests destined for the MME or ePDG will be rejected during the overload period.

reject-non-emergency-sessions

Specifies in the overload message to the eNodeB that all non-emergency sessions will be rejected during the overload period.

enobeb-percentage *percentage*

Configures the percentage of known eNodeBs that will receive the overload report.

percentage must be an integer from 1 through 100.

Usage Guidelines

Configures the MME or ePDG to invoke the S1 overload procedure (using the S1AP OVERLOAD START message) to report overload conditions to the specified proportion of eNodeBs to which this MME has an S1 interface connection. The MME or ePDG selects the eNodeBs at random, such that two overloaded MMEs or ePDGs in the same pool do not send overload messages to the same eNodeBs. When the MME or ePDG has recovered and can increase its load, the it sends an OVERLOAD STOP message to the eNodeBs.

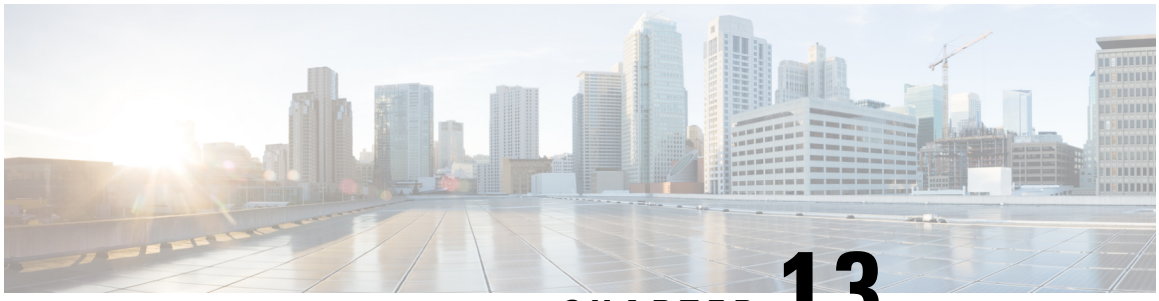


Important The 'report-overload' option must be configured before the threshold is exceeded in order for the action to take place.

Example

The following command configures the MME or ePDG to report an overload condition to 50% of all known eNodeBs and to request the eNodeBs to reject all non-emergency sessions to this MME or ePDG until the overload condition is cleared:

```
report-overload reject-non-emergency-sessions enodeb-percentage 50
```



CHAPTER 13

Connected Apps Configuration Mode Commands

The Connected Apps (CA) Configuration Mode is used to define CA client session parameters and High Availability (HA) settings for ASR 9000 VSMs supporting wsg-service virtual machines (VMs)

Important The StarOS commands described in this chapter are only supported for VPC running within a VM on the ASR 9000 VSM.

Command Modes Exec > Global Configuration > Connected Apps Configuration

`configure > connectedapps`

Entering the above command sequence results in the following prompt:

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

- activate, on page 309
- ca-certificate-name, on page 310
- end, on page 311
- exit, on page 311
- ha-chassis-mode, on page 311
- ha-network-mode, on page 312
- rri-mode, on page 313
- sess-ip-address, on page 314
- sess-name, on page 314
- sess-passwd, on page 315
- sess-userid, on page 316

activate

Initiates a ConnectedApps (CA) client session with the IOS-XR server on the ASR 9000.

Product SecGW (WSG)

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Connected Apps Configuration

configure > connectedapps

Entering the above command sequence results in the following prompt:

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

Syntax Description

activate
no activate

no

Disconnects an established CA session.

Usage Guidelines

Use this command to establish or disconnect a ConnectedApps (CA) client session with the IOS-XR server on the ASR 9000. CA client session parameters must have been previously entered for this command to work.

Example

The following command establishes a CA client session:

activate

ca-certificate-name

Configures a ConnectedApps (CA) client session with the IOS-XR server using TLS (Transport Layer Security) and CA (Certification Authority) certificate. This is an IOS-XR 5.2.0 requirement.

Product

SecGW (WSG)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Connected Apps Configuration

configure > connectedapps

Entering the above command sequence results in the following prompt:

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

Syntax Description

ca-certificate-name *cert_name*

cert_name

Specifies a CA certificate name as an alphanumeric string of 1 through 125 characters.

Usage Guidelines

Use this command to configure a ConnectedApps client session with the IOS-XR server using TLS (Transport Layer Security) and a specified CA certificate.

Example

The following command configures a ConnectedApps session using a CA certificate named *ux1345perm*:

ca-certificate-name ux1345perm

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.

ha-chassis-mode

Sets the High Availability (HA) mode for wsg-service virtual machines on VSMs in an ASR 9000.

Product SecGW (WSG)

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Connected Apps Configuration

configure > connectedapps

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(config-connectedapps)#

Syntax Description **ha-chassis-mode { inter | intra | standalone }**
no ha-chassis-mode

no

Disables the current HA chassis mode

{ inter | intra | standalone }

Specifies the type of chassis mode as:

- **inter** – HA is established between VSMs in two ASR 9000 chassis.
- **intra** – HA is established between VSMs in a single ASR 9000 chassis.
- **standalone** – This is a standalone card; HA cannot be enabled.

Usage Guidelines

Use this command to set or disable HA for VSMs within or across ASR 9000 chassis. To complete HA configuration you must also set its network mode.

Example

The following command sets HA mode between two ASR 9000 chassis:

```
ha-chassis-mode inter
```

ha-network-mode

Sets the network mode for High Availability (HA) network configuration between VSMs in ASR 9000 chassis.

Product

SecGW (WSG)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Connected Apps Configuration

```
configure > connectedapps
```

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
ha-network mode { L2 | L3 | NA }
no ha-network mode
```

no

Deletes the current setting for HA network mode.

{ L2 | L3 | NA }

Specifies the desired HA network mode as:

- **L2** – Layer 2
- **L3** – Layer 3
- **NA** – Not Applicable (standalone VSM)

Usage Guidelines

Use this command to set the network mode for the HA network configuration between VSMs in ASR 9000 chassis.

Example

The following command sets the HA network mode to Layer 2:

ha-network-mode L2

rri-mode

Configures Reverse Route Injection (RRI) mode. (VPC-VSM only)

Product

SecGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Connected Apps Configuration

configure > connectedapps

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(config-connectedapps)#

Syntax Description

rri-mode { both | none | ras | s2s }
no rri-mode

no

Disables the current RRI mode setting.

both

Support RAS and S2S modes.

none

Support neither RAS nor S2S mode.

ras

Support Remote Access Service mode only.

s2s

Support Site-to-Site mode only.

Usage Guidelines

Use this command to set the RRI mode.

Example

The following command sets the RRI mode to RAS.

rri-mode ras

sess-ip-address

Sets the IP address for a Connected Apps (CA) session.

Product

SecGW (WSG)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Connected Apps Configuration

configure > connectedapps

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(config-connectedapps)#

Syntax Description

sess-ip-address *ip_address*
no sess-ip-address

no

Deletes the current CA session IP address.

ip_address

Specifies the IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage Guidelines

Use this command to set the IP address for a Connected Apps (CA) session.

Example

The following command sets an IPv4 address for a CA session.

sess-ip-address 209.165.200.225

sess-name

Sets the name for a CA session.

Product

SecGW (WSG)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Connected Apps Configuration

configure > connectedapps

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(config-connectedapps)#

Syntax Description

sess-name *session_name*
no sess-name

no

Deletes the current CA session name.

session_name

Specifies the CA session name as an alphanumeric string of 1 through 125 characters.

Usage Guidelines

Use this command to set the name for a CA client session.

Example

The following command sets the CA session name to *vsm0-1*:

sess-name vsm0-1

sess-passwd

Sets a password for a CA session.

Product

SecGW (WSG)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Connected Apps Configuration

configure > connectedapps

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(config-connectedapps)#

Syntax Description

sesss-passwd { encrypted | password } *password*
no sess-passwd

no

Deletes the current CA session password.

encrypted

This keyword is only used by StarOS when you save the configuration file. StarOS displays the encrypted keyword in the configuration file as a flag indicating that the variable following the keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

password

Specifies that the password will appear in plain text in the configuration file.

password

Specifies the password as an alphanumeric string of 1 through 63 characters that is case sensitive.

Usage Guidelines

Use this password to set a password for a CA session.

Example

The following command sets a plain text password for a CA session:

```
sess-passwd password admin012
```

sess-userid

Defines a user identifier (username) for the CA session.

Product

SecGW (WSG)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Connected Apps Configuration

```
configure > connectedapps
```

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
sess-userid username
no sess-userid
```

no

Deletes the current user identifier for the CA session.

username

Specifies the user identifier for the CA session as an alphanumeric string of 1 through 64 characters.

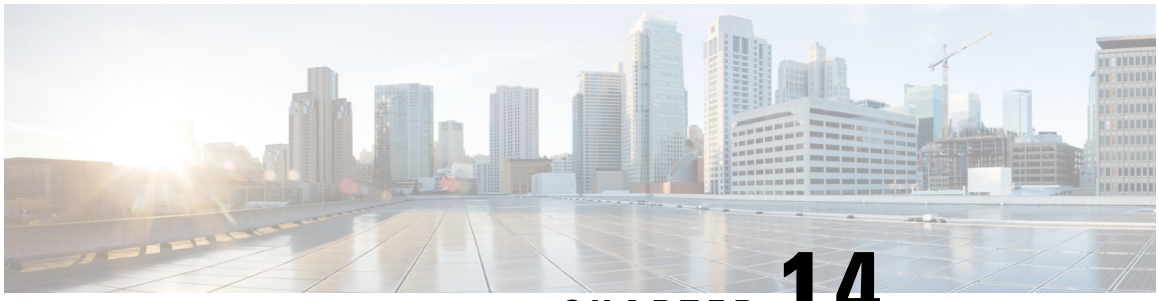
Usage Guidelines

Use this command to define a user identifier (username) for the CA session.

Example

The following command sets the user identifier to *vsm-admin02*:

```
sess-userid vsm-admin02
```



CHAPTER 14

Content Filtering Policy Configuration Mode Commands

The Content Filtering Policy Configuration Mode allows you to configure analysis and action when Content Filtering (CF) matches a Content Filtering Category Policy Identifier.

Command Modes

Exec > ACS Configuration > CFP Configuration

active-charging service *service_name* **> content-filtering category policy-id** *cf_policy_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-content-filtering-policy)#
```

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

- analyze, on page 317
- discarded-flow-content-id, on page 322
- end, on page 323
- exit, on page 323
- failure-action, on page 323
- timeout action, on page 325

analyze

Specifies the action to take for the indicated result after content filtering analysis.

Product

CF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > CFP Configuration

active-charging service *service_name* **> content-filtering category policy-id** *cf_policy_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-content-filtering-policy)#
```

Syntax Description

In 12.2 and later releases:

analyze priority *priority* **{ all | category** *category* **| x-category** *string* **}**
action { allow | content-insert *content_string* **| discard | redirect-url** *url*
| terminate-flow | www-reply-code-and-terminate-flow *reply_code* **} [**
reporting-edr *reporting_edr_format_name* **]**
no analyze priority *priority*

In 12.1 and earlier releases:

analyze priority *priority* **{ all | category** *category* **| x-category** *string* **}**
action { allow | content-insert *content_string* **| discard | redirect-url** *url*
| terminate-flow | www-reply-code-and-terminate-flow *reply_code* **} [edr**
edr_format_name **]**
no analyze priority *priority*

no

Removes the specified analyze priority configuration.

priority *priority*

Specifies the precedence of a category in the content filtering policy.

priority must be an integer from 1 to 65535 that is unique in the content filtering policy.

all

Specifies the default action to take if the category returned after rating is not configured in the subscriber's content filtering policy. This has the lowest priority.

category *category*

Specifies the category.

category must be one of the following.

- ABOR
- ADULT
- ADVERT
- ANON
- ART
- AUTO
- BACKUP
- BLACK
- BLOG
- BUSI

- CAR
- CDN
- CHAT
- CMC
- CRIME
- CULT
- DRUG
- DYNAM
- EDU
- ENERGY
- ENT
- FIN
- FORUM
- GAMB
- GAME
- GLAM
- GOVERN
- HACK
- HATE
- HEALTH
- HOBBY
- HOSTS
- KIDS
- LEGAL
- LIFES
- MAIL
- MIL
- NEWS
- OCCULT
- PEER
- PERS
- PHOTO

- PLAG
- POLTIC
- PORN
- PORTAL
- PROXY
- REF
- REL
- SCI
- SEARCH
- SHOP
- SPORT
- STREAM
- SUIC
- SXED
- TECH
- TRAV
- VIOL
- VOIP
- WEAP
- WHITE
- UNKNOW



Important Content can simultaneously match multiple categories, therefore specific **priority** must be used for required evaluation precedence.

x-category *string*

This keyword can be used to configure runtime categories not present in the CLI.

string specifies the unclassified category to be rated, and must be an alphanumeric string of 1 through 6 characters.

A maximum of 10 x-categories can be configured.

action { allow | content-insert *content_string* | discard | redirect-url *url* | terminate-flow | www-reply-code-and-terminate-flow *reply_code* }

Specifies the action to take for the indicated result of content filtering analysis.

allow: With static content filtering, this option allows the request for content. In dynamic content filtering it allows the content itself.

content-insert *content_string*: Specifies the content string to be inserted in place of the message returned from prohibited/restricted site or content server.

For static content filtering, *content_string* is used to create a response to the subscriber's attempt to get content. In dynamic content filtering, it is used to replace the content returned by a server.

content_string must be an alphanumeric string of 1 through 1023 characters.

discard: For static content filtering, this option discards the packet(s) that requested. In dynamic content filtering, it discards the packet(s) that contain(s) the content.

redirect-url *url*: Redirects the subscriber to the specified URL.

url must be an alphanumeric string of 1 through 1023 characters in the *http://search.com/subtarg=#HTTP.URL#* format.

terminate-flow: Terminates the TCP connection gracefully between the subscriber and server, and sends a TCP FIN to the subscriber and a TCP RST to the server.

www-reply-code-and-terminate-flow *reply_code*: Terminates the flow with the specified reply code. *reply_code* must be a reply code that is an integer from 100 through 599.



Important Static-and-Dynamic Content Filtering is only supported in 9.0 and later releases.

edr *edr_format_name*



Important This option is available only in 12.1 and earlier releases. In 12.2 and later releases, it is deprecated and replaced by the **reporting-edr** option.

Generates separate EDRs for content filtering based on action and content category using a specified EDR file format name.

edr_format_name is the name of a pre-defined EDR file format name in the EDR Format Configuration Mode, and must be an alphanumeric string of 1 through 63 characters.



Important EDRs generated through this keyword are different from charging EDRs generated for subscriber accounting and billing. For more information on generation of charging EDRs, refer to the *ACS Rulebase Configuration Mode Commands* chapter.

reporting-edr *reporting_edr_format_name*



Important This option is available only in 12.2 and later releases.

Generates separate reporting EDRs for Content Filtering based on the action and content category using the specified EDR file format name.

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

Usage Guidelines

Use this command to specify the action and priorities for the indicated result of content filtering analysis.

Up to 64 priorities and actions can be entered with this command.

Example

The following command sets priority *10* for category *ADULT* with action as **terminate-flow**:

```
analyze priority 10 category ADULT action terminate-flow
```

discarded-flow-content-id

Accounts for packets discarded as a result of content filtering action.

Product

CF

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > CFP Configuration

active-charging service *service_name* **> content-filtering category policy-id** *cf_policy_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-content-filtering-policy)#
```

Syntax Description

discarded-flow-content-id *content_id*
no discarded-flow-content-id

content_id

Specifies the content ID for discarded flows as an integer from 1 through 65535.

Usage Guidelines

Use this command in the configuration to account for packets discarded as a result of CF action.

A flow end-condition EDR would be generated as a charging EDR for content-filtered packets. No billing EDRs (even with flow-end) would be generated for a discarded packet as the flow will not end. Dual EDRs would exist for customers who want to use "flow end" to get EDRs for charging, plus CF-specific EDRs. The second EDR for charging comes from the **flow end-condition content-filtering** configuration in the Rulebase Configuration Mode.

The **discarded-flow-content-id** configuration can be used for accumulating statistics for UDR generation in case CF discards the packets. These statistics for UDR generation (based on the CF content ID) would also be accumulated in case of ACS error scenarios where the packets are discarded but the flow does not end.

If, in the Rulebase Configuration Mode, the **content-filtering flow-any-error** configuration is set to **deny**, then all the denied packets will be accounted for by the **discarded-flow-content-id** config. That is, the *content_id* will be used to generate UDRs for the denied packets in case of content filtering.

Example

Use the following command to set the accumulation of statistics for UDR generation based on the CF content ID *1003*:

```
discarded-flow-content-id 1003
```

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.

failure-action

Specifies the failure action when the content filtering analysis results are not available to analyze.

Product CF

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > CFP Configuration

active-charging service *service_name* **> content-filtering category policy-id** *cf_policy_id*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-content-filtering-policy)#
```

Syntax Description

failure-action { allow | content-insert *content_string* **| discard | redirect-url** *url* **| terminate-flow | www-reply-code-and-terminate-flow** *reply_code* **} [edr** *edr_format_name* **]**
default failure-action [edr *edr_format_name* **]**

default

Configures the default setting to terminate the flow.

allow

In static content filtering, this option allows the request for content. In dynamic content filtering it allows the content itself.

Important Static-and-Dynamic Content Filtering is only supported in 9.0 and later releases.

content-insertion *content_string*

Specifies the content string to be inserted in place of the message returned from the content server due to connection timeout or when no category policy ID is available for the content.

For content filtering, the *content_string* is used to create a response to the subscriber's attempt to get content. In dynamic content filtering it replaces the content returned by a server.

content_string is an alphanumeric string of 1 through 1023 characters.

Important Static-and-Dynamic Content Filtering is only supported in 9.0 and later releases.

discard

In static content filtering, specifies discarding the packet(s) that requested. In dynamic content filtering it discards the packet(s) that contain the content.

Important Static-and-Dynamic Content Filtering is only supported in 9.0 and later releases.

redirect-url *url*

Redirects the subscriber to the specified URL.

url must be an alphanumeric string of 1 through 1023 characters, in the following format: *http://search.com/subtarg=#HTTP.URL#*

terminate-flow

Terminates the TCP connection gracefully between the subscriber and external server and sends a TCP FIN to the subscriber and a TCP RST to the server. This is the default behavior.

www-reply-code-and-terminate-flow *reply_code*

Sets action as terminate-flow with a reply code that is a 3-digit integer from 100 through 599.

edr *edr_format_name*

Specifies the name of a pre-defined EDR format to be generated on the content filtering action as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to set the failure action to take when no content filtering analysis result is available to analyze for **analyze priority** *priority* **category** *category_string* command.

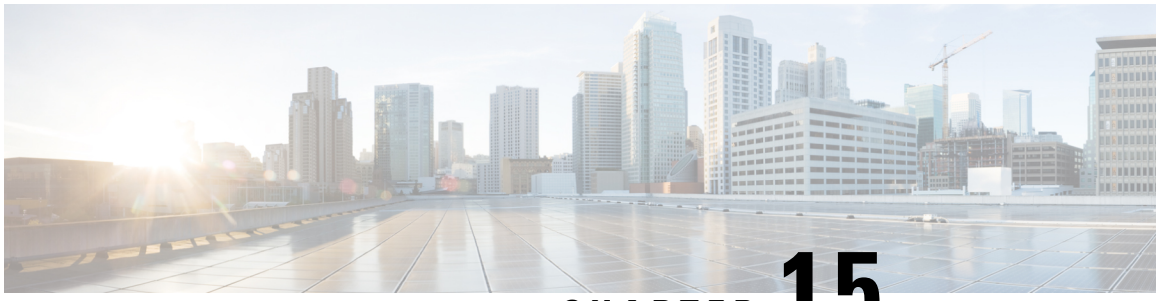
Example

The following command sets the failure action as **discard**:

```
failure-action discard
```

timeout action

This command has been deprecated, and is replaced by the command.



CHAPTER 15

Content Filtering Server Group Configuration Mode Commands

Content Filtering Server Group Configuration Mode sets the parameters for interoperating with a group of external servers. It is accessed by entering the **content-filtering server-group** command in the Context Configuration Mode.

Command Modes

Exec > Global Configuration > Context Configuration > CFSG Configuration

configure > context *context_name* **> content-filtering server-group** *server_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-content-filtering)#
```

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

- connection retry-timeout, on page 327
- deny-response code, on page 328
- dictionary, on page 329
- end, on page 331
- exit, on page 331
- failure-action, on page 331
- header extension options, on page 334
- icap server, on page 334
- origin address, on page 336
- response-timeout, on page 337
- timeout action, on page 338
- url-extraction, on page 338

connection retry-timeout

Configures the TCP connection retry timer for Internet Content Adaptation Protocol (ICAP) server and client.

Product CF

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > CFSG Configuration

configure > context *context_name* **> content-filtering server-group** *server_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-content-filtering)#`

Syntax Description

connection retry-timeout *duration*
{ default | no } connection retry-timeout

default

Configures the default setting of 30 seconds.

no

Removes the connection retry timeout configuration.

duration

Specifies the duration (in seconds) as an integer from 1 to 3600. Default: 30

Usage Guidelines Use this command to configure the connection retry timer between ICAP server and client TCP connection, i.e. how long to wait before re-attempting to establish a TCP connection.

Example

The following command sets the ICAP client and server connection retry timer to 120 seconds:

connection retry-timeout 120

deny-response code

Configures the deny response message that is to be sent from the ICAP server to the subscribers.

Product ICAP

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > CFSG Configuration

configure > context *context_name* **> content-filtering server-group** *server_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-content-filtering)#`

Syntax Description

deny-response code { 200 message *string* **| 403 }**
{ default | no } deny-response code

default

Configures the default setting of **deny-response code 200**.

no

Removes previously configured deny response message setting.

deny-response code 200 message *string*

Specifies a text message that is to be returned to the subscriber in a code 200 deny response. as an alphanumeric string of 1 through 511 characters.

If **deny-response code 200** is configured, the response sent to the subscriber will be of the form 200 OK with deny messages denied. If a message is configured for response code 200, that message will be used instead of "Access denied".

deny-response code 403

This keyword is used to set response code 403 for the deny response message.

When this keyword is configured, the deny response from the ICAP server will be sent "as is" to the subscriber.

Usage Guidelines

Use this command to define a text message that is returned to the subscriber in a deny response.

Example

The following command sets the text message to *Not allowed* in a deny response message:

```
deny-response code 200 message Not allowed
```

dictionary

Specifies the dictionary to use for requests to the server(s) in this Content Filtering Server Group (CFSG).

Product

CF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CFSG Configuration

configure > context *context_name* **> content-filtering server-group** *server_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-content-filtering)#
```

Syntax Description

```
dictionary { custom1 | custom10 |custom2 | custom3 | custom4 | | custom5
 | custom6 | custom7 | custom8 | custom9 | standard }
{ default | no } dictionary
```

default

Sets the default dictionary.

Default: **default**

no

Removes the previously configured dictionary setting.

custom1

Specifies a custom-defined dictionary that conforms to TS 32.015 v 3.6.0 for R99. It provides proprietary header fields for MSISDN and APN/subscriber. Please contact your local Cisco representative for more information.

custom2

Custom-defined dictionary. Please contact your local Cisco representative for additional information.

custom3

Custom-defined dictionary. Please contact your local Cisco representative for additional information.

Specifies a custom-defined dictionary that conforms to TS 32.015 v 3.6.0 for R99 except that it supports the encoding of IP addresses in binary format for G-CDRs.

custom4

Specifies a custom-defined dictionary that conforms to RFC 3507. Please contact your local Cisco representative for additional information.

custom4

Specifies a custom-defined dictionary that conforms to TS 32.015 v 3.6.0 for R99 except that:

- IP addresses are encoded in binary format.
- The Data Record Format Version information element contains 0x1307 instead of 0x1308.
- QoSRequested is not present in the LoTV containers.
- QoSnegotiated is added only for the first container and the container after a QoS change.

custom5 ... custom10

Specifies custom-defined dictionaries conforming to TS 32.215 v 4.6.0 for R4 (and also R5 - extended QoS format).

standard

Default: Enabled

This dictionary uses an HTTP Get Request to specify the URL. It conforms to TS 32.215 v 4.6.0 for R4 (and also R5 - extended QoS format).

Usage Guidelines

Use this command to specify the standard and customized encoding mechanism used for elements included messages.

Example

The following command configures the system to use standard dictionary to encode messages:

default dictionary

end

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.

failure-action

Specifies the actions to be taken when communication between ICAP endpoints within this Content Filtering Server Group (CFSG) fail.

Product CF

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > CFSG Configuration

configure > context *context_name* **> content-filtering server-group** *server_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-content-filtering)#`

Syntax Description

failure-action { allow | content-insertion *content_string* **| discard | redirect-url** *url* **| terminate-flow }**
{ default | no } failure-action

default

Configures the default setting of **terminate-flow**.

no

Removes previously configured failure action.

allow

For static content filtering, this option allows the request for content. In dynamic content filtering, it allows the content itself.

content-insertion *content_string*

Specifies the content string to be used for failure action.

For static content filtering, the specified text is used to create a response to the subscriber's attempt to get content. In dynamic content filtering, the specified text replaces the content returned by a server.

content_string must be an alphanumeric string of 1 through 128 characters.

discard

For static content filtering, this option discards the packet(s) requested. In dynamic content filtering, it discards the packet(s) that contain(s) the content.

redirect-url *url*

Redirects the subscriber to the specified URL.

url must be an alphanumeric string of 1 through 128 characters in the following format: *http://search.com/subtarg=#HTTP.URL#*

terminate-flow

For TCP, gracefully terminates the connection between the subscriber and external server, and sends a TCP FIN to the subscriber and a TCP RST to the server.

For WAP-Connection Oriented, the WSP session is gracefully terminated by sending WTP Aborts for each of the outstanding requests, and WSP Disconnect to the client and the server. For WSP-Connectionless, only the current WSP request is rejected.

Usage Guidelines

Use this command to set the actions on failure for server connection.

ICAP rating is enabled for retransmitted packets when the default ICAP failure action was taken on an ICAP request for that flow. ICAP default failure action is taken on the pending ICAP request for a connection when the connection needs to be reset and there is no other redundant connection available. For example, in the ICAP request timeout and ICAP connection timeout scenarios, the retransmitted packet in the uplink direction is sent for ICAP rating again.

For WAP CO, uplink retransmitted packets for the WAP transactions for which ICAP failure action was taken will be sent for ICAP rating. The WSP header of the retransmitted packet is not parsed by the WSP analyzer. The URL received in the previous packet for that transaction is used for ICAP rating. If failure action was taken on multiple WTP transactions for the same flow (case: WTP concatenated GET request), the uplink retransmitted packet for each of the transactions is sent for rating again.

For HTTP, uplink retransmitted packets for the HTTP flow on which ICAP failure action is taken are sent for ICAP rating. The URL present in the current secondary session (last uplink request) is used for ICAP rating. However, if there were multiple outstanding ICAP requests for the same flow (pipelined request), the retransmitted packet for the URL sent for rating will be that of the last GET request.

Retransmission in various cases of failure-action taken on retransmitted packets when the ICAP response is not received for the original request and the retransmitted request comes in:

- WSP CO:
  - Permit: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed/blocked. It is possible that the WAP gateway sends the response for the permitted GET request. Hence, there is a race condition and the subscriber may be able to view the web page even thought the rating was redirect or content insert.
  - Content Insert: The retransmitted packet is not sent for ICAP rating.
  - Redirect: The retransmitted packet is not sent for ICAP rating.
  - Discard: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed/blocked.
  - Terminate flow: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed or blocked. The WAP gateway may send an Abort transaction for this GET request if the WSP disconnect packet sent while terminating the flow is received by the WAP gateway.
- HTTP:
  - Permit: The uplink packet is sent for ICAP rating and depending on the ICAP response the last HTTP GET request. It is possible that the HTTP server sends the response for the permitted GET request. Hence there is a race condition and the subscriber may be able to view the web page even thought the rating was redirect or content insert.
  - Content Insert: Retransmitted packets are dropped and not charged.
  - Redirect: Retransmitted packets are dropped and not charged.
  - Discard: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction allowed/blocked.
  - Terminate flow: Retransmitted packets will be dropped and not charged.

Example

The following command sets the failure action to terminate:

```
failure-action terminate-flow
```

header extension options

Configures the extension options for the ICAP header in the ICAP request message.

Product

CF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CFSG Configuration

configure > context *context_name* **> content-filtering server-group** *server_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-content-filtering)#
```

Syntax Description

header extension options { cipa-category *cipa_category_name* **| subscriber-number** *subscriber_num_string* **}**
no header extension options

no

When configured, CIPA category and subscriber number will not be inserted in the ICAP request message to ICAP server. The values are string names present in the ICAP request message.

cipa-category ***cipa_category_name***

Specifies the CIPA category in the ICAP Request message.

cipa_category_name must be an alphanumeric string of 1 through 31 characters.

subscriber-number ***subscriber_num_string***

Specifies the subscriber number in the ICAP Request message.

subscriber_num_string must be an alphanumeric string of 1 through 31 characters.

Usage Guidelines

Use this command to configure header extension options in the ICAP request header - CIPA category and Subscriber number.

Example

The following command configures the ICAP header with CIPA category **x-icap-cipa-category**:

header extension options cipa-category x-icap-cipa-category

icap server

Adds an Internet Content Adaptation Protocol (ICAP) server configuration to the current Content Filtering Server Group (CFSG).



Important A maximum of five ICAP servers and only one ICAP Server can be configured per Content Filtering Server Group.

Product

CF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CFSG Configuration

configure > context *context_name* **> content-filtering server-group** *server_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-content-filtering)#
```

Syntax Description

```
icap server ip_address [ port port_number ] [ max messages ] [ priority priority ] [ standby ]
no icap server ip_address [ port port_number ] [ priority priority ] [ standby ]
```

no

Removes the specified ICAP server configuration from the current Content Filtering Server Group.

ip_address

Specifies the ICAP server's IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

port *port_number*

Specifies the ICAP server's port number to use for communications as an integer from 1 to 65535. Default: 1344

max *messages*

Specifies the maximum number of unanswered outstanding messages that may be allowed to the ICAP server as an integer from 1 to 4096. Default: 256



Important The maximum outstanding requests per ICAP connection is limited to one. Therefore the value configured using the **max** keyword will be ignored.

priority *priority*

Specifies priority of the ICAP server in the current Content Filtering Server Group. The priority is used in server selection to determine which standby server becomes active. *priority* must be an integer from 1 (highest priority) to 65535 (lowest priority). Default: 1



Important The **priority** keyword is only available in 8.1 and later releases.

standby

Configures the ICAP server as standby. A maximum of ten active and standby servers per group can be configured.

Usage Guidelines

This command is used to add an ICAP server configuration to a Content Filtering Server Group with which the system is to communicate for content filtering communication.

The ICAP solution supports only one connection between ACS Manager and ICAP server.

Multiple ICAP server connections are supported per manager. At any time only one connection is active with the other connections acting as standby. In case of a connection failure, based on its priority, a standby connection becomes active. Any pending ICAP requests are moved to the new active connection. If a standby connection is unavailable, failure action is taken on all pending ICAP requests. See the command.

A maximum of five ICAP servers can be configured per Content Filtering Server Group with a priority associated with each server. Once configured, an ICAP server's priority cannot be changed. To change a server's priority, the server configuration must be removed, and added with the new priority.

A maximum of ten active and standby servers per group can be configured.

Example

The following command sets the ICAP server IP address to *209.165.200.225* and port to *1024*:

```
icap server 209.165.200.225 port 1024
```

The following command specifies an ICAP server with IP address *209.165.200.226*, port number *1024*, and priority *3*:

```
icap server 209.165.200.226 port 1024 priority 3
```

origin address

Specifies a bind address for the Content Filtering Server Group (CFSG) endpoint.

Product

CF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CFSG Configuration

configure > context *context_name* **> content-filtering server-group** *server_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-content-filtering)#
```

Syntax Description

```
origin address ip_address
no origin address
```

no

Disables/releases the binding address for the CFSG endpoint.

ip_address

Specifies the IP address to bind the CFSG endpoint in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage Guidelines Use this command to set the bind address for the CFSG endpoint.

Example

The following command sets the origin address of *209.165.200.225*:

```
origin address 209.165.200.225
```

response-timeout

Sets the response timeout for the ICAP connection between the ICAP server and client.

Product CF

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > CFSG Configuration

configure > context *context_name* **> content-filtering server-group** *server_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-content-filtering)#
```

Syntax Description

```
response-timeout duration
{ default | no } response-timeout
```

default

Configures the default setting of 30 seconds.

no

Removes the response timeout configuration.

duration

Specifies the timeout duration (in seconds) as an integer from 1 to 300. Default: 30

Usage Guidelines Use this command to set the ICAP connection response timeout, after which connection will be marked as unsuccessful between ICAP endpoint.

Example

The following command sets the ICAP connection response timeout to *100* seconds:

```
response-timeout 100
```

timeout action

This command has been deprecated, and is replaced by the failure-action, on page 331 command.

url-extraction

Enables configuration of ICAP URL extraction behavior.

Product

CF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CFSG Configuration

configure > context *context_name* **> content-filtering server-group** *server_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-content-filtering)#
```

Syntax Description

```
url-extraction { after-parsing | raw }
default url-extraction
```

default

Configures the default setting of **after-parsing**.

after-parsing

Specifies sending the parsed URI and host name. Percent-encoded hex characters in URLs sent from the ACF client to the ICAP server will be converted to corresponding ASCII characters before being sent.

For example, the URL: *http://www.google.co.uk/?this%20is%20a%20test* will be sent to the ICAP server as:

http://www.google.co.uk/?this is a test

raw

Specifies sending raw URI and host name. The URLs will contain percent-encoded hex characters "as is".

For example, the URL *http://www.google.co.uk/?this%20is%20a%20test* will be sent to the ICAP server as:

http://www.google.co.uk/?this%20is%20a%20test

Important The raw URL configuration asserts that there are no changes in the URL before sending the request to ICAP. However, if there are spaces in the original URI then the same is forwarded to ICAP.

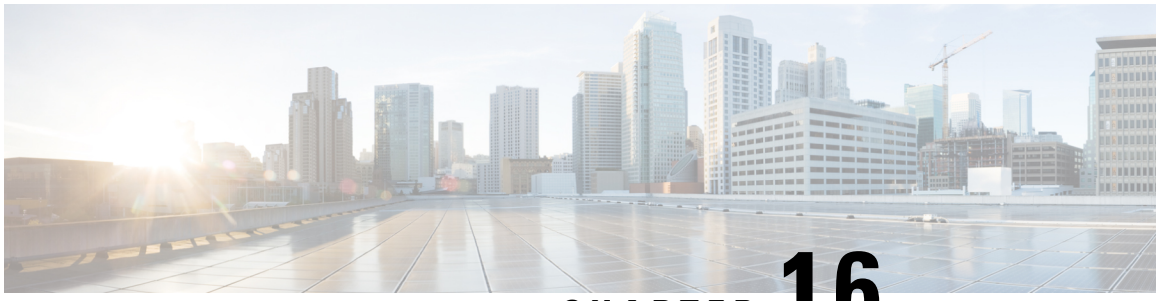
Usage Guidelines

Use this command to configure the ICAP URL extraction behavior. Percent-encoded hex characters—for example, space (%20) and the percent character (%25)—in URLs sent from the ACF client to the ICAP server can be sent either as percent-encoded hex characters or as their corresponding ASCII characters.

Example

The following command configures URLs sent from the ACF client to the ICAP server to contain the escape encoding as is:

```
url-extraction raw
```



CHAPTER 16

Context Configuration Mode Commands A-D

Command Modes

This section includes the commands **aaa accounting** through **domain** service.

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

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

- aaa accounting, on page 342
- aaa authentication, on page 344
- aaa constructed-nai, on page 345
- aaa filter-id rulebase mapping, on page 347
- aaa group, on page 348
- aaa nai-policy, on page 349
- aaa tacacs+, on page 350
- access-list undefined, on page 351
- administrator, on page 351
- apgroupname-list, on page 355
- apn, on page 356
- asn-qos-descriptor, on page 357
- asn-service-profile, on page 359
- asngw-service, on page 360
- asnpc-service, on page 361
- associate, on page 362
- bfd-protocol, on page 363
- bgp extended-asn-cap, on page 364
- bmsc-profile, on page 364
- busyout ip, on page 365
- busyout ipv6, on page 367
- cae-group, on page 370

- camel-service, on page 371
- cbs-service, on page 372
- cipher-suite, on page 373
- class-map, on page 374
- closedrp-rp handoff, on page 375
- config-administrator, on page 376
- content-filtering, on page 379
- credit-control-service, on page 380
- crypto dns-nameresolver, on page 381
- crypto group, on page 382
- crypto ipsec transform-set, on page 383
- crypto map, on page 385
- crypto template, on page 386
- crypto vendor-policy, on page 388
- css server, on page 389
- cups chunk-threshold-timer, on page 389
- cups enabled, on page 389
- cups max-user-planes, on page 390
- cups min-chunks-threshold-per-pool, on page 390
- cups-redundancy-protocol, on page 391
- description, on page 392
- dhcp-client-profile, on page 392
- dhcp-server-profile, on page 393
- dhcp-service, on page 394
- dhcpv6-service, on page 396
- diameter accounting, on page 397
- diameter authentication, on page 400
- diameter authentication failure-handling, on page 402
- diameter dictionary, on page 404
- diameter endpoint, on page 404
- diameter-hdd-module , on page 406
- diameter sctp, on page 407
- diameter origin, on page 408
- dns-client, on page 408
- domain, on page 409

aaa accounting

This command enables/disables accounting for subscribers and context-level administrative users for the current context.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
aaa accounting { administrator radius-diameter | subscriber [
radius-diameter ] }
default aaa accounting { administrator | subscriber }
no aaa accounting { administrator | subscriber } [ radius-diameter ]
```

default

Configures the default setting.

Default: RADIUS

no

Disables AAA accounting per the options specified.

radius-diameter

Enables AAA accounting for context-level administrative users.

subscriber

Enables AAA accounting for subscribers.

radius-diameter

Enables RADIUS or Diameter accounting for subscribers.

Usage Guidelines

Use this command to enable/disable accounting for subscribers and context-level administrative users for the current context.

To enable or disable accounting for individual local subscriber configurations refer to the **accounting-mode** command in the *Subscriber Configuration Mode Commands* chapter.



Important The accounting parameters in the APN Configuration Mode take precedence over this command for subscriber sessions. Therefore, if accounting is disabled using this command but enabled within the APN configuration, accounting is performed for subscriber sessions.

Example

The following command disables AAA accounting for context-level administrative users:

```
no aaa accounting administrator
```

The following command enables AAA accounting for context-level administrative users:

```
aaa accounting administrator radius-diameter
```

aaa authentication

This command enables/disables authentication for subscribers and context-level administrative users for the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] aaa authentication { administrator | subscriber } { local | none
| radius-diameter }
default aaa authentication { administrator | subscriber }
```

default

Configures the default setting for the specified parameter.

- **administrator**: local+RADIUS
- **subscriber**: RADIUS

no

Disables AAA authentication for administrator(s)/subscribers as specified.

- **local**: Disables local authentication for current context.
- **none**: Disables NULL authentication for current context, which enables both local and RADIUS-based authentication.
- **radius-diameter**: Disables RADIUS or Diameter-based authentication.

administrator | subscriber

- **administrator**: Enables authentication for administrative users.
- **subscriber**: Enables authentication for subscribers.

local | none | radius-diameter

Enables AAA authentication for administrator(s)/subscribers as specified.

- **local**: Enables local authentication for the current context.
- **none**: Disables authentication for the current context.
- **radius-diameter**: Enables RADIUS or Diameter-based authentication.

Usage Guidelines Use this command to enable/disable AAA authentication during specific maintenance activities or during test periods. The authentication can then be enabled again for the entire context as needed.

Example

The following command disables RADIUS or Diameter-based authentication for subscribers for the current context:

```
no aaa authentication subscriber radius-diameter
```

The following command enables RADIUS or Diameter-based authentication for subscribers for the current context:

```
aaa authentication subscriber radius-diameter
```

aaa constructed-nai

This command configures the password used during authentication for sessions using a Constructed Network Access Identifier (NAI) or an APN-specified user name.

Product PDSN

GGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
aaa constructed-nai authentication [ [ encrypted ] password user_password |
 use-shared-secret-password ]
no aaa constructed-nai authentication
```

no

Disables authentication based upon the constructed NAI.

[encrypted] password *user_password*

encrypted: Specifies that the user password should be encrypted.

password *user_password*: Specifies an authentication password for the NAI-constructed user.

In 12.1 and earlier releases, the *user_password* must be an alphanumeric string of 0 through 63 characters with or without encryption.

In 12.2 and later releases, the *user_password* must be an alphanumeric string of 0 through 63 characters without encryption, or 1 through 132 characters with encryption.

use-shared-secret-password

Specifies using RADIUS shared secret as the password. Default: No password

Usage Guidelines

This command configures passwords for user sessions that utilize a constructed NAI assigned via a PDSN service or a user name assigned via the APN configuration.

For simple IP sessions facilitated by PDSN services in which the **authentication allow-noauth** and **aaa constructed-nai** commands are configured, this command provides a password used for the duration of the session.

For PDP contexts using an APN in which the outbound user name is configured with no password, this command is used to provide the password.Additionally, this command is also used to provide a password for situations in which an outbound username and password are configured and the **authentication imsi-auth** command has been specified.

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

If a password is configured with this keyword, then the specified password is used. Otherwise, an empty user-password attribute is sent.

Note that this configuration works in a different way for GGSN services. If a password is configured with this keyword for GGSN service, the specified password is used.Otherwise, if an outbound password is configured, that password is used. If no outbound password is configured, the RADIUS server secret is used as the user-password string to compute the user-password RADIUS attribute.

The NAI-construction consists of the subscriber's MSID, a separator character, and a domain. The domain that is used is either the domain name supplied as part of the subscriber's user name or a domain alias.



Important The domain alias can be set with the **nai-construction domain** command in the PDSN Service Configuration mode, or the **aaa default-domain subscriber** command in the Global Configuration mode for other core network services.

The domain alias is determined according to the following rules:

- If the domain alias is set by **nai-construction domain**, that value is always used and the **aaa default-domain subscriber** value is disregarded, if set. The NAI is of the form **<msid><symbol><nai-construction domain>**.
- If the domain alias is not set by **nai-construction domain**, and the domain alias is set by **aaa default-domain subscriber**, the **aaa default-domain subscriber** value is used. The NAI is of the form **<msid><symbol><aaa default-domain subscriber>**.
- If the domain alias is not set by **nai-construction domain** or **aaa default-domain subscriber**, the domain name alias is the name of the source context for the PDSN service. The NAI is of the form **<msid><symbol><source context of PDSN Service>**.

The special separator character can be one of the following six: @, -, %, \,-, /

The subscriber's MSID is constructed in one of the formats displayed in the following figure.

Example

The following command configures the authentication password for the NAI-constructed user.

aaa constructed-nai authentication

aaa filter-id rulebase mapping

This command configures the system to use the value of the Filter-Id AVP as the ACS rulebase name.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no | default] aaa filter-id rulebase mapping

no

Disables the mapping of Filter-Id AVP and ACS rulebase name.

default

Configures the default setting. Default: Disabled

Usage Guidelines

Use this command to enable the mapping of Filter-Id attribute's value returned during RADIUS authentication as the ACS rulebase name.

This feature provides the flexibility for operator to transact between multi-charging-service support for postpaid and prepaid subscribers through Access Control Lists (ACLs) entered in AAA profiles in RADIUS server to single-charging-service system based on rulebase configuration for postpaid and prepaid subscribers.

This feature internally maps the received ACL in to rulebase name and configures subscriber for postpaid or prepaid services accordingly.

When this feature is enabled and ACS rulebase attribute is not received from RADIUS or not configured in local default subscriber template system copies the filter-id attribute value to ACS rulebase attribute.

This copying happens only if the filter-id is configured and received from RADIUS server and ACS rulebase is not configured in ACS or not received from RADIUS.

Example

The following command enables the mapping value of the Filter-Id attribute to ACS rulebase name:

aaa filter-id rulebase mapping

aaa group

This command enables/disables the creation, configuration or deletion of AAA server groups in the context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

aaa group *group_name* **[-noconfirm]**
no aaa group *group_name*

no

Deletes the specified AAA group.

group_name

Specifies name of the AAA group.

If the specified AAA group does not exist, it is created, and the prompt changes to the AAA Server Group Configuration Mode, wherein the AAA group can be configured.

If the specified AAA group already exists, the prompt changes to the AAA Server Group Configuration Mode, wherein the AAA group can be configured.

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

-noconfirm

Executes the command without any prompt and confirmation from the user.

Usage Guidelines

Use this command to create/configure/delete AAA server groups within the context.

Entering this command results in the following prompt:

[*context_name*]*hostname*(config-aaa-group)#

AAA Server Group Configuration Mode commands are defined in the *AAA Server Group Configuration Mode Commands* chapter.

Example

The following command enters the AAA Server Group Configuration Mode for a AAA group named *test321*:

aaa group test321

aaa nai-policy

This command sets policies on how Network Access Identifiers (NAIs) are handled during the authentication process.

Product

GGSN

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ default | no ] aaa nai-policy reformat-alg-hex-0-9`

default

Sets the NAI policy back to its default setting which is to remap hexadecimal digits in NAIs and accept calls with embedded 0x00 hexadecimal digits.

no

Disable remapping of hexadecimal digits in the NAI and reject calls that have a 0x00 hexadecimal digit embedded in the NAI.

reformat-alg-hex-0-9

Default: Enabled

Controls remapping of NAIs that consist only of hex digits 0x00 through 0x09 or if a 0x00 hexadecimal digit is embedded in the NAI.

By default, the system remaps NAIs that consist solely of characters 0x00 through 0x09to their ASCII equivalent. For example; 0x00 0x01 0x2 0x03 will get remapped to 123.

Also by default the system accepts an NAI containing one or more 0x00 characters within the NAI ignoring all characters after the first 0x00.

When this keyword is disabled NAIs are processed as follows:

- Remapping of hexadecimal digits 0x00 through 0x09 within the user-provided NAI is disabled.
- When the NAI has an embedded 0x00 character anywhere within it (including if there is an extra 0x00 character at the end) the call is rejected.

Usage Guidelines

Use this command to disable or re-enable remapping of hexadecimal digits in the NAI.

Example

The following command disables the remapping of hexadecimal digits in the NAI:

```
no aaa nai-policy reformat-alg-hex-0-9
```

aaa tacacs+

Enables and disables TACACS+ AAA services for this context

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ default | no ] aaa tacacs+
```

default

Enables TACSCS+ services for this context.

no

Disables TACACS+ services for this context.

Usage Guidelines

Use this command to disable or re-enable TACACS+ AAA services for this context.



Important You must first enable TACACS+ services using the Global Configuration mode **aaa tacacs+** command. This command enables TACACS+ services for all contexts. You can then use the Context Configuration mode **no aaa tacacs+** command to selectively disable TACACS+ per context.

Example

The following command disables TACACS+ AAA services for this context:

```
no aaa tacacs+
```

access-list undefined

Configures the behavior of access control for the current context when an undefined access control list is specified.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`access-list undefined { deny-all | permit-all }`
`{ default | no } access-list undefined`

default

Configures the default setting.

no

Disables handling undefined access lists.

deny-all

Specifies to drop all packets when an undefined ACL is specified.

permit-all

Specifies to forward all packets when an undefined ACL is specified.

Usage Guidelines

Use this command to specify the default behavior when an ACL specified does not exist.

When the security policies require strict access control the **deny-all** handling should be configured.

Example

The following command sets the packet handling to ignore (drop) all packets when an undefined ACL is specified.

`access-list undefined deny-all`

administrator

Configures a user with Administrator privileges in the current context.

Product

All

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

administrator *user_name* **[encrypted] [nopassword] password** *password* **[max-age** *days***][no-max-age]| [ecs] [expiry-date** *date_time* **] [ftp [sftp-server** *sftp_name* **]] [li-administration] [nocli] [noconsole] [noecs] [timeout-absolute** *timeout_absolute* **] [timeout-min-absolute** *timeout_min_absolute* **] [timeout-idle** *timeout_idle* **][timeout-min-idle** *timeout_min_idle* **][exp-grace-interval** *days***][exp-warn-interval** *days***][no-exp-grace-interval][no-exp-warn-interval]**

Syntax Description

no administrator *user_name*

no

Removes Security Administrator privileges for the specified user name.

user_name

Specifies the username for which Security Administrator privileges must be enabled in the current context. *user_name* must be an alphanumeric string of 1 through 32 characters.

[encrypted] password *password*

Specifies password for the user name. Optionally, the **encrypted** keyword can be used to specify the password uses encryption.

password must be an alphanumeric string of 1 through 63 characters without encryption, and 1 through 132 characters with encryption.

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

[nopassword]

This option allows you to create an administrator without an associated password. Enable this option when using ssh public keys (**authorized key** command in SSH Configuration mode) as a sole means of authentication. When enabled this option prevents someone from using an administrator password to gain access to the user account.

ecs

Permits the user to use ACS-specific configuration commands. Default: Permitted

expiry-date *date_time*

Specifies the date and time that this login account expires.

Enter the date and time in the YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss format. Where YYYY is the year, MM is the month, DD is the day of the month, HH is the hour, mm is minutes, and ss is seconds.

ftp

Permits the user to use FTP and SFTP. Default: Not permitted

[sftp-server *sftp_name*]

Assigns an optional root directory and access privilege to this user. *sftp_name* must have been previously created via the SSH Server Configuration mode **subsystem sftp** command.

li-administration

Refer to the *Lawful Intercept Configuration Guide* for a description of this parameter.

nocli

Prevents the user from using the command line interface. Default: Permitted

noconsole

Disables user access to a Console line.



Note The Global Configuration mode **local-user allow-aaa-authentication noconsole** command takes precedence in a normal (non-Trusted) StarOS build. In this case, all AAA-based users cannot access a Console line.

noecs

Prevents the user from accessing ACS-specific commands.

timeout-absolute *timeout_absolute*



Important This keyword is obsolete. It has been left in place for backward compatibility. If used, a warning is issued and the value entered is rounded to the nearest whole minute.

Specifies the maximum time, in seconds, the Security Administrator may have a session active before the session is forcibly terminated. *timeout_absolute* must be an integer from 0 through 300000000.

The value 0 disables this timeout configuration.

Default: 0

timeout-min-absolute *timeout_min_absolute*

Specifies the maximum time (in minutes) the Security Administrator may have a session active before the session is forcibly terminated. *timeout_min_absolute* must be an integer from 0 through 525600. The value 0 disables this timeout configuration. Default: 0

timeout-idle *timeout_idle*



Important This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.

Specifies the maximum time, in seconds, the Security Administrator may have a session active before the session is terminated. *timeout_idle* must be an integer from 0 through 300000000.

The value 0 disables the idle timeout configuration.

Default: 0

timeout-min-idle *timeout_min_idle*

Specifies the maximum time, in minutes, the Security Administrator may have a session active before the session is terminated. *timeout_min_idle* must be an integer from 0 through 525600. The value 0 disables the idle timeout configuration. Default: 0

Usage Guidelines

Use this command to create new Security Administrators or modify existing user's settings.

Security Administrator users have read-write privileges and full access to all contexts and command modes. Refer to the *Command Line Interface Overview* chapter for more information.



Important A maximum of 128 administrative users and/or subscribers may be locally configured per context.

[max-age *days*]

Defines the maximum age of a user password before it has to be changed. **max-age** is the replacement for **expiry-date**.

[no-max-age]

This parameter ensures that password never expires (these are non expiring passwords).

exp-warn-interval *days*

Impends password expiry warning interval in days. There is no default value at per user level. If any of the value is specified, Context global values are considered.

For example:

```
administrator trexpac111 password pass@1234
```

In the previous example, there are no values for expiry, grace, and warn are provided. In this case, Global values for both of them will be considered.

[no-exp-warn-interval]

Disables impending password expiry warnings .

exp-grace-interval *days*

Specifies password expiry grace interval in days. Default = 3 days after expiry.

[no-exp-grace-interval]

Disables grace period of expired password.

Example

The following command creates a Security Administrator account named *user1* with access to ACS configuration commands:

```
administrator user1 password secretPassword
```

The following removes the Security Administrator account named *user1*:

```
no administrator user1
```

Example

The following command shows the notifications you will receive if the password is not reset before the expiration date:

administrator *user_name* **password** *password* **[max-age** *days*]**[password-exp-grace-interval** *days*]**[password-exp-grace-interval** *days*]

```
login: xxx
password: xxx
1. <Normal>
# <you are logged in>

2. <When in warning period>
Warning: Your password is about to expire in 0 days.
We recommend you to change password after login.
Logins are not allowed without acknowleding this.
Do you wish to continue [y/n] (times out in 30 seconds) :

3.<when in grace period>
Your password has expired
Current password:
New password:
Repeat new password:

4. <after the grace period>
Password Expired (even beyond grace period, if configured). Contact Security Administrator
 to reset password
```

apgroupname-list

Configure apgroupname-list under the samog context with blocked apgroupnames.

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

```
[ no ] apgroupname-list aplistname1
          [ no ] apgrp apgrpname1
```

no apgroupname-list*aplistname1*

apgroupname-list: Configures the APGROUPNAME list.

Only 25 AP group names are allowed to be configured in the list. You can create a maximum of 10 AP group name lists per context.

If the **apgroupname-list** is dis-associated for any specific samog-service, then AP group names under the list are considered as allowed for the session continuation.

no apgrp *apgrpname1*

no: Removes APGROUPNAME entry from APGROUPNAME list.

apgrp: Configures blocked apgroup names within the list.

apgrp: Configures blocked apgroup names within the list.

apn

Creates or deletes Access Point Name (APN) templates and enters the APN Configuration Mode within the current context.

Product GGSN

P-GW

SAEGW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] apn apn_name [ -noconfirm ]
```

no

Deletes a previously configured APN template.

apn_name

Specifies a name for the APN template as an alphanumeric string of 1 through 62 characters that is case insensitive. It may also contain dots (.) and/or dashes (-).

-noconfirm

Executes the command without any additional prompt and confirmation from the user.



Caution If this keyword option is used with the **no apn** *apn_name* command, the APN named *apn_name* will be deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage Guidelines This command creates an APN within the system and causes the CLI to enter the APN Configuration Mode.

The APN is a logical name for a packet data network and/or a service to which the system supports access. When a create PDP context request is received by the system, it examines the APN information element within the packet. The system determines if an APN with the identical name is configured. If so, the system uses the configuration parameters associated with that APN as a template for processing the request. If the names do not match, the request is rejected with a cause code of 219 (DBH, Missing or unknown APN).

APN templates should be created/configured within destination contexts on the system.

- Up to 1000 APNs can be configured in the GGSN.
- In StarOS v12.x and earlier, up to 1024 APNs can be configured in the P-GW.
- In StarOS v14.0 and later, up to 2048 APNs can be configured in the P-GW (SAEGW).

Example

The following command creates an APN template called *isp1*:

```
apn isp1
```

asn-qos-descriptor

Creates, deletes or manages the Quality of Service (QoS) descriptor table identifier for Access Service Node Gateway (ASN-GW) service and enters the ASN QoS Descriptor Table Identifier Configuration mode within the source context.

Product ASN-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
asn-qos-descriptor id qos_table_id [ default ] dscp [ be | af11 | af12 |
af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af 43 |
ef ] [ -noconfirm ]
no asn-qos-descriptor qos_table_id [ default ] dscp [ be | af11 | af12 |
af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af 43 |
ef ] [ -noconfirm ]
```

no

Deletes a preciously configured ASN QoS descriptor table identifier.

id *qos_table_id*

Specifies a unique identifier for ASN QoS descriptor table to create/configure. *qos_table_id* must be an integer from 1 through 65535.

[default] dscp

Specifies DSCP marking for this QoS descriptor.

[be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af 43 | ef]

The DSCP marking for this QoS descriptor. Default value is be (best effort).

-noconfirm

Executes the command without any additional prompt and confirmation from the user.



Caution If this keyword option is used with **no asn-qos-descriptor id** *qos_table_id* command, the ASN QoS descriptor table with identifier *qos_table_id* will be deleted with all active/inactive configurations without prompting any warning or confirmation.

Usage Guidelines

Use this command to configure a QoS description table to manage QoS functionality for an ASN-GW service subscriber. This command creates and allows the configuration of QoS tables with in a context. This command is also used to remove previously configured ASN-GW services QoS descriptor table.

A maximum of 16 QoS Descriptor Tables can be configured per system.

Refer to the *ASN QoS Descriptor Configuration Mode Commands* chapter of this reference for additional information.

Example

The following command creates a QoS descriptor table with identifier *1234* for the ASN-GW service subscribers:

```
asn-qos-descriptor id 1234
```

asn-service-profile

Creates, deletes or manages the Service Profiles Identifier for Access Service Node Gateway (ASN-GW) service subscribers and enters the ASN Service Profile Configuration mode within the current context.

Product

ASN-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
asn-service-profile id asn_profile_id direction { bi-directional | downlink
 | uplink } [ activation-trigger { activate | admit | dynamic-reservation
 | provisioned } [ -noconfirm ]
no asn-service-profile id asn_profile_id [ -noconfirm ]
```

no

Deletes a preciously configured ASN service profile identifier.

id *asn-profile_id*

Specifies a unique identifier for ASN profile to create/configure.

direction { bi-directional | downlink | uplink }

Specifies the direction of data traffic to apply this service profile.

bi-directional: Enables this service profile in both direction of uplink and downlink.

downlink: Enables this service profile in downlink direction, towards the subscriber.

uplink: Enables this service profile in uplink direction, towards the system.

activation-trigger { activate | admit | dynamic-reservation | provisioned

Use this option to configure the activation-trigger for the asn-service-profile. Default: provisioned | admit | activate

-noconfirm

Executes the command without any additional prompt and confirmation from the user.



Caution If this keyword option is used with **no asn-service-profile id** *asn_profile_id* command, the ASN service profile with identifier *asn_profile_id* will be deleted with all active/inactive configurations without prompting any warning or confirmation.

Usage Guidelines

Use this command to configure a service profile to apply the ASN-GW service subscribers. This command creates and allows the configuration of service profiles with in a context. This command is also used to remove previously configured ASN-GW services profiles.

A maximum of 32 ASN Service Profiles can be configured per context.

Refer to the *ASN Service Profile Configuration Mode Commands* chapter of this reference for additional information.

Example

The following command creates an ASN Service Profile with identifier *1234* for the ASN-GW service subscribers:

```
asn-service-profile id 1234 direction uplink
```

asngw-service

Creates, deletes or manages an Access Service Node Gateway (ASN-GW) service and enters the ASN Gateway Service Configuration Mode within the current context.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
asngw-service asngw_name [ -noconfirm ]
no asn-service asngw_name
```

no

Deletes a previously configured ASN-GW service.

asngw_name

Specifies the name of the ASN-GW service to create/configure as an alphanumeric string of 1 through 63 characters that is case sensitive.



Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.



Caution If this keyword option is used with **no asn-service** *asngw_name* command, the ASN-GW service named *asngw_name* will be deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage Guidelines Services are configured within a context and enable certain functionality. This command creates and allows the configuration of services enabling the system to function as an ASN Gateway in a WiMAX network. This command is also used to remove previously configured ASN-GW services.

A maximum of 256 services (regardless of type) can be configured per system.



Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Refer to the *ASN Gateway Service Configuration Mode Commands* chapter of this reference for additional information.

Example

The following command creates an ASN-GW service name *asn-gw1*:

```
asngw-service asn-gw1
```

asnpc-service

Creates, deletes or manages an ASN Paging Controller service to manage the ASN paging controller service and enters the ASN Paging Controller Configuration mode within the current context.

Product ASN-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **[no] asnpc-service** *asn_pc_svc_name* **[-noconfirm]**

no

Deletes a preciously configured ASN paging controller service.

asnpc-service *asn_pc_svc_name*

Specifies the name of the ASN Paging Controller Service to create and enable as an alphanumeric string of 1 through 63 characters that is case sensitive.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Caution If this keyword option is used with **no asnpc-service** *asn_pc_svc_name* command, the ASN Paging Controller service named *asn_pc_svc_name* will be deleted and disabled with all active/inactive paging groups and paging agents configured in a context for ASN paging controller service without prompting any warning or confirmation.

Usage Guidelines

Use this command to create and enable the ASN paging controller services in the system to provide functionality of an ASN Paging Controller service within a context. Additionally this command provides the access to the ASN Paging Controller Service Configuration mode and also used to remove previously configured ASN Paging Controller services.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Refer to the *ASN Paging Controller Service Configuration Mode Commands* chapter of this reference for additional information.

Example

The following command creates an ASN paging controller service name *asnpc_1*:

```
asnpc-service asnpc_1
```

associate

Associate a global QoS Level 2 mapping table to a VPN context.

Product

ePDG

HSGW

P-GW

SAEGW

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context*context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

associate l2-mapping-table name *map_table_name*
default associate l2-mapping-table

default

Associates the system-default table with this context.

name*map_table_name*

Specifies the name of an existing internal table from which to map QoS to L2 values.

map_table_name is an alphanumeric string of 0 through 80 characters.

Usage Guidelines

This command is used to associate an internal QoS L2 mapping table to a VPN context. If no explicit association is created/configured, the system-default mapping table is used.

Important If an l2-mapping-table association is made at both the VRF and VPN level, the VRF level takes precedence.

The mapping table is configured via the Global Configuration mode **qos l2-mapping-table** command.

Example

The following command associates an internal QoS L2 mapping table to a VPN context:

```
associate l2-mapping-table qostable1
```

bfd-protocol

Enables or disables Bidirectional Forwarding Detection (BFD) protocol and enters the BFD Configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

```
[ no ] bfd-protocol
```

no

If previously configured, disables BFD protocol.

Usage Guidelines Use this command to set configuration parameters for detecting faults in paths established with BFD-enabled routers.

Refer to the *BFD Configuration Mode Commands* chapter for additional information.

Example

The following command enables BFD Configuration mode:

```
bfd-protocol
```

bgp extended-asn-cap

Enables or disables the router to send 4-octet ASN capabilities.

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
[ no ] bgp extended-asn-cap
```

no

Disables the ability of the router to send 4-octet ASN capabilities.

Example

The following command enables the router to send 4-octet ASN Capabilities:

```
bgp extended-asn-cap
```

bmsc-profile

Creates or deletes Broadcast Multicast Service Center (BM-SC) profiles and enters the BMSC Profile Configuration Mode within the current context.

Product GGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] bmsc-profile name` *`bmsc_profile_name`* `[ -noconfirm ]`

no

Deletes a previously configured BM-SC profile.

name *bmsc_profile_name*

Specifies a name for the BM-SC profile as an alphanumeric string of 1 through 62 characters that is case insensitive. It may also contain dots (.) and/or dashes (-).

-noconfirm

Executes the command without any additional prompt and confirmation from the user.



Caution If this keyword option is used with **no bmsc-profile name** *bmsc_profile_name* command, the BM-SC profile named *bmsc_profile_name* is deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage Guidelines

Use this command to create a BM-SC profile within the context and take the user to enter the BMSC Profile Configuration Mode.

The BM-SC profile is a logical name for a Broadcast Multicast Service Center in Multimedia Broadcast and Multicast service.

BM-SC profile should be created/configured within contexts on the system. Up to four BM-SC profiles can be configured.

Example

The following command creates a BM-SC Profile called *mbms_sc_1*:

```
bmsc-profile name mbms_sc_1
```

busyout ip

Makes addresses from an IPv4 pool in the current context unavailable once they are free.

Product

GGSN

HA

NAT

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] busyout ip pool { all | all-dynamic | all-static | name *pool_name* **vrf** *vrf_name* **} [address-range** *start_address end_address* **| lower-percentage** *percent* **| upper-percentage** *percent* **]**

no

Disables the busyout command specified.

ip

Configure IPv4 busyout information.

pool

Configure IPv4 pool busyout information.

all

Applies to all IPv4 pools in the current context.

all-dynamic

Applies to all dynamic IPv4 pools in the current context.

all-static

Applies to all static IPv4 pools in the current context.

name *pool_name*

Applies the named IP pool or IP pool group in the current context. *pool_name* must be the name of an existing IP pool or IP pool group in the current context.

Important Adding the IP Pool command and the Busyout command of the same IP Pool at the same time creates a race condition. To avoid the issues, run the IP Pool command and Busyout command separately.

vrf *vrf_name*

Busyout the IP pool by the VRF name. You can busyout and unbusy all pools in the VRF up to the limits of the context.

Note If a IP pool is already marked as **busyout** and associated with a VRF, the IP Pool busyout status remains the same .

address-range *start_address end_address*

Busyout all addresses from *start_address* through *end_address*. *start_address*: The beginning IP address of the range of addresses to busyout entered in IPv4 dotted-decimal notation.

end_address: The ending IP address of the range of addresses to busyout. This IP address must exist in the pool specified and entered in IPv4 dotted-decimal notation.

lower-percentage *percent*

Busyout the percentage of IPv4 addresses specified, beginning at the lowest numbered IP address. This is a percentage of all of the IP addresses in the specified IP pool. *percent* must be an integer from 1 through 100.

upper-percentage *percent*

Busyout the percentage of IPv4 addresses specified, beginning at the highest numbered IP address. This is a percentage of all of the IPv4 addresses in the specified IP pool. *percent* must be an integer from 1 through 100.

Usage Guidelines

Use this command to busyout IPv4 addresses when resizing an IPv4 pool.

Up to 32 instances of this command can be executed per context.

A single instance of this command can busy-out multiple IPv4 address pools in the context through the use of the **all**, **all-static**, or **all-dynamic** keywords.

Example

Assume an IPv4 pool named *Pool10* with addresses from *198.51.100.1* through *192.51.100.255*. To busy out the addresses from *192.51.100.50* through *192.51.100.100*, enter the following command:

```
busyout ip pool name Pool10 address-range 192.51.100.50 192.51.100.100
```

To restore the IPv4 addresses from the previous example and make them accessible again, enter the following command:

```
no busyout ip pool name Pool10 address-range 192.51.100.50 192.51.100.100
```

To busyout configuration for IPv4 pool, enter:

```
busyout ip pool vrf vrf_1001
```

To unbusyout configuration for IPv4 pool, enter:

```
no busyout ip pool vrf vrf_1001
```

busyout ipv6

Makes addresses from an IPv6 pool in the current context unavailable once they are free.

Product

GGSN

HA

NAT

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] busyout ipv6 pool { all | all-dynamic | all-static | name *pool_name* **vrf** *vrf_name* **} [address-range** *start_address end_address* **| lower-percentage** *percent* **| upper-percentage** *percent* **]**

no

Disables the busyout command specified.

ipv6

Configure IPv6 busyout information.

pool

Configure IPv6 pool busyout information.

all

Applies to all IPv6 pools in the current context.

all-dynamic

Applies to all dynamic IPv6 pools in the current context.

all-static

Applies to all static IPv6 pools in the current context.

name *pool_name*

Applies the named IPv6 pool or IPv6 pool group in the current context. *pool_name* must be the name of an existing IPv6 pool or IPv6 pool group in the current context.

Important Adding the IPv6 Pool command and the Busyout command of the same IPv6 Pool at the same time creates a race condition. To avoid the issues, run the IPv6 Pool command and Busyout command separately.

vrf *vrf_name*

Busyout the IP pool by the VRF name. You can busyout and unbusy all pools in the VRF up to the limits of the context.



Note If a IP pool is already marked as **busyout** and associated with a VRF, the IP Pool busyout status remains the same..

address-range *start_address end_address*

Busyout all addresses from *start_address* through *end_address*. *start_address*: The beginning IP address of the range of addresses to busyout entered in IPv6 colon-separated-hexadecimal notation.

end_address: The ending IP address of the range of addresses to busyout. This IP address must exist in the pool specified and entered in IPv6 colon-separated-hexadecimal notation.

lower-percentage *percent*

Busyout the percentage of IP addresses specified, beginning at the lowest numbered IPv6 address. This is a percentage of all of the IP addresses in the specified IP pool. *percent* must be an integer from 1 through 100.

upper-percentage *percent*

Busyout the percentage of IP addresses specified, beginning at the highest numbered IPv6 address. This is a percentage of all of the IP addresses in the specified IP pool. *percent* must be an integer from 1 through 100.

Usage Guidelines

Use this command to busyout IPv6 addresses when resizing an IPv6 pool.

Up to 32 instances of this command can be executed per context.

A single instance of this command can busy-out multiple IP address pools in the context through the use of the **all**, **all-static**, or **all-dynamic** keywords.

Example

Assume an IP pool named *Pool12*. To busy out the addresses from *2700:2010:8003::* through *2700:2010:8003::*, enter the following command:

```
busyout ipv6 pool name Pool12 address-range 2700:2010:8003::
2700:2010:8003::
```

To restore the IPv6 addresses from the previous example and make them accessible again, enter the following command:

```
no busyout ipv6 pool name Pool10 address-range 2700:2010:8003::
2700:2010:8003::
```

To busyout configuration for IPv6 pool, enter:

```
busyout ipv6 pool vrf vrf_1001
```

cae-group

Creates a CAE group, which is a CAE server cluster that services TCP video requests from the Mobile Video Gateway. The Mobile Video Gateway uses the configured CAE group for CAE load balancing. The CAE (Content Adaptation Engine) is an optional component of the Mobile Videoscape.

Important In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

Product

MVG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] cae-group *cae_group_name* **[-noconfirm]**

no*cae_group_name*

Deletes the CAE group if previously configured.

cae_group_name

Creates the specified CAE group and enters the Video Group Configuration Mode. *cae_group_name* is an alphanumeric string of 1 through 79 characters.

-noconfirm

Executes the command without any prompt and confirmation from the user.

Usage Guidelines

Use this command to create a CAE group and enter the Video Group Configuration Mode. This command gets issued from the Context Configuration Mode.

Example

The following command creates a CAE group named *group_1* and enters the Video Group Configuration Mode:

cae-group group_!

camel-service

Creates an instance of the Customized Applications for Mobile Enhanced Logic (CAMEL) service and enters the CAMEL service configuration mode. This mode configures or edits the configuration for the parameters which control the CAMEL functionality on the SGSN.



Important For details about the commands and parameters, check the *CAMEL Service Configuration Mode* chapter.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] camel-service` *`srvc_name`*

no

Remove the configuration for the specified SGSN service from the configuration of the current context.

srvc_name

Creates a CAMEL service instance having a unique name expressed as an alphanumeric string of 1 through 63 characters.



Important Service names must be unique across all contexts within a chassis.

Usage Guidelines

Use this command to create, edit, or remove an CAMEL service

Example

The following command creates an CAMEL service named *camel1* in the current context:

```
camel-service camel1
```

The following command removes the CAMEL service named *camel2* from the configuration for the current context:

```
no camel-service camel2
```

cbs-service

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. This command must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

Creates a new Cell Broadcasting Service (CBS) or specifies an existing CBS and enters the CBS Configuration Mode.

Product

HNB-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] cbs-service *name*

no

Removes the specified CBS service from the context.

name

Specifies the name of a new or existing CBS service as an alphanumeric string of 1 through 63 characters that must be unique within the same context and across all contexts.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines

Use this command to create a new CBS service or modify an existing one.

CBS Configuration Mode commands are defined in the *CBS Configuration Mode Commands* chapter of this guide.

Example

Following command creates a new CBS service names *test-cbs* in the context configuration mode:

cbs-service*test-cbs*

cipher-suite

Creates a new SSL cipher suite or specifies an existing cipher suite and enters the Cipher Suite Configuration Mode.

Product

SCM

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] cipher-suite *name*

no

Removes the specified SSL cipher suite from the context.

name

Specifies the name of a new or existing SSL cipher suite as n alphanumeric string of 1 through 127 characters that must be unique across all CSCF services within the same context and across all contexts.

Usage Guidelines

Use this command to create a new SSL cipher suite or modify an existing one.

Important One SSL cipher suite can be created per SSL template.

A cipher suite contains the cryptographic algorithms supported by the client, and defines a key exchange and a cipher spec, which specifies the encryption and hash algorithms used during authentication. SSL cipher suites allow operators to select levels of security and to enable communication between devices with different security requirements.

Entering this command results in the following prompt:

```
[context_name]hostname(cfg-ctx-cipher-suite)#
```

Cipher Suite Configuration Mode commands are defined in the *Cipher Suite Configuration Mode Commands* chapter.

Example

The following command specifies the SSL cipher suite *cipher_suite_1* and enters the Cipher Suite Configuration Mode:

```
cipher-suite cipher_suite_1
```

class-map

Creates or deletes a class map. If the class-map is newly created, the system enters the Class-Map Configuration Mode within the current destination context to configure the match rules for packet classification to flow-based traffic policing for a subscriber session flow.

Product

ASN-GW

HA

HSGW

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] class-map name` *`class_name`* **`[ match-all | match-any ]`**

no

Deletes configured Class-Map within the context.

class_name

Specifies the name of Class-Map rule as an alphanumeric string of 1 through 15 characters and is case sensitive.

match-all

Default: Enabled.

Enables AND logic for all matching parameters configured in specific Class-Map to classify traffic flow/packets. It indicates to match all classification rules in specific Class-Map to consider the specified Class-Map as a match.

match-any

Default: Disabled.

Enables OR logic for matching parameters configured in specific Class-Map to classify traffic flow/packets. It indicates to match any of the classification rule in specific Class-Map to consider the specified Class-Map as a match.

Usage Guidelines

Use this command to enter in Class-Map Configuration Mode to set classification parameters or filters in traffic policy for a subscriber session flow.

Important In this mode classification rules added sequentially with **match** command to form a Class-Map. To change and/or delete or re-add a particular rule entire Class-Map is required to delete.

Example

Following command configures classification map *class_map1* with option to match any condition in match rule.

```
class-map name class_map1 match-any
```

closedrp-rp handoff

Enables or disables session handoff between Closed-RP and RP connections. Default: Disabled

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ default | no ] closedrp-rp handoff
```

default

Resets the command to its default setting of disabled.

no

Disables Closed-RP to RP session handoff.

Usage Guidelines

Use this command to enable a PDSN service to handoff sessions between Closed-RP and RP connections.

Example

To enable Closed-RP to RP handoffs, use the following command:

```
closedrp-rp handoff
```

To disable Closed-RP to RP handoffs, use the following command:

```
no closedrp-rp handoff
```

config-administrator

Configures a context-level configuration administrator account within the current context.

Product

All

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

config-administrator *user_name* **[encrypted] [nopassword] password***password* **[ecs] [expiry-date** *date_time* **] [ftp [sftp-server** *sftp_name* **] }] [li-administration] [noconsole] [nocli] [noecs] [timeout-absolute** *abs_seconds* **] [timeout-min-absolute** *abs_minutes* **] [timeout-idle** *timeout_duration* **] [timeout-min-idle** *idle_minutes* **][exp-grace-interval** *days***][exp-warn-interval** *days***][no-exp-grace-interval][no-exp-warn-interval]**
no config-administrator *user_name*

no

Removes a previously configured context-level configuration administrator account.

user_name

Specifies the name for the account as an alphanumeric string of 1 through 32 characters.

[encrypted] password *password*

Specifies the password to use for the user which is being given context-level administrator privileges within the current context. The encrypted keyword indicates the password specified uses encryption.

password is 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 system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the password keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

[nopassword]

This option allows you to create a configuration administrator without an associated password. Enable this option when using ssh public keys (**authorized key** command in SSH Configuration mode) as a sole means of authentication. When enabled this option prevents someone from using a configuration administrator password to gain access to the user account.

ecs

Permits the user access to ACS-specific configuration commands. Default: Enhanced Charging Service (ECS / ACS) specific configuration commands allowed.

expiry-date *date_time*

Specifies the date and time that this account expires in the format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss.

Where YYYY is the year, MM is the month, DD is the day of the month, HH is the hour, mm is minutes, and ss is seconds.

ftp

Indicates the user gains FTP and SFTP access with the administrator privileges. Default: FTP and SFTP are not allowed.

[sftp-server *sftp_name*]

Assigns an optional root directory and access privilege to this user. *sftp_name* must have been previously created via the SSH Server Configuration mode **subsystem sftp** command.

li-administration

Refer to the *Lawful Intercept Configuration Guide* for a description of this parameter.

nocli

Indicates the user is not allowed to access the command line interface. Default: CLI access allowed.

noconsole

Disables user access to a Console line.



Note The Global Configuration mode **local-user allow-aaa-authentication noconsole** command takes precedence in a normal (non-Trusted) StarOS build. In this case, all AAA-based users cannot access a Console line.

noecs

Prevents the specific user from accessing ACS-specific configuration commands.

timeout-absolute *abs_seconds*



Important This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.

Specifies the maximum amount of time (in seconds) that the administrator may have a session active before the session is forcibly terminated. *abs_seconds* must be an integer from 0 through 300000000. The value 0 disables the absolute timeout. Default: 0

timeout-min-absolute *abs_minutes*

Specifies the maximum amount of time (in minutes) the context-level administrator may have a session active before the session is forcibly terminated. *abs_minutes* must be an integer from 0 through 525600 (365 days). The value 0 disables the absolute timeout. Default: 0

timeout-idle *timeout_duration*

Important This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.

Specifies the maximum amount of idle time, in seconds, the context-level administrator may have a session active before the session is terminated. *timeout_duration* must be a value in the range from 0 through 300000000. The value 0 disables the idle timeout. Default: 0

timeout-min-idle *idle_minutes*

Specifies the maximum amount of idle time, in minutes, the context-level administrator may have a session active before the session is terminated. *idle_minutes* must be a value in the range from 0 through 525600 (365 days). The value0 disables the idle timeout. Default: 0

Usage Guidelines

Create new context-level configuration administrators or modify existing administrator's options, in particular, the timeout values.

Configuration administrator users have read-write privileges and full access to all contexts and command modes except for security functions. Refer to the *Command Line Interface Overview* chapter of this guide for more information.

Important A maximum of 128 administrative users and/or subscribers may be locally configured per context.

[max-age *days*]

Defines the maximum age of a user password before it has to be changed. **max-age** is the replacement for **expiry-date**.

[no-max-age]

This parameter ensures that password never expires (these are non expiring passwords).

exp-warn-interval *days*

Impends password expiry warning interval in days. There is no default value at per user level. If any of the value is specified, Context global values are considered.

For example:

```
config-administrator trexpac111 password pass@1234
```

In the previous example, there are no values for expiry, grace, and warn are provided. In this case, Global values for both of them will be considered.

[no-exp-warn-interval]

Disables impending password expiry warnings .

exp-grace-interval *days*

Specifies password expiry grace interval in days. Default = 3 days after expiry.

[no-exp-grace-interval]

Disables grace period of expired password.

Example

The following configures a context-level administration named *user1* with ACS parameter control:

```
config-administrator user1 password secretPassword ecs
```

The following command removes a context-level administrator named *user1*:

```
no config-administrator user1
```

Example

The following command shows the notifications you will receive if the password is not reset before the expiration date:

config-administrator *user_name* **password** *password* **[max-age** *days*]**[password-exp-grace-interval** *days*]**[password-exp-grace-interval** *days*]

```
login: xxx
password: xxx
1. <Normal>
# <you are logged in>

2. <When in warning period>
Warning: Your password is about to expire in 0 days.
We recommend you to change password after login.
Logins are not allowed without acknowleding this.
Do you wish to continue [y/n] (times out in 30 seconds) :

3.<when in grace period>
Your password has expired
Current password:
New password:
Repeat new password:

4. <after the grace period>
Password Expired (even beyond grace period, if configured). Contact Security Administrator
 to reset password
```

content-filtering

Enables or disables the creation, configuration or deletion of Content Filtering Server Groups (CFSG).

Product CF

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
content-filtering server-group cf_server_group_name [ -noconfirm ]
no content-filtering server-group cf_server_group_name
```

no

Removes the specified CFSG previously configured in this context.

server-group *cf_server_group_name*

Specifies the name of the CFSG as an alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any prompt and confirmation from the user.

Usage Guidelines Use this command to create/configure/delete a CFSG.

Example

The following command creates a CFSG named *CF_Server1*:

```
content-filtering server-group CF_Server1
```

credit-control-service

Enables or disables the creation, configuration or deletion of credit-control services.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
credit-control-service service_name [ -noconfirm ]
no credit-control-service service_name
```

no

Deletes the specified credit-control service.

service_name

Specifies name of the credit-control service as an alphanumeric string of 1 through 63 characters.

If the named credit-control service does not exist, it is created, and the CLI mode changes to the Credit Control Service Configuration Mode wherein the service can be configured.

If the named credit-control service already exists, the CLI mode changes to the Credit Control Service Configuration Mode wherein the service can be configured.



Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to create, configure or delete credit-control services.

Entering this command results in the following prompt:

[*context_name*]*hostname*(config-credit-control-service)

Credit control Service Configuration commands are described in the *Credit Control Service Configuration Mode Commands* chapter.

Example

The following command enters the Credit Control Service Configuration Mode for a credit-control service named *test159*:

```
credit-control-service test159
```

crypto dns-nameresolver

Enables or disables the reverse DNS query from a Security Gateway to DNS.

Product

All IPsec security gateway products



Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] crypto dns-nameresolver

no

Disables the Reverse DNS query.

Usage Guidelines

Use this command to enable or disable the reverse DNS query from a WSG to DNS.

Important You must configure the DNS client prior to enabling the Reverse DNS query.

Example

The following command enables the reverse DNS query:

crypto dns-nameresolver

crypto group

Creates or deletes a crypto group and enters the Crypto Configuration Mode allowing the configuration of crypto group parameters.

Product

HA

GGSN

PDIF

PDSN

SCM

Privilege

Administrator, Config-Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] crypto group *group_name*

no

Deletes a previously configured crypto group.

group_name

Specifies the name of the crypto group as an alphanumeric string of 1 through 127 characters that is case sensitive.

Important A maximum of 32 crypto groups per context can be configured.

Usage Guidelines

Use this command to enter the configuration mode allowing the configuration of crypto group parameters.

Crypto (tunnel) groups are used to support the Redundant IPSec Tunnel Fail-over feature and consist of two configured ISAKMP crypto maps. Each crypto map defines the IPSec policy for a tunnel. In the crypto group, one tunnel serves as the primary, the other as the secondary (redundant).

Example

The following command configures a crypto group called *group1*:

```
crypto group group1
```

crypto ipsec transform-set

Configures transform-sets on the system and enters the Crypto IPSec Transform Set Configuration Mode.

Product

PDSN

PDIF

HA

GGSN

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
crypto ipsec transform-set transform_name [ ah { hmac { md5-96 | none |
sha1-96 } { esp { hmac { { md5-96 | sha1-96 } { cipher { 3des-cbc |
aes-cbc-128 | aes-cbc-256 | des-cbc } } | none } } } } ]
no crypto ipsec transform-set transform_name
```

no

Removes a previously configured transform set

transform_name

Specifies the name of the transform set as an alphanumeric string of 1 through 127 characters that is case sensitive.

ah hmac

Configures the Authentication Header (AH) hash message authentication codes (HMAC) parameter for the transform set to one of the following:

- **md5-96**:Message Digest 5 truncated to 96 bits
- **sha1-96**:Secure Hash Algorithm-1 truncated to 96 bits

esp hmac

Configures the Encapsulating Security Payload (ESP) hash message authentication codes (HMAC) parameter for the transform set to one of the following:

- **md5-96**:Message Digest 5 truncated to 96 bits
- **none**: Disables the use of the AH protocol for the transform set.
- **sha1-96**:Secure Hash Algorithm-1 truncated to 96 bits

cipher

If ESP is enabled, this option must be used to set the encapsulation cipher protocol to one of the following:

- **3des-cbc**: Triple Data Encryption Standard (3DES) in chain block (CBC) mode.
- **aes-cbc-128**: Advanced Encryption Standard (AES) in CBC mode with a 128-bit key.
- **aes-cbc-256**: Advanced Encryption Standard (AES) in CBC mode with a 256-bit key.
- **des-cbc**: DES in CBC mode.

Usage Guidelines

Use this command to create a transform set on the system.

Transform Sets are used to define IPSec security associations (SAs). IPSec SAs specify the IPSec protocols to use to protect packets.

Transform sets are used during Phase 2 of IPSec establishment. In this phase, the system and a peer security gateway negotiate one or more transform sets (IPSec SAs) containing the rules for protecting packets. This negotiation ensures that both peers can properly protect and process the packets.

Example

Create a transform set that has the name *tset1*, no authentication header, an encapsulating security protocol header hash message authentication code of **md5**, and a bulk payload encryption algorithm of **des-cbc** with the following command:

```
crypto ipsec transform-set tset1 ah hmac none esp hmac md5 cipher des-cbc
```

crypto map

Configures the name of the policy and enters the specified Crypto Map Configuration mode.

Product

PDSN

HA

GGSN

SCM

P-GW

PDIF

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

crypto map *name* **[ikev2-ipv6 | ipsec-dynamic | ipsec-ikev1 | ipsec-manual]**
no crypto map *name*

no

Removes a previously configured crypto map.

name

Specifies the name of the crypto map as an alphanumeric string of 1 through 127 characters that is case sensitive.

ikev2-ipv6

Refer to the *Lawful Intercept Configuration Guide* for a description of this parameter.

ipsec-dynamic

Creates a dynamic crypto map and/or enters the Crypto Map Dynamic Configuration Mode.

ipsec-ikev1

Creates an IKEv1 crypto map and/or enters the Crypto Map IKEv1 Configuration Mode.

ipsec-manual

Creates a manual crypto map and/or enters the Crypto Map Manual Configuration Mode.

Usage Guidelines

Crypto Maps define the policies that determine how IPSec is implemented for subscriber data packets. There are several types of crypto maps supported by the system. They are:

- **Manual crypto maps**: These are static tunnels that use pre-configured information (including security keys) for establishment. Because they rely on statically configured information, once created, the tunnels never expire; they exist until their configuration is deleted.

Important Because manual crypto map configurations require the use of static security keys (associations), they are not as secure as crypto maps that rely on dynamically configured keys. Therefore, it is recommended that they only be configured and used for testing purposes.

- **IKEv1 crypto maps**: These tunnels are similar to manual crypto maps in that they require some statically configured information such as the IP address of a peer security gateway and that they are applied to specific system interfaces. However, IKEv1 crypto maps offer greater security because they rely on dynamically generated security associations through the use of the Internet Key Exchange (IKE) protocol.
- **IKEv2-IPv6 cryptomaps**: Refer to the *Lawful Intercept Configuration Guide* for a description of this parameter.
- **Dynamic crypto maps:** These tunnels are used for protecting L2TP-encapsulated data between the system and an LNS/security gateway or Mobile IP data between an FA service configured on one system and an HA service configured on another.

Important The crypto map type (dynamic, IKEv1, IKEv2-IPv6, or manual) is specified when the map is first created using this command.

Example

Create a dynamic crypto map named *map1* and enter the Crypto Map Dynamic Configuration Mode by entering the following command:

```
crypto map map1 ipsec-dynamic
```

crypto template

Creates a new or specifies an existing crypto template or crypto vendor template and enters the Crypto Template Configuration Mode or Crypto Template IKEv2-Vendor Configuration Mode.

Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. This command must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

HeNBGW

PDIF

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
crypto template name { ikev2-dynamic | ikev2-vendor }
 [ no ] notify-payload pdn-type-allowed
no crypto template name
```

no

Removes a previously configured crypto template.

***name* ikev2-pdif**

Specifies the name of a new or existing crypto template as an alphanumeric string of 1 through 127 characters.

ikev2-dynamic

Configures the Crypto Template to be used for IPSec functionalities.

ikev2-vendor

Configures the Crypto Vendor Template to be used for IPSec functionalities.

notify-payload pdn-type-allowed

Enables sending of PDN type notification in Notify Payload.

no notify-payload pdn-type-allowed

Disables sending of PDN type notification in Notify Payload.

Usage Guidelines

Use this command to create a new or enter an existing crypto template or crypto vendor template.

The Crypto Template Configuration Mode commands are defined in the *Crypto Template Configuration Mode Commands* chapter.

The Crypto Template IKEv2-Vendor Configuration Mode commands are defined in the *Crypto Template IKEv2-Vendor Configuration Mode Commands* chapter.

Example

The following command configures a IKEv2 dynamic crypto template called *crypto1* and enters the Crypto Template Configuration Mode:

```
crypto template crypto1 ikev2-dynamic
```

crypto vendor-policy

Creates a new or specifies an existing crypto vendor policy and enters the Crypto Vendor Policy Configuration Mode.

Product

ePDG

HeNBGW

PDIF

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] crypto vendor-policy` *`policy_name`*

no

Removes the previously configured vendor policy.

policy_name

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

Usage Guidelines

Use this command to Creates a new or specifies an existing crypto vendor policy and enters the Crypto Vendor Policy Configuration Mode. A maximum of 32 vendor policies can be configured.

The Crypto Vendor Policy Configuration Mode commands are defined in the *Crypto Vendor Policy Configuration Mode Commands* chapter.

Example

The following command configures a crypto vendor policy called *vodvp1* and enters the Crypto Vendor Policy Configuration Mode:

```
crypto vendor-policy vodvp1
```

css server

In StarOS 9.0 and later releases, this command is obsolete. And, in earlier releases, this command is restricted.

cups chunk-threshold-timer

Configures CUPS IP pool chunk threshold timer for a context.

Product

CUPS

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

cups chunk-threshold-timer *threshold_timer_seconds*
default cups chunk-threshold-timer

default

Sets the default value of 60 seconds.

threshold_timer_seconds

threshold_timer_seconds specifies the chunk threshold timer value in seconds, integer 30 to 300.

Usage Guidelines

Use this command to configure CUPS IP pool chunk threshold timer for a context.

Example

The following command configures CUPS IP pool chunk threshold timer for *120* seconds:

cups chunk-threshold-timer 120

cups enabled

Enables CUPS for a context.

Product

CUPS

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description `cups enabled`

Usage Guidelines Use this command to enable CUPS for a context.

cups max-user-planes

Configures maximum number of User Planes expected to be functional in a system.

Product CUPS

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
cups max-user-planes value
default max-user-planes
```

default

Sets the default maximum number of User Planes to 10.

value

The value should be in the range of 1 through 1000.

Usage Guidelines Use this command to configure maximum number of User Planes expected to be functional in a system.

Example

The following command configures maximum number of User Planes to *15*:

```
cups max-user-planes 15
```

cups min-chunks-threshold-per-pool

Configures minimum percentage of chunks per pool in a context.

Product CUPS

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

cups min-chunks-threshold-per-pool *threshold_percent*
default min-chunks-threshold-per-pool

default

Sets the default percentage to 10.

threshold_percent

threshold_percent specifies minimum chunks in percentage of 0 to 50.

Usage Guidelines

Use this command to configure minimum percentage of chunks per pool in a context.

Example

The following command configures minimum percentage of chunks per pool in a context to *20* %:

```
cups min-chunks-threshold-per-pool 20
```

cups-redundancy-protocol

Enables or disables CUPS Redundancy Protocol (CRP) and enters the CRP Configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] cups-redundancy-protocol

no

If previously configured, disables CRP.

Usage Guidelines

Enables or disables the CRP Configuration Mode on a chassis.

Entering this command results in the following prompt:

```
[context_name]hostname(config-crp)#
```

Refer to the *CRP Configuration Mode Commands* chapter for additional information.

Example

The following command enters CRP Configuration mode:

cups-redundancy-protocol

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.

dhcp-client-profile

Adds a specified Dynamic Host Control Protocol (DHCP) client profile name to allow configuration of DHCP client profile to the current context and enters the configuration mode for that profile.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no]dhcp-client-profile *clnt_profile_name* **[-noconfirm]**

no

Removes a previously configured DHCP client profile from the current context.

clnt_profile_name

Specifies the name of the DHCP client profile as an alphanumeric string of 1 through 63 characters that is case sensitive.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

⚠

Caution If this keyword option is used with **no dhcp-client-profile** *clnt_profile_name* command the DHCP client profile named *clnt_profile_name* is deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage Guidelines

Use this command to add a DHCP client profile to a context configured on the system and enter the DHCP Client Profile Configuration Mode.

Entering this command results in the following prompt:

```
[context_name]hostname(config-dhcp-client-profile)#
```

DHCP Client Profile Configuration Mode commands are defined in the *DHCP Client Profile Configuration Mode Commands* chapter.

Example

The following command creates a DHCP client profile called *test_profile* :

dhcp-client-profile *test_profile*

dhcp-server-profile

Adds a specified Dynamic Host Control Protocol (DHCP) server profile name to allow configuration of DHCP server profile to the current context and enters the configuration mode for that profile.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no]dhcp-server-profile *srvr_profile_name* **[-noconfirm]**

no

Removes a previously configured DHCP server profile from the current context.

srvr_profile_name

Specifies the name of the DHCP server profile as an alphanumeric string of 1 through 63 characters that is case sensitive.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

⚠

Caution If this keyword option is used with **no dhcp-server-profile** *srvr_profile_name* command the DHCP server profile named *srvr_profile_name* is deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage Guidelines

Use this command to add a DHCP server profile to a context configured on the system and enter the DHCP Server Profile Configuration Mode.

Entering this command results in the following prompt:

```
[context_name]hostname(config-dhcp-server-profile)#
```

DHCP Server Profile Configuration Mode commands are defined in the *DHCP Server Profile Configuration Mode Commands* chapter.

Example

The following command creates a DHCP server profile called *test_server_profile* :

dhcp-server-profile *test_server_profile*

dhcp-service

Adds a Dynamic Host Control Protocol (DHCP) service instance to the current context and enters the DHCP Service Configuration mode for that service.

Product

ASN-GW

eWAG

GGSN

HA

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

dhcp-service *service_name* **[-noconfirm]**
no dhcp-service *service_name*

no

Removes a previously configured DHCP service from the current context.

service_name

Specifies the name of the DHCP service as an alphanumeric string of 1 through 63 characters that is case sensitive.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to add a DHCP service to a context configured on the system and enter the DHCP Service Configuration Mode. A DHCP service is a logical grouping of external DHCP servers.

The DHCP Configuration Mode provides parameters that dictate the system's communication with one or more of these DHCP servers.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Refer to the *DHCP Service Configuration Mode* chapter of this reference for additional information.

Example

The following command creates a DHCP service called *dhcp1* and enters the DHCP Service Configuration Mode:

```
dhcp-service dhcp1
```

dhcpv6-service

Creates a specified DHCPv6 service name to allow configuration of DHCPv6 service to the current context and enters the configuration mode for that service.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no]dhcpv6-service *service_name* **[-noconfirm]**

no

Removes a previously configured DHCPv6 service from the current context.

service_name

Specifies the name of the DHCPv6 service as an alphanumeric string of 1 through 63 characters that is case sensitive.



Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.



Caution If this keyword option is used with **no dhcpv6-service** *service_name* command the DHCPv6 service named *service_name* is deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage Guidelines

Use this command to add a DHCPv6 service to a context configured on the system and enter the DHCPv6 Service Configuration Mode.

The DHCPv6 Service Configuration Mode provides parameters that dictate the system's communication with one or more of these DHCPv6 servers.

Entering this command results in the following prompt:

```
[context_name]hostname(config-dhcpv6-service)#
```

DHCPv6 Service Configuration Mode commands are defined in the *DHCPv6 Service Configuration Mode Commands* chapter.



Important A maximum of 256 services (regardless of type) can be configured per system.

Example

The following command creates a DHCPv6 service called *dhcpv6* and enter the DHCPv6 Service Configuration Mode:

dhcpv6-service dhcpv6

diameter accounting

This command configures Diameter accounting related settings.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

diameter accounting { dictionary { aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | dynamic-load | nasreq | rf-plus } | endpoint *endpoint_name* **| hd-mode fall-back-to-local | hd-storage-policy** *hd_policy* **| max-retries** *max_retries* **| max-transmissions** *transmissions* **| request-timeout** *duration* **| server** *host_name* **priority** *priority* **}**
default diameter accounting { dictionary | hd-mode | max-retries | max-transmissions | request-timeout }
no diameter accounting { endpoint | hd-mode | hd-storage-policy | max-retries | max-transmissions | server *host_name* **}**

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

endpoint: Removes the currently configured accounting endpoint. The default accounting server configured in the default AAA group will be used.

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

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

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

max-transmissions: Disables the maximum number of transmission attempts for Diameter accounting in this AAA group.

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

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

dictionary: Sets the context's dictionary to the default.

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

max-retries:0 (disabled)

max-transmissions:0 (disabled)

request-timeout:20 seconds

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

Specifies the Diameter accounting dictionary.

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

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

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

rf-plus:RF Plus dictionary.

endpoint *endpoint_name*

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

endpoint_name is an alphanumeric string of 1 through 63 characters.

hd-mode fall-back-to-local

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

hd-storage-policy *hd_policy*

Specifies the HD Storage policy name.

hd_policy must be the name of a configured HD Storage policy, expressed as an alphanumeric string of 1 through 63 characters.

HD storage policies are configured through the Global Configuration Mode.

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

max-retries *max_retries*

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

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

Default: 0

max-transmissions *transmissions*

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

transmissions specifies the maximum number of transmission attempts for a Diameter request. The value must be an integer from 1 through 1000. Default: 0

request-timeout *duration*

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

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

server *host_name* priority *priority*

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

host_name specifies the Diameter host name, expressed as an alphanumeric string of 1 through 63 characters.

priority specifies the relative priority of this Diameter host. The priority is used in server selection. The priority must be an integer from 1 through 1000.

Usage Guidelines

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

Example

The following command configures the Diameter accounting dictionary as **aaa-custom4**:

```
diameter accounting dictionary aaa-custom4
```

The following command configures the Diameter endpoint named *aaaa_test*:

```
diameter accounting endpoint aaaa_test
```

diameter authentication

This command configures Diameter authentication related settings.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

diameter authentication { allow any-host | dictionary { aaa-custom1 | aaa-custom10 | aaa-custom11 | aaa-custom12 | aaa-custom13 | aaa-custom14 | aaa-custom15 | aaa-custom16 | aaa-custom17 | aaa-custom18 | aaa-custom19 | aaa-custom2 | aaa-custom20 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | dynamic-load | nasreq } | endpoint *endpoint_name* **| max-retries** *max_retries* **| max-transmissions** *transmissions* **| redirect-host-avp { just-primary | primary-then-secondary } | request-timeout** *duration* **| server** *host_name* **priority** *priority* **}**
default diameter authentication { dictionary | max-retries | max-transmissions | redirect-host-avp | request-timeout }
no diameter authentication { endpoint | max-retries | max-transmissions | server *host_name* **}**

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

- **allow any-host**: Accept the response from any-host.
- **endpoint**: Removes the authentication endpoint. The default server configured in default AAA group will be used.
- **max-retries**: Disables the retry attempts for Diameter authentication in this AAA group.
- **max-transmissions**: Disables the maximum transmission attempts for Diameter authentication in this AAA group.
- **server** *host_name*: Removes the Diameter host *host_name* from this AAA server group for Diameter authentication.

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

Configures default setting for specified parameter.

- **allow any-host**: Sets the default behaviour.

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

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

Specifies the Diameter authentication dictionary.

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



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

aaa-custom9: Configures the STa standard dictionary.

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

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

endpoint *endpoint_name*

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

endpoint_name is an alphanumeric string of 1 through 63 characters.

max-retries *max_retries*

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

max_retries specifies the maximum number of retry attempts, and must be an integer from 1 through 1000. Default: 0

max-transmissions *transmissions*

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

transmissions specifies the maximum number of transmission attempts, and must be an integer from 1 through 1000. Default: 0

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

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

just-primary:Redirect only to primary host.

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

Default: **just-primary**

request-timeout *duration*

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

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

server *host_name* priority *priority*

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

host_name specifies the Diameter host name, expressed as an alphanumeric string of 1 through 63 characters.

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

Usage Guidelines

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

Example

The following command configures the Diameter authentication dictionary *aaa-custom14*:

```
diameter authentication dictionary aaa-custom14
```

The following command configures the Diameter endpoint named *aaau1*:

```
diameter authentication endpoint aaau1
```

diameter authentication failure-handling

This command configures error handling for Diameter EAP requests.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

diameter authentication failure-handling { authorization-request | eap-request | eap-termination-request } { request-timeout action { continue | retry-and-terminate | terminate } | result-code *result_code* **{ [to** *end_result_code* **] action { continue | retry-and-terminate | terminate } } }**
no diameter authentication failure-handling { authorization-request | eap-request | eap-termination-request } result-code *result_code* **[to** *end_result_code* **]**
default diameter authentication failure-handling { authorization-request | eap-request | eap-termination-request } request-timeout action

no

Disables Diameter authentication failure handling.

default

Configures the default Diameter authentication failure handling setting.

authorization-request

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

eap-request

Specifies configuring failure handling for EAP requests.

eap-termination-request

Specifies configuring failure handling for EAP termination requests.

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

Specifies the action to be taken for failures:

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

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

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

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

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

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

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

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

Example

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

```
diameter authentication failure-handling eap-request result-code 5002 to
 5005 action continue
diameter authentication failure-handling eap-request result-code 5003
action terminate
```

diameter dictionary

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

diameter endpoint

This command enables the creation, configuration or deletion of a Diameter endpoint.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] diameter endpoint *endpoint_name* **[-noconfirm]**

no

Removes the specified Diameter endpoint.

Important In 19.5, 21.0 and later releases, deleting the endpoint using the "no diameter endpoint" command throws the following warning message and prompts for user's confirmation:

```
Warning: It is not recommended to remove the diameter endpoint when there are active calls
 on the system. Hence, please adhere to the 'Method of Procedure' to remove the endpoint.
Otherwise, the system behavior would be undefined.

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

Method of Procedure: The following two steps should be performed in the same order to remove the Diameter endpoint:

1. To disable/breakdown the link/transport connections:
   a. Disable all the peers in the endpoint using the **diameter disable endpoint** *endpoint_name* **peer** *peer-name* CLI command. Repeat this command for all the peers in the endpoint. This will trigger the Disconnect-Peer-Request (DPR) towards the peers with the configured disconnection cause, that is to indicate, graceful shut down.
   b. Remove the endpoint in the respective context, under Diameter configuration, by using the **no endpoint** *endpoint-name* CLI command.
2. To enable/bring up the transport connections, follow the standard procedure of adding the endpoints and corresponding peers in it.
   a. Add the endpoints with "use diamproxy" option. Else, the links will be established from Session Manager via diabase library.
   b. Add the corresponding peers in the endpoints.

endpoint_name

Specifies name of the Diameter endpoint as an alphanumeric string of 1 through 63 characters that should be unique within the system.

If the named endpoint does not exist, it is created, and the CLI mode changes to the Diameter Endpoint Configuration Mode wherein the endpoint can be configured.

If the named endpoint already exists, the CLI mode changes to the Diameter Endpoint Configuration Mode wherein the endpoint can be reconfigured.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to create/configure/delete a Diameter origin endpoint.

Entering this command results in the following prompt:

[*context_name*]*hostname*(config-ctx-diameter)

Diameter origin endpoint configuration commands are described in the *Diameter Endpoint Configuration Mode Commands* chapter.

Example(s)

The following command changes to the Diameter Endpoint Configuration CLI mode for Diameter origin endpoint named *test13*:

diameter endpoint test13

The following command will throw the warning message and prompt for user's confirmation to remove the Diameter endpoint named *test13*. **Yes** will remove the endpoint *test13*. **No** will abort the action and the endpoint *test13* will not be removed:

```
no diameter endpoint test13
Warning: It is not recommended to remove the diameter endpoint when there are active calls
 on the system. Hence, please adhere to the 'Method of Procedure' to remove the endpoint.
Otherwise, the system behavior would be undefined.
Are you sure? [Yes|No]: No
Action aborted
```

The following command will remove the endpoint *test13* without any additional prompt and confirmation from the user:

no diameter endpoint test13 -noconfirm

diameter-hdd-module

This command enables/disables the creation, configuration or deletion of the Hard Disk Drive (HDD) module in the context.

Important This command is license dependent. For more information, contact your Cisco account representative.

Product

HA

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] diameter-hdd-module

no

Deletes the HDD module from the context.

Usage Guidelines

In cases where the Assume-Positive interim-quota is allocated, and CCR-T message is not reported/answered, the failed CCR-T message is written to a local file, and saved in the HDD. This local file and directory information can be passed to the customer, and can be fetched and parsed to account for the lost bytes/usage. The retrieval of the file can be done with the PULL mechanism.



Important This feature requires a valid license to be installed prior to configuring this feature. Contact your Cisco account representative for more information on the licensing requirements.

The **diameter-hdd-module** CLI command is used to create the HDD module for the context, and configure the HDD module for storing the failed CCR-T messages.

Entering this command results in the following prompt:

[*context_name*]*hostname*(config-diameter-hdd)#

Diameter HDD Module Configuration Mode commands are defined in the *Diameter HDD Module Configuration Mode commands* chapter.



Important This feature is applicable only when Assume Positive feature is enabled.

This feature is controlled through the **diameter hdd** CLI command introduced in the Credit Control Group configuration mode. For more information on the command, see the *Credit Control Configuration Mode Commands* chapter.

Example

The following command configures the Diameter HDD module in a context:

```
diameter hdd-module
```

diameter sctp

This command configures Diameter SCTP parameters for all Diameter endpoints within the context. In 12.2 and later releases, this command is obsolete and replaced with **associate sctp-parameters-template** command in the Diameter Endpoint Configuration Mode.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

diameter sctp { hearbeat-interval *interval* **| path max-retransmissions** *retransmissions* **}**
default diameter sctp { heartbeat-interval | path max-retransmissions }

default

Configures this command with the default settings.

- **heartbeat-interval**: Sets the heartbeat interval to the default value.
- **path max-retransmissions**: Sets the SCTP path maximum retransmissions to the default value.

hearbeat-interval *interval*

Specifies the time interval between heartbeat chunks sent to a destination transport address in seconds.

interval must be an integer from 1 through 255.

Default: 30 seconds

path max-retransmissions *retransmissions*

Specifies the maximum number of consecutive retransmissions over a destination transport address of a peer endpoint before it is marked as inactive.

retransmissions must be an integer from 1 through 10.

Default: 10

Usage Guidelines

Use this command to configure Diameter SCTP parameters for all Diameter endpoints within the context.

Example

The following command configures the heartbeat interval to *60* seconds:

```
diameter sctp hearbeat-interval 60
```

The following command configures the maximum number of consecutive retransmissions to *6*, after which the endpoint is marked as inactive:

```
diameter sctp path max-retransmissions 6
```

diameter origin

This command is deprecated and is replaced by the **diameter endpoint** command.

dns-client

Creates a DNS client and/or enters the DNS Client Configuration Mode.

Product

ePDG

MME

P-GW

SAEGW

SCM

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] dns-client` *`name`* `[ -noconfirm ]`

no

Removes the specified DNS client from the context.

dns-client *name*

Specifies a name for the DNS client as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to create a new DNS client and enter the DNS Client Configuration Mode or enter the mode for an existing client.

Entering this command results in the following prompt:

```
[context_name]hostname(config-dns-client)#
```

DNS Client Configuration Mode commands are defined in the *DNS Client Configuration Mode Commands* chapter.

Example

The following command enters the DNS Client Configuration Mode for a DNS client named *dns1*:

```
dns-client dns1
```

domain

Configures a domain alias for the current context.

Product

HA

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

domain [*]*domain_name* **[default subscriber** *subscriber_template_name* **]**
no domain [*]*domain_name*

no

Indicates the domain specified is to be removed as an alias to the current context.

[*]*domain_name*

domain_name specifies the domain alias to create/remove from the current context. If the domain portion of a subscribers user name matches this value, the current context is used for that subscriber.

domain_name must be an alphanumeric string of 1 through 79 characters. The domain name can contain all special characters, however note that the character * (wildcard character) is only allowed at the beginning of the domain name.

If the domain name is prefixed with * (wildcard character), and an exact match is not found for the domain portion of a subscriber's username, subdomains of the domain name are matched. For example, if the domain portion of a subscriber's user name is abc.xyz.com and you use the domain command **domain** **xyz.com* it matches. But if you do not use the wildcard (**domain** *xyz.com*) it does not match.



Important The domain alias specified must not conflict with the name of any existing context or domain names.

default subscriber *subscriber_template_name*

Specifies the name of the subscriber template to apply to subscribers using this domain alias.

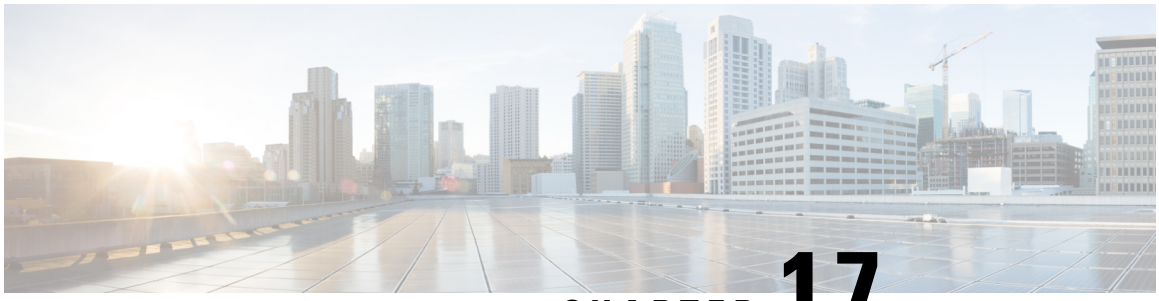
subscriber_template_name must be an alphanumeric string of 1 through 127 characters. If this keyword is not specified the default subscriber configuration in the current context is used.

Usage Guidelines

Use this command to configure a domain alias when a single context may be used to support multiple domains via aliasing.

Example

```
domain sampleDomain.net
no domain sampleDomain.net
```



CHAPTER 17

Context Configuration Mode Commands E-H

Command Modes

This section includes the commands **edr-module active-charging-service** through **hss-peer-service**.

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

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

- eap-profile, on page 412
- edr-module active-charging-service, on page 413
- egtp-service, on page 414
- end, on page 416
- epdg-service, on page 416
- event-report-conn, on page 417
- event-notif-endpoint, on page 418
- exit, on page 419
- external-inline-server, on page 420
- fa-service, on page 420
- firewall max-associations, on page 421
- fng-service, on page 421
- ggsn-service, on page 422
- gprs-service, on page 423
- gs-service, on page 425
- gtpc high-throughput-sub , on page 426
- gtpc overload-protection egress, on page 427
- gtpc overload-protection ingress, on page 428
- gtpc peer-salvation , on page 432
- gtpc-system-param-poll interval, on page 434
- gtpp algorithm, on page 435
- gtpp attribute, on page 436

- gtpp charging-agent, on page 447
- gtpp data-record-format-version, on page 448
- gtpp data-request sequence-numbers, on page 449
- gtpp dead-server suppress-cdrs, on page 450
- gtpp deadtime, on page 451
- gtpp detect-dead-server, on page 452
- gtpp dictionary, on page 453
- gtpp duplicate-hold-time, on page 456
- gtpp echo-interval, on page 457
- gtpp egcdr, on page 458
- gtpp error-response, on page 462
- gtpp group, on page 462
- gtpp max-cdrs, on page 464
- sgtpp max-pdu-size, on page 465
- gtpp max-retries, on page 466
- gtpp node-id, on page 467
- gtpp redirection-allowed, on page 468
- gtpp redirection-disallowed, on page 469
- gtpp server, on page 469
- gtpp source-port-validation, on page 471
- gtpp storage-server, on page 472
- gtpp storage-server local file, on page 473
- gtpp storage-server max-retries, on page 477
- gtpp storage-server mode, on page 477
- gtpp storage-server timeout, on page 479
- gtpp suppress-cdrs zero-volume, on page 479
- gtpp suppress-cdrs zero-volume-and-duration, on page 481
- gtpp timeout, on page 482
- gtpp trigger, on page 482
- gtpp transport-layer, on page 483
- gtpu-service, on page 484
- gtpu peer statistics threshold, on page 485
- ha-service, on page 486
- hexdump-module, on page 487
- hnbgw-service, on page 488
- hsgw-service, on page 489
- hss-peer-service, on page 490

eap-profile

Creates a new, or specifies an existing, Extensible Authentication Protocol (EAP) profile and enters the EAP Configuration Mode.

Product

ASN-GW

ePDG

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] eap-profile *name*

no

Removes the specified EAP profile.

name

Specifies the name of a new or existing EAP profile as an alphanumeric string of 1 through 256 characters.

Usage Guidelines

Use this command to create a new or enter an existing EAP profile.

Entering this command results in the following prompt:

```
[context_name]hostname(config-ctx-eap-profile)#
```

EAP Configuration Mode commands are defined in the *EAP Configuration Mode Commands* chapter.

Example

The following command configures an EAP profile called *eap1* and enters the EAP Configuration Mode:

```
eap-profile eap1
```

edr-module active-charging-service

Enables the creation, configuration, or deletion of the Event Data Record (EDR) module for this context. In releases prior to 15.0, the SGSN re-used the existing 'EDR" module for generating event logs which is primarily used for charging records. But from release 15.0 onwards, the session-event module is used by SGSN for event logging. For more information see the **session-event-module** command.

Product

ACS

GGSN

HA

LNS

PDSN

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] edr-module active-charging-service [ charging | reporting ]`

no

Removes the EDR module configuration for the current context.

charging

Enables the EDR module for charging EDRs that are stored in the /records/edr directory.

reporting

Enables the EDR module for reporting EDRs that are stored in the /records/redr directory.

Usage Guidelines

Use this command to create the EDR module for the context, and configure the EDR module for active charging service records. You must be in a non-local context when specifying this command, and you must use the same context when specifying the UDR module command.

If this CLI command is configured without the **charging** or **reporting** keywords, by default the EDR module is enabled for charging EDRs.

On entering the command with the **charging**keyword or without any keywords, the CLI prompt changes to:

[*context_name*]*hostname*(config-edr)#

On entering the command with the **reporting**keyword, the CLI prompt changes to:

[*context_name*]*hostname*(config-redr)#

Example

The following command creates the EDR module for the context for charging EDRs, and enters the EDR Module Configuration Mode:

`edr-module active-charging-service`

egtp-service

Creates an eGTP service or specifies an existing eGTP service and enters the eGTP Service Configuration Mode for the current context.

Product

MME

P-GW

SAEGW

SGSN

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] egtp-service` *`service_name`* **`[ -noconfirm ]`**

egtp-service *service_name*

Specifies the name of the eGTP service as an alphanumeric string of 1 through 63 characters. If *service_name* does not refer to an existing service, the new service is created if resources allow.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

no egtp-service *service_name*

Removes the specified eGTP service from the context.

Usage Guidelines

Enter the eGTP Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-egtp-service)#
```

eGTP Service Configuration Mode commands are defined in the *eGTP Service Configuration Mode Commands* chapter.

Use this command when configuring the following GTP SAE components: MME, P-GW, and S-GW. Also use this command when configuring an S4-SGSN. Once the eGTP service has been created on the S4-SGSN, the eGTP service must be configured using the **gtpc**, **validation-mode** and **interface-type** commands in *eGTP*

Service Configuration Mode. Once the service is created and configured, it then must be associated with the 2G and/or 3G services configured on the S4-SGSN using the**associate** command in *Call Control Profile Configuration Mode*.



Important If you modify the **interface-type** command, the parent service (service within which the eGTP/GTP-U service is configured) will automatically restart. Service restart results in dropping of active calls associated with the parent service.

Example

The following command enters the existing eGTP Service Configuration Mode (or creates it if it does not already exist) for the service named *egtp-service1*:

```
egtp-service egtp-service1
```

The following command will remove *egtp-service1* from the system:

```
no egtp-service egtp-service1
```

end

Exits the 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.

epdg-service

Creates Evolved Packet Data GateWay service and enters EPDG service configuration mode.

Product ACS

ePDG

GGSN

HA

LNS

PDSN

SGSN

Privilege Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] epdg-service` *`name`* **`[ -noconfirm ]`**

no

Indicates the evolved packet data gateway service specified is to be removed.

name

Specifies the name of the ePDG service to configure as an alphanumeric string of 1 through 63 characters. If *name* does not refer to an existing service, the new service is created if resources allow.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Enter the ePDG Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

Example

The following command will enter the ePDG Service Configuration Mode creating the service *sampleService*, if necessary.

```
epdg-service sampleService
```

The following command will remove *sampleService* as being a defined ePDG service.

```
no epdg-service sampleService
```

event-report-conn

Configures a GMPC Event Report Connection.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] event-report-conn` *event_report_conn_name* **`[ -noconfirm ]`**

no

Indicates the event report connection name that is specified is to be removed.

name

Specifies the name of the event-report-conn to configure as an alphanumeric string of 1 to 32 characters. If *event-report-conn name* does not refer to an existing configuration, then new configuration is created if resources allow.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines

Enter the event-report-conn name for a newly defined configured connection. This command is also used to remove an existing connection.

Example

The following command will create the event-report-conn name Configuration Mode .

```
event-report-conn name Config
```

The following command will remove *event-report-conn name Config* as being a defined event-report-conn service.

```
no event-report-conn name Config
```

event-notif-endpoint

Enables creation, configuration or deletion of an Event Notification collection server endpoint.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] event-notif-endpoint` *en_node_name* **`[ -noconfirm ]`**

no

Removes the specified Event Notification collection server endpoint.

en_node_name

Specifies name of the Event Notification collection server endpoint as an alphanumeric string of 1 through 31 characters.

If the named endpoint does not exist, it is created, and the CLI mode changes to the Event Notification Interface Endpoint Configuration Mode wherein the endpoint can be configured.

If the named endpoint already exists, the CLI mode changes to the Event Notification Interface Endpoint Configuration Mode wherein the endpoint can be reconfigured.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to create/configure/delete an Event Notification collection server endpoint.

Only 1 Event Notification interface across a chassis can be configured on a system.

Entering this command results in the following prompt:

```
[context_name]hostname(config-ntfyintf-endpoint)#
```

The commands configured in this mode are defined in the *Event Notification Interface Endpoint Configuration Mode Commands* chapter of *Command Line Interface Reference*.



Caution This is a critical configuration. The PCC Event notification can not be collected on a server without this configuration. Any change to this configuration would lead to the loss of event notifications from PCC service on IPCF node.

Example

The following command creates an Event Notification Interface Endpoint named *event_intfc_3*:

```
event-notif-endpoint event_intfc_3
```

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.

fa-service

Creates or deletes a foreign agent (FA) service or specifies an existing FA service for which to enter the FA Service Configuration Mode for the current context.

Product

ASN-GW

PDSN

FA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] fa-service` *`name`* **`[ -noconfirm ]`**

no

Indicates the foreign agent service specified is to be removed.

name

Specifies the name of the FA service to configure as an alphanumeric string of 1 through 63 characters. If *name* does not refer to an existing service, the new service is created if resources allow.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Enter the FA Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Example

The following command will enter the FA Service Configuration Mode creating the service *sampleService*, if necessary.

```
fa-service sampleService
```

The following command will remove *sampleService* as being a defined FA service.

```
no fa-service sampleService
```

firewall max-associations

This command is obsolete.

fng-service

Creates a new, or specifies an existing FNG service and enters the FNG Service Configuration Mode. A maximum of 16 FNG services can be created. This limit applies per ASR 5000 chassis and per context.

Product FNG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
fng-service name [ -noconfirm ]
no fng-service name
```

fng-service *name*

Specifies the name of a new or existing FNG service as an alphanumeric string of 1 through 63 characters that must be unique across all FNG services within the same context and across all contexts.

Important Service names must be unique across all contexts within a chassis.

no fng-service *name*

Deletes the specified FNG service.

Usage Guidelines

Use this command in Context Configuration Mode to create a new FNG service or modify an existing one. Executing this command enters the FNG Service Configuration Mode.

Example

The following command configures an FNG service named *fng1* and enters the FNG Service Configuration Mode:

```
fng-service fmg1
```

ggsn-service

Creates or deletes a Gateway GPRS Support Node (GGSN) service and enters the GGSN Service Configuration Mode within the current context to configure it.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

ggsn-service *svc_name* **[-noconfirm] handover-immediate-flush-enabled**
no ggsn-service *svc_name*

no

Deletes a preciously configured GGSN service.

svc_name

Specifies the name of the GGSN service to create/configure as an alphanumeric string of 1 through 63 characters that is case sensitive.



Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

handover-immediate-flush-enabled

Configures the GGSN service associated to saegw-service with immediate flush of handover information from sessmgr to demux (egtpinmgr). The **handover-immediate-flush-enabled** CLI should be configured only if the pgw-service is associated with ggsn-service, which is associated with saegw-service.



Note By default, this CLI is disabled.

Usage Guidelines

Services are configured within a context and enable certain functionality. This command creates and allows the configuration of services enabling the system to function as a GGSN in a GPRS or UMTS network. This command is also used to remove previously configured GGSN services.

A maximum of 256 services (regardless of type) can be configured per system.



Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Example

The following command creates a GGSN service named *ggsn1*:

```
ggsn-service ggsn1
```

The following command controls the immediate flush functionality of the aggregation list from sessmgr to demux for 3g to 4g handover scenario.

```
qvpc-si(config-ggsn-service)# handover-immediate-flush-enabled
```

```
local]laas-setup(config)# context EPC2
[EPC2]laas-setup(config-ctx)# ggsn-service GGSN
[EPC2]laas-setup(config-ggsn-service)#
accounting
associate
authorize-with-hss
bind
cc
.......
gx-li
handover-immediate-flush-enabled
internal-qos
.....

[EPC2]laas-setup(config-ggsn-service)# handover-immediate-flush-enabled
[EPC2]laas-setup(config-ggsn-service)#
```

gprs-service

Creates a GPRS service instance and enters the GPRS Service Configuration Mode. This mode configures all of the parameters specific to the operation of an SGSN in a GPRS network.

Important For details about the commands and parameters for this mode, check the *GPRS Service Configuration Mode* chapter.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gprs-service *srvc_name* **[-noconfirm]**
no gprs-service *srvc_name*

no

Removes the configuration for the specified IGPRS service from the configuration for the current context.

srvc_name

Specifies the name of the GPRS service as a unique alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to create or remove a GPRS service. Entering this command will move the system to the GPRS Service Configuration Mode and change the prompt to:

```
[context_name]hostname(config-gprs-service)#
```

Example

The following command creates an GPRS service named *gprs1*:

```
gprs-service gprs1
```

The following command removes the GPRS service named *gprs1*:

```
no gprs-service gprs1
```

gs-service

Creates a Gs service instance and enters the Gs Service Configuration Mode. This mode configures the parameters specific to the Gs interface between the SGSN and the MSC/VLR.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gs-service svc_name [ -noconfirm ]
no gs-service svc_name
```

no

Remove the configured Gs service from the current context.

svc_name

Specifies the Gs service as a unique alphanumeric string of 1 through 63 characters.



Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to create, edit, or remove a Gs service.

A maximum of 32 Gs service can be configured in one context/system. This limit is subject to maximum of 256 services (regardless of type) can be configured per system.



Important For details about the commands and parameters for this mode, refer *Gs Service Configuration Mode* chapter.

Example

The following command creates an Gs service named *gs1*:

```
gs-service gs1
```

The following command removes the Gs service named *gs1*:

```
no gs-service gs1
```

gtpc high-throughput-sub

This command enables the GTPC configuration for high throughput subscribers.

Product

P-GW

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] gtpc high-throughput-sub dcnr-based sessmgr-select round-robin`

no

Disables the GTPC configuration for high throughput subscribers.

dcnr-based

Applies this configuration to all Create Session Requests that have a DCNR flag.

sessmgr-select

Specifies the method to select a session manager for a DCNR session.

round-robin

Selects the session managers for a high throughput session using the round-robin method.

Usage Guidelines

Use this command to enable the GTPC configuration for high throughput subscribers.

The gateway – S-GW, SAEGW or P-GW, classifies a session as a high throughput session based on a DCNR flag present in the IE: FLAGS FOR USER PLANE FUNCTION (UPF) SELECTION INDICATION, in the Create Session Request. This DCNR flag is check-pointed and recovered by the gateway.

A high throughput session is placed on a session manager that has no other high throughput session. If all session manager are handling a high throughput session then these sessions are allocated using the Round-Robbin method.

gtpc overload-protection egress

Configures the overload protection of GGSN/P-GW by throttling outgoing GTPv1 and GTPv2 control messages over Gn/Gp(GTPv1) or S5/S8 (GTPv2) interface using rate-limiting-function (RLF) template for services configured in a context.

Product

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpc overload-protection egress [rlf-template *rlf_template_name* **| throttling-override-policy** *throttling_override_policy_name*
[no] gtpc overload-protection egress

no

Disables the GTP Outgoing Control Message Throttling for GGSN/P-GW services in this context.

rlf-template ***rlf_template_name***

Associates a pre-configured Rate-Limiting-Function (RLF) template for throttling the GTP outgoing control messages for the GGSN/P-GW services in this context. This is a mandatory parameter to enable throttling.

Important Use the **rlf-template** command in Global Configuration mode to configure an RLF template.

throttling-override-policy*throttling_override_policy_name*

Associates a pre-configured GTP-C Throttling Override Policy to selectively bypass throttling for a specific message type. This is a mandatory parameter to bypass enabled throttling.

Important Use the **throttling-override-policy** command in Global Configuration mode to configure a GTP-C Throttling Override Policy.

Usage Guidelines

Use this command to enable the GTP Outgoing Control Message Throttling for GGSN/P-GW services configured in the same context. The RLF template associated with this command controls the throttling parameters.

Associating a GTP-C Throttling Override Policy determines which message types can bypass the rate limiting function.

Example

The following command enables the outgoing GTP control messages in a context using rlf-template *gtpc_1*:

```
gtpc overload-protection egress rlf-template gtpc_1
```

gtpc overload-protection ingress

Configures the over-load protection of GGSN/PGW/SAEGW/S-GW by throttling incoming new call GTPv1 and GTPv2 control messages over Gn/Gp (GGSN GTPv1) or S5/S8 (PGW GTPv2) or S4/S11 (S-GW GTPv2) interface with other parameters for GGSN/PGW/S-GW/SAEGW services configured in the same context.

Product

GGSN

P-GW

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpc overload-protection ingress { msg-rate msg_rate } delay-tolerance
dur ] [ queue-size size ] [ exclude { sgw-interface [ priority-message ] }
 | { priority-message [ sgw-interface ] } ]
[default] gtpc overload-protection ingress
```

ingress

Configures throttling parameters for incoming new call GTPC messages for GGSN, PGW, SGW, and SAEGW services in this context.

default

Resets the GTP incoming control message throttling parameters of *msg-rate*, *delay-tolerance*, and *queue-size* to their default values for GGSN, P-GW, SAEGW, and S-GW services.

msg-rate *msg_rate*

Defines the number of GTP incoming messages that can be processed per second.

msg_rate is an integer with a minimum value of 100 and maximum value that is dependent on the chassis or card used as shown in the following table.

Value	Chassis/Card

2000	SSI SMALL
3000	SSI MEDIUM
20000	SSI LARGE
12000	SCALE MEDIUM
20000	SCALE LARGE
12000	ASR5000 PSC
20000	ASR5000 PSC2
20000	ASR5000 PSC3
20000	ASR5000 PPC
20000	ASR5500 DPC
20000	ASR5500 DPC2
3000	SSI FORGE

The default value of *msg_rate* is 0, which implies that it is disabled.

delay-tolerance *dur*

Defines the maximum number of seconds a incoming GTP message can be queued before it is processed. After exceeding this, the message is dropped.

dur is an integer between 1 through 10. The default value is 5.

queue-size *size*

Defines the maximum size of the queue to be maintained for incoming GTPC messages. If the queue exceeds the defined size *size*, any new incoming messages will be dropped.

size is an integer between 100 through 10000. The default value is 10000.

exclude

Excludes the specified interface.

sgw-interface resets the incoming throttling parameters "msg-rate" and "queue-size" to their default values for GTPC incoming new call messages at SGW ingress interface (S4, S11). “delay-tolerance” continues to be applied as the configured value for the GTPC messages on the SGW interface (S4, S11). The message queue size considered for Congestion Control feature for PGW/SGW/GGSN is reset to default value of 10K, if this keyword is configured.

priority-message enables bypassing of demux incoming throttling for incoming GTPC request messages that have the Message Priority (MP) flag set as “1” and Message Priority value set as “0” in the GTP header.

Note The priority-message" keyword is applicable only for the P-GW.

Usage Guidelines

Use this command to enable the GTP incoming control message throttling for GGSN/PGW/SAEGW/S-GW services configured in the same context.

New keywords **exclude** and **sgw-interface** have been added to the CLI command **gtpc overload-protection ingress** to disable throttling exclusively for S-GW ingress GTPC interfaces (S4, S11).

1. When **gtpc overload-protection ingress** CLI is configured without the **exclude sgw-interface** option, the configured values of msg rate, delay tolerance and queue-size are enabled on new call messages at S-GW ingress interface (S4, S11).
2. When **exclude sgw-interface**is configured for the GTPC messages on the S-GW interface (S4, S11), below are the values taken by different parameters:
3. If **exclude sgw-interface**is configured, GTPC ingress messages throttling is applied (with the configured values of **msg rate**, **delay tolerance** and **queue-size**) to the external interfaces of P-GW and GGSN such as S5, S8, S2b, Gn/Gp, only to the new call create messages incoming from outside of the ASR5k. GTPC ingress message throttling is also applied (with the configured values of *msg-rate*, *delay-tolerance*, and *queue-size*) to the internal interfaces of the SAEGW such as the S5/S8 interfaces, only to the new call create messages received at the local P-GW of the SAEGW.
4. If ingress throttling is configured using **gtpc overload-protection ingress** with **exclude sgw-interface**, then for congestion control calculation for P-GW/S-GW/GGSN/SAEGW demuxmgr based on message queue size, the default queue size value of 10K is used.

   If ingress throttling is configured using **gtpc overload-protection ingress** without **exclude sgw-interface**, then for congestion control calculation for P-GW/S-GW/GGSN/SAEGW demuxmgr based on message queue size, the configured queue-size value will be used.

   The following table describes various scenarios of the configuration:

GTPC Incoming Throttling Queue-size Configuration (100..10K)	If "exclude sgw-interface" configured	Queue-size used for GTPC Incoming Throttling for P-GW/GGSN	Queue-size used for GTPC Incoming Throttling for S-GW	Queue-size considered for Congestion Control Threshold for P-GW/GGSN/S-GW	Behaviour Change
No configuration/Default configuration	No	10K (Default)	10K (Default)	Configured congestion threshold * 10K (Default)	No
No configuration/Default configuration	Yes	10K (Default)	10K (Default)	Configured congestion threshold * 10K (Default)	No
5K (or any configured value from 100..10K)	No	5k (or the configured value)	5k (or the configured value)	Configured congestion threshold * 5k (or the configured value)	No

GTPC Incoming Throttling Queue-size Configuration (100..10K)	If "exclude sgw-interface" configured	Queue-size used for GTPC Incoming Throttling for P-GW/GGSN	Queue-size used for GTPC Incoming Throttling for S-GW	Queue-size considered for Congestion Control Threshold for P-GW/GGSN/S-GW	Behaviour Change
5k (or Any configured value from 100..10K)	Yes	5k (or the configured value)	10k (because "exclude sgw-interface" is configured)	Configured congestion threshold * 10k (this is the behaviour change for congestion control, if "exclude sgw-interface" is configured)	Yes

In Release 21.4, the **priority-message** keyword is added to the existing gtpc overload-protection ingress CLI to enable bypassing of demux incoming throttling for incoming GTPC request messages where the “MP” flag is set as 1 and Message Priority value set as 0 in the GTP header.

This keyword is disabled by default.

If the new **exclude priority-message** CLI keyword is configured, it applies the following behaviour to bypass incoming throttling for high priority messages:

- High priority messages, the default configuration for “msg-rate” and “queue-size” of demux are applicable (even if they are configured with a different value). The default value for “msg-rate” is 0, which implies that High Priority setting is disabled. The default value for “queue-size” is 10000.
- There is no throttling applied due to the “delay-tolerance” parameter for High Priority messages.
- Also High Priority Create Session Request (CSReq) messages are prioritized over other messages. However, High Priority CSReq messages are processed in sequence.
- When a High Priority message is received and the queue is overloaded then a Low Priority message is discarded from the queue to accommodate the High Priority message.
- In a rare scenario where all the messages in the queue are High Priority and the queue is overloaded, then the new High Priority message may get dropped.
- If ingress throttling is configured using "gtpc overload-protection ingress" with "exclude priority-message" option, then for congestion control calculation for P-GW, S-GW, GGSN, and SAEGW demux manager based on the demux message queue size, the default queue size value of 10,000 is used. (This is the same behaviour if **exclude sgw-interface** is selected.)
- If ingress throttling is configured using "gtpc overload-protection ingress" without the "exclude" option, then for congestion control calculation for P-GW, S-GW, GGSN, and SAEGW demux manager based on demux message queue size, the configured queue-size value is used.

  The following table describes the behavior when the **exclude priority-message** is configured:

GTPC Incoming Throttling Demux Queue-size Configuration (100 to 10000)	Is "exclude priority-message" configured	Demux Queue-size used for GTPC Incoming Throttling for S-GW/GGSN/ "Low Priority" P-GW messages	Demux Queue-size used for "High Priority messages" P-GW messages	Queue-size considered for Congestion Control Threshold for P-GW/GGSN/S-GW
No configuration/Default configuration	No	10000 (default)	10000 (default)	Configured_congestion_threshold * 10000 (default)
No configuration/Default configuration	Yes	10000 (default)	10000 (default)	Configured_congestion_threshold * 10000 (default)
5000 (or any configured value from 100 to10000)	No	5000 (or the configured value)	5000 (or the configured value)	Configured_congestion_threshold * 5000 (default)
5000 (or any configured value from 100 to10000)	Yes	5000 (or the configured value)	10000 (because "exclude priority-message" is configured)	Configured_congestion_threshold * 10000 (this is the behavior change for congestion control, if "exclude priority-message" is configured)

Example

The following command enables the throttling of incoming new call GTP control messages in a context using message rate *1000* per second with message queue size *10000* and delay tolerance of *1* second:

```
gtpc overload-protection ingress msg-rate 1000 delay-tolerance 1 queue-size
 10000
```

Example

The following command bypasses incoming throttling for high priority messages.

```
gtpc overload-protection ingress msg-rate 100 exclude priority-message
```

gtpc peer-salvation

Configures peer salvation for inactive GTPv2 peers for EGTP services in this context.

Product P-GW

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] gtpc peer-salvation { min-peers *value* **| timeout** *value* **}**

no

Disables peer salvation for inactive GTPv2 peers for EGTP services in the context.

min-peers *value*

Configures the minimum number of accumulated GTPv2 peers across all EGTP services to start salvaging the inactive peers. The value ranges from 2000 to 12000.

timeout *value*

Configures the peer salvation timeout. The peer that is inactive for salvation time is salvaged, in hours. The value ranges from 1 to 48 hours.

Usage Guidelines

Use this command to enable peer salvation for inactive GTPv2 peers for EGTP services in this context. The **peer-salvation** keyword is introduced in the Context Configuration Mode. Minimum peers and timeout values can be provided with this CLI, which will be per egtpmgr (separate for egtpinmgr and egtpegmgr) and across all the egtp-services configured in that context.

This command is disabled by default.

Important

- When the **peer-salvation** keyword is enabled at the context level, but not enabled at egtp-service level, then peer salvation does not occur.
- All the information (peer statistics/recovery counter and so on) of the particular peer is lost after it is salvaged.
- The context level configuration is applied to egtpinmgr and egtpegmgr separately.
- The **min-peers** value should be applied judiciously to ensure that the Session Manager in a fully loaded chassis does not go into warn/over state with many peer records. If the Session Manager goes into a warn/over state, then it is recommended to configure a lesser value for min-peers to ensure that the peers are salvaged.
- **min-peers** configuration is not considered during a new peer creation.
- Only peers with zero number of sessions are salvaged for the configured timeout value. Non-zero number of sessions is not salvaged even if there are few.

Example

The following command specifies the number of peers to be salvaged and the timeout value.

```
gtpc peer-salvation min-peers 4000 timeout 5
```

gtpc-system-param-poll interval

Sets the time period over which to monitor the chassis level CPU, Memory and Session count information from the resource manager.

Product

P-GW

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpc-system-param-poll interval seconds
default gtpc-system-param-poll interval
```

default

Returns the GTP-C system parameter polling interval to the default setting of 30 seconds.

gtpc-system-param-poll interval *seconds*

Sets the time period over which to monitor the chassis level CPU, Memory and Session count information from the resource manager.

Valid entries are from 15 to 300 seconds.

The default setting is 30 seconds.

⚠

Caution Setting the time interval to a low value may impact system performance.

Usage Guidelines

In capacity testing and also in customer deployments it was observed that the chassis load factor for the R12 Load and Overload Support feature was providing incorrect values even when the sessmgr card CPU utilization was high. The root cause is that when the load factor was calculated by taking an average of CPU utilization of sessmgr and demux cards, the demux card CPU utilization never increased more than the sessmgr card CPU utilization. As a result, the system did not go into the overload state even when the sessmgr card CPU utilization was high.

This feature has been enhanced to calculate the load factor based on the higher value of similar types of cards for CPU load and memory. If the demux card's CPU utilization value is higher than the sessmgr card's CPU utilization value, then the demux card CPU utilization value is used for the load factor calculation.

This CLI command is introduced to configure different polling intervals for the resource manager so that the demuxmgr can calculate the load factor based on different system requirements.

Example

The following command sets the GTP-C system parameter polling interval to 40 seconds:

```
gtpc-system-param-poll interval 40
```

gtpp algorithm

Configures GTPP routing algorithms for the current context. This command is deprecated but available for backward compatibility.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp algorithm { first-server | round-robin | first-n *count* **}**

first-server

Specifies that accounting data is sent to the first available charging gateway function (CGF) based upon the relative priority of each configured CGF. Default: Enabled

round-robin

Specifies that accounting data is transmitted in a circular queue fashion such that data is sent to the highest priority CGF first, then to the next available CGF of the highest priority, and so on. Ultimately, the queue returns to the CGF with the highest configured priority. Default: Disabled

first-n *count*

Specifies that the AGW must send accounting data to *count* (more than one) CGFs based on their priority. Response from any one of the *count* CGFs would suffice to proceed with the call. The full set of accounting data is sent to each of the *count* CGFs.

count is the number of CGFs to which accounting data will be sent, and must be an integer from 2 through 65535. Default: 1 (Disabled)

Usage Guidelines Use this command to control how G-CDR/P-CDR accounting data is routed among the configured CGFs.

Example

The following command configures the system to use the round-robin algorithm when transmitting G-CDR/P-CDR accounting data:

```
gtpp algorithm round-robin
```

gtpp attribute

Allows the specification of the optional attributes to be present in the Call Detail Records (CDRs) that the GPRS/PDN/UMTS access gateway generates. It also defines that how the information is presented in CDRs by encoding the attribute field values.

Product

GGSN

SGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpp attribute { apn-ambr [ include-for-all-bearers |
include-for-default-bearer | include-for-non-gbr-bearers ] | apn-ni |
apn-selection-mode | charging-characteristic-selection-mode | camel-info
 | cell-plmn-id |  { ciot-cp-optind | ciot-unipdu-cponly } | diagnostics
 [ abnormal-release-cause ] | direct-tunnel | duration-ms | dynamic-flag
 | dynamic-flag-extension | furnish-charging-information | imei |
imsi-unauthenticated-flag | lapi last-ms-timezone | last-uli |
local-record-sequence-number | losdv | ms-timezone | msisdn | node-id |
node-id-suffix STRING | pdn-connection-id | pdp-address | pdp-type |
pgw-ipv6-addr | pgw-plmn-id | plmn-id | qos max-length | rat |
recordextension | record-extensions rat | record-type { sgsnpdprecord |
sgwrecord } | served-mnai | served-pdp-pdn-address-extension |
served-pdp-pdn-address-prefix-length | sgsn-change |  sms {
destination-number | recording-entity | service-centre } | sgw-ipv6-addr
 | sna-ipv6-addr | sponsor-id | start-time | stop-time | twanuli | uli |
 user-csg-information } +
default gtpp attribute { apn-ambr [ include-for-all-bearers |
```

```
include-for-default-bearer | include-for-non-gbr-bearers ] | apn-ni |
apn-selection-mode | charging-characteristic-selection-mode | camel-info
 | cell-plmn-id |  { ciot-cp-optind | ciot-unipdu-cponly } | diagnostics
 [ abnormal-release-cause ] | direct-tunnel | duration-ms | dynamic-flag
 | dynamic-flag-extension | furnish-charging-information | imei |
imsi-unauthenticated-flag | lapi last-ms-timezone | last-uli |
local-record-sequence-number | losdv | ms-timezone | msisdn | node-id |
node-id-suffix STRING | pdn-connection-id | pdp-address | pdp-type |
pgw-ipv6-addr | pgw-plmn-id | plmn-id | qos max-length | rat |
recordextension | record-extensions rat | record-type { sgsnpdprecord |
sgwrecord } | served-mnai | served-pdp-pdn-address-extension |
served-pdp-pdn-address-prefix-length | sgsn-change |  sms {
destination-number | recording-entity | service-centre } | sgw-ipv6-addr
 | sna-ipv6-addr | sponsor-id | start-time | stop-time | twanuli | uli |
 user-csg-information } +
no gtpp attribute { apn-ambr [ include-for-all-bearers |
include-for-default-bearer | include-for-non-gbr-bearers ] | apn-ni |
apn-selection-mode | charging-characteristic-selection-mode | camel-info
 | cell-plmn-id |  { ciot-cp-optind | ciot-unipdu-cponly } | diagnostics
 [ abnormal-release-cause ] | direct-tunnel | duration-ms | dynamic-flag
 | dynamic-flag-extension | furnish-charging-information | imei |
imsi-unauthenticated-flag | lapi last-ms-timezone | last-uli |
local-record-sequence-number | losdv | ms-timezone | msisdn | node-id |
node-id-suffix STRING | pdn-connection-id | pdp-address | pdp-type |
pgw-ipv6-addr | pgw-plmn-id | plmn-id | qos max-length | rat |
recordextension | record-extensions rat | record-type { sgsnpdprecord |
sgwrecord } | served-mnai | served-pdp-pdn-address-extension |
served-pdp-pdn-address-prefix-length | sgsn-change |  sms {
destination-number | recording-entity | service-centre } | sgw-ipv6-addr
 | sna-ipv6-addr | sponsor-id | start-time | stop-time | twanuli | uli |
 user-csg-information } +
```

default

Sets the default GTPP attributes in the generated CDRs. It also sets the default presentation of attribute values in generated CDRs.

no

Removes the configured GTPP attributes from the CDRs.

apn-ambr [include-for-all-bearers | include-for-default-bearer | include-for-non-gbr-bearers]

Default: Disabled

This keyword controls the inclusion of the optional field "apn-ambr" in the PGW-CDRs in the custom24 GTPP dictionary.



Important This keyword option will be available only if a valid license is installed. For more information, contact your Cisco account representative.

The APN Aggregate Maximum Bit Rate (AMBR) is a subscription parameter stored per APN. It limits the aggregate bit rate that can be expected to be provided across all non-GBR bearers and across all PDN connections of the same APN. Each of these non-GBR bearers potentially utilize the entire APN AMBR, e.g. when the other non-GBR bearers do not carry any traffic. The APN AMBR is present as part of QoS information.

In 15.0 and later releases, this CLI command should be configured along with the following additional options to support APN-AMBR reporting in SGW-CDRs in all GTPP dictionaries.

- **include-for-all-bearers**: Includes the APN-AMBR information in SGW-CDRs for all bearers (GBR and NON-GBR)
- **include-for-default-bearer**: Includes APN-AMBR information in SGW-CDRs only for default bearer.
- **include-for-non-gbr-bearers**: Includes APN-AMBR information for non-gbr-bearers.

This feature is required to enable post-processing of CDRs to verify MVNO subscribers actual QoS against invoicing systems.



Important This CLI command and the associated options are not available for products other than S-GW and P-GW. The option "**non-gbr-bearers-only**" is available in S-GW and P-GW but the other options are available in S-GW only.

In the P-GW implementation, if the CLI command "**gtpp attribute apn-ambr**" is configured, it will be treated as "**gtpp attribute apn-ambr non-gbr-bearers-only**". In case of S-GW/P-GW combo if any of the options is configured, it will be considered that the attribute is available.

apn-ni

Default: Enabled

This keyword controls the inclusion of the optional field "APN" in the x-CDRs.

apn-selection-mode

Default: Enabled

This keyword controls the inclusion of the optional field "APN Selection Mode" in the x-CDRs.

camel-info

SGSN only

Enter this keyword to include CAMEL-specific fields in SGSN CDRs. Default: Disabled

cell-plmn-id

SGSN only

Enter this keyword to enable the system to include the Cell PLMN ID field in the M-CDR. Default: Disabled

charging-characteristic-selection-mode

Default: Enabled

This keyword controls the inclusion of the optional field "Charging Characteristic Selection Mode" in the x-CDRs.

ciot-cp-optind

Includes optional field "CP CIoT EPS optimisation indicator" in the CDR.

ciot-unipdu-cponly

Includes optional field "UNI PDU CP Only Flag" in the CDR.

diagnostics [abnormal-release-cause]

Default: Disabled

Enables the system to include the Diagnostic field in the CDR that is created when PDP contexts are released. The field will include one of the following values:

- **26** - For GGSN: if the GGSN sends "delete PDP context request" for any other reason (e.g., the operator types "clear subscribers" on the GGSN). For SGSN: The SGSN includes this cause code in the S-CDR to indicate that a secondary PDP context activation request or a PDP context modification request has been rejected due to insufficient resources.
- **36** - For GGSN: this cause code is sent in the G-CDR to indicate the PDP context has been deactivated in the GGSN due to the SGSN having sent a "delete PDP context request" to the GGSN. For SGSN, this cause code is used to indicate a regular MS or network-initiated PDP context deactivation.
- **37** - when the network initiates a QoS modification, the SGSN sends in the S-CDR to indicate that the MS initiation deactivate request message has been rejected with QoS not accepted as the cause.
- **38** - if the GGSN sends "delete PDP context request" due to GTP-C/GTP-U echo timeout with SGSN. If the SGSN sends this cause code, it indicates PDP context has been deactivated due to path failure, specifically GTP-C/GTP-U echo timeout.
- **39** - SGSN only - this code indicates the network (GGSN) has requested a PDP context reactivation after a GGSN restart.
- **40** - if the GGSN sends "delete PDP context request" due to receiving a RADIUS Disconnect-Request message.

abnormal-release-cause: This keyword controls the inclusion of abnormal bearer termination information in diagnostics field of SGW-CDR. Note that the CLI command "**gtpp attribute diagnostics**" will disable **abnormal-release-cause** and enable the **diagnostics** field. The **no gtpp attribute diagnostics** command will disable both **abnormal-release-cause** and **diagnostics** field.



Important The Abnormal Bearer Termination feature is currently applicable only to custom34 and custom35 GTPP dictionaries. That is, the bearer termination cause is populated in SGW-CDR for custom34 and custom35 dictionaries, and PGW-CDRs for custom35 GTPP dictionary when the cause for record closing is "Abnormal Release".

direct-tunnel

Default: Disabled

Includes the Direct Tunnel field in PGW-CDR/eG-CDRs.

This keyword is applicable for GGSN, P-GW and S-GW only.

duration-ms

Specifies that the information contained in the mandatory Duration field be reported in milliseconds instead of seconds (as the standards require). Default: Disabled

dynamic-flag

Default: Enabled

This keyword controls the inclusion of the optional field "Dynamic Flag" in the x-CDRs.

dynamic-flag-extension

Default: Enabled

This keyword controls the inclusion of the optional field "Dynamic Address Flag Extension" in the x-CDRs.

This field is seen in the CDR when the IPv4 address is dynamically assigned for a dual PDP context. This extension field is required in the 3GPP Release 10 compliant CDRs so that the Dual Stack Bearer support is available.

furnish-charging-information

Default: Disabled

This keyword controls the inclusion of the optional field "pSFurnishChargingInformation" in the eG-CDRs and PGW-CDRs.



Important The Furnish Charging Information (FCI) feature is applicable to all GTPP dictionaries compliant to 3GPP Rel.7 and 3GPP Rel.8 except custom43 dictionary. This keyword option will be available only if a valid license is installed. For more information, contact your Cisco account representative.

PGW-CDR and eG-CDR will contain FCI only if it is enabled at command level, i.e. using the **gtpp attribute furnish-charging-information** command in GTPP Server Group Configuration mode.

Whenever FCI changes, a new Free-Format-Data (FFD) value is either appended to existing FFD or overwritten on the existing FDD depending on Append-Free-Format-Data (AFFD) flag. CDR is not generated upon FCI change.

FCI is supported in main CDR as well as in LOSDV. Whenever a trigger (volume, time, RAT, etc.) happens current available FFD at command level is added to the main body of the CDR. The same FFD at command level is added to the main body of the next CDRs until it is not appended or overwritten by next Credit-Control-Answer message at command level.

In the case of custom43 dictionary, the FCI implementation will be as follows:

- Whenever FCI changes PGW-CDR will generate CDR i.e close old bucket and will have old FCI details in the generated CDR.
- Translation for the PS-Free-Format-Data in CDR will be conversion of hexadecimal values in ASCII format (for numbers 0 to 9) to decimal values as integers.
- PS-Append-Free-Format-Data always OVERWRITE.

imei

Default: Disabled

For SGSN: includes the IMEI value in the S-CDR.

For GGSN: includes the IMEISV value in the G-CDR.

imsi-unauthenticated-flag

Default: Enabled

This keyword controls the inclusion of the optional field "IMSI Unauthenticated Flag" in the x-CDRs.

When the served IMSI is not authenticated, this field "IMSI Unauthenticated Flag" if configured, will be present in the P-GW CDR record for custom35 dictionary. This field is added per 3GPP TS 32.298 v10.7.

lapi

Default: Disabled

Includes the Low Access Priority Indicator (LAPI) field in the CDRs. This field is required to support MTC feature.

When UE indicates low priority connection, then the "lowPriorityIndicator" attribute will be included in the CDR.

last-ms-timezone

Default: Disabled

Sets the "Last MS-Timezone" in the CDR field. This option would be disabled when the default option is used.

last-uli

Default: Disabled

Sets the "Last ULI" in the CDR field. This option would be disabled when the default option is used.

local-record-sequence-number

Default: Disabled

This keyword provides both the local record sequence number and the Node ID. In the x-CDRs, this field indicates the number of CDRs generated by the node and is unique within the session manager.

The Node ID field is included in the x-CDR for any of several reasons, such as when PDP contexts are released or if partial-CDR is generated based on configuration. The field will consist of a AAA Manager identifier automatically appended to the name of the SGSN or GGSN service.

The name of the SGSN or GGSN service may be truncated, because the maximum length of the Node ID field is 20 bytes. Since each AAA Manager generates CDRs independently, this allows the Local Record Sequence Number and Node ID fields to uniquely identify a CDR.



Important If the **gtpp single-source centralized-lrsn** is configured, the 'Node-ID' field consists of only the specified NodeID-suffix. If NodeID-suffix is not configured, GTPP group name is used. For default GTPP groups, GTPP context-name is used. If the **gtpp single-source centralized-lrsn** is not configured, then node-id format for CDRs generated by Sessmgr is as follows: <1-byte Sessmgr restartvalue><3-byte Sessmgr instance number> <node-id-suffix>. If the **gtpp single-source centralized-lrsn** is not configured, then node-id format for CDRs generated by ACSmgr is as follows: <1-byte ACSmgr restart-value> <3-byte ACSmgr instance number> <Active charging service-name>.

losdv

Default: Enabled

This keyword controls the inclusion of the optional field "List of Service Data" in the x-CDRs.

ms-timezone

Default: Enabled

This keyword controls the inclusion of the optional field "MS-Timezone" in the x-CDRs.

msisdn

Default: Enabled

This keyword controls the inclusion of the optional field "MSISDN" in the x-CDRs.

node-id

Default: Enabled

This keyword controls the inclusion of the optional field "Node ID" in the x-CDRs.

node-id-suffix *STRING*

Default: Disabled

Specifies the configured Node-ID-Suffix to use in the NodeID field of GTPP CDRs as an alphanumeric string of 1 through 16 characters. Each Session Manager task generates a unique NodeID string per GTPP context.



Important The NodeID field is a printable string of the *ndddSTRING* format: *n*: The first digit is the Sessmgr restart counter having a value between 0 and 7. *ddd*: The number of sessmgr instances. Uses the specified NodeID-suffix in all CDRs. The "Node-ID" field consists of sessMgr Recovery counter (1 digit) *n* + AAA Manager identifier (3 digits) *ddd* + the configured Node-Id-suffix (1 to 16 characters) *STRING*. If the centralized LRSN feature is enabled, the "Node-ID" field will consist of only the specified NodeID-suffix (NodeID-prefix is not included). If this option is not configured, then GTPP group name will be used instead (For default GTPP groups, context-name will be used).



Important If this **node-id-suffix** is not configured, the GGSN uses the GTPP context name as the Node-id-suffix (truncated to 16 characters) and the SGSN uses the GTPP group named as the node-id-suffix.

pdn-connection-id

Default: Enabled

This keyword controls the inclusion of the optional field "PDN Connection ID" in the x-CDRs.

pdp-address

Default: Enabled

This keyword controls the inclusion of the optional field "PDP Address" in the x-CDRs.

pdp-type

Default: Enabled

This keyword controls the inclusion of the optional field "PDP Type" in the x-CDRs.

pgw-ipv6-addr

Default: Disabled

Specifying this option allows to configure the P-GW IPv6 address.



Important This attribute can be controllably configured in custom24 and custom35 SGW-CDR dictionaries.

pgw-plmn-id

Default: Enabled

This keyword controls the inclusion of the optional field "PGW PLMN-ID" in the x-CDRs.

plmn-id [unknown-use]

Default: Enabled

For SGSN, reports the SGSN PLMN Identifier value (the RAI) in the S-CDR provided if the dictionary supports it.

For GGSN, reports the SGSN PLMN Identifier value (the RAI) in the G-CDR if it was originally provided by the SGSN in the GTP create PDP context request. It is omitted if the SGSN does not supply one.

Normally when SGSN PLMN-id information is not available, the attribute sgsnPLMNIdentifier is not included in the CDR. This keyword enables the inclusion of the sgsnPLMNIdentifier with a specific value when the SGSN PLMN-id is not available.

unknown-use *hex_num*: is aa hexadecimal number from 0x0 through 0xFFFFFF that identifies a foreign SGSN that has not provided a PLMN-id. For GGSN only.

qos max-length

Default: Disabled

Specifying this option will change the parameters related to QoS sent in S-CDR and SaMOG CDR. The **max-length** option is used to modify the length of QoS sent in CDR. The **qos_value** must be an integer from 4 through 24.

This feature is introduced to support Rel.7+ QoS formats.

rat

Default: Enabled

For SGSN: includes the RAT (identifies the radio access technology type) value in the S-CDR.

For GGSN: includes the RAT (identifies the radio access technology type) value in the G-CDR.

recordextension

Default: Disabled

This keyword controls the inclusion of the optional field "RecordExtension" in the x-CDRs.

record-extensions rat

Default: Disabled

Enables network operators and/or manufacturers to add their own recommended extensions to the CDRs according to the standard record definitions from 3GPP TS 32.298 Release 7 or higher.

record-type { sgsnpdprecord | sgwrecord }



Important This keyword is available only when the SaMOG Mixed Mode license (supporting both 3G and 4G) is configured.

Default: sgwrecord

Specifies the SaMOG CDR type to use.

For an SaMOG 3G license, this keyword will not be available. However, sgsnpdprecord type will be used as the default record type.

served-mnai

Default: Disabled

This keyword controls the inclusion of the optional field "Served MNAI" in the x-CDRs.

served-pdp-pdn-address-extension

Default: Disabled

In support of IPv4v6 dual-stack PDP address types, this keyword causes the service to include IPv4v6 address information in the CDR. The IPv4 address goes in the Served PDP PDN Address Extension field and the IPv6 address goes in the Served PDP Address or Served PDP PDN Address field.

Important This attribute will not be displayed if the GTPP dictionary is set to custom34.

Note For SGSN, on enabling **served-pdp-pdn-address-extension** all custom S-CDR dictionaries will support the CDR field "Served PDP/ PDN Address extension" except for the following dictionaries:

- custom17
- custom18
- custom23
- custom42
- custom41

served-pdp-pdn-address-prefix-length

Default: Enabled

In support of IPv6 prefix delegation, this keyword causes the service to include this field "Served PDP PDN Address" in the x-CDRs.

If this field is configured, the servedPDPPDNAddress field will support reporting the IPv6 prefix length as outlined in 3GPP 32.298. The prefix length will only be reported if:

- it is configured
- it is not the default length of 64
- it is an IPv6 or IPv4v6 call

sgsn-change

Default: Enabled

This keyword is specific to SGSN and is license restricted.

This keyword controls the inclusion of the S-CDR attribute "SGSN Change" in the S-CDRs. It is enabled by default and the attribute "SGSN Change" is included in the S-CDRs by default.

Note For SGSN specific custom33 dictionary, it is recommended to disable this keyword before an upgrade to prevent billing issues.

sgw-ipv6-addr

Default: Disabled

Specifying this option allows to configure the S-GW IPv6 address.

Important This attribute can be controllably configured in custom24 and custom35 SGW-CDR dictionaries.

sms { destination-number | recording-entity | service-centre }

This keyword is specific to the SGSN.

Entering this keyword causes the inclusion of an SMS-related field in the SMS-MO-CDR or SMS-MT-CDR.

destination-number: Includes the "destinationNumber" field in the SMS-MO-CDR or SMS-MT-CDR.

recording-entity: Includes the "recordingEntity" field in the SMS-MO-CDR or SMS-MT-CDR.

service-centre: Includes the "serviceCentre" field in the SMS-MO-CDR or SMS-MT-CDR.

sna-ipv6-addr

Default: Disabled

Specifying this option allows to configure the Serving Node IPv6 Address (SNAv6).



Important This attribute can be controllably configured in custom24 and custom35 SGW-CDR dictionaries.

sponsor-id

Default: Disabled

Includes the Sponsor ID and Application-Service-Provider-Identity fields in PGW-CDR.

Note that the "Sponsor ID" and "Application-Service-Provider-Identity" attributes will be included in PGW-CDR if the PCEF supports Sponsored Data Connectivity feature or the required reporting level is sponsored connectivity level as described in 3GPP TS 29.212.

This feature is implemented to be in compliance with Release 11 3GPP specification for CDRs. So, this behavior is applicable to all GTPP dictionaries that are Release 11 compliant, i.e. custom35.

start-time

Default: Enabled

This keyword controls the inclusion of the optional field "Start-Time" in the x-CDRs.

stop-time

Default: Enabled

This keyword controls the inclusion of the optional field "Stop-Time" in the x-CDRs.

twanuli

Default: Disabled

This keyword controls the inclusion of the optional field "TWAN User Location Information" in the CDRs.

uli

Default: Enabled

This keyword controls the inclusion of the optional field "User Location Information" in the x-CDRs.

user-csg-information

Default: Disabled

This keyword controls the inclusion of the optional field "User CSG Information" in the x-CDRs.

Important Currently, UCI values are only supported for SGW-CDRs.

This attribute will not be displayed if the GTPP dictionary is set to custom11, custom34, or custom35.

+

Indicates that this command can be entered multiple times to configure multiple attributes.

Usage Guidelines Use this command to configure the type of optional information fields to include in generated CDRs (M-CDRs, S-CDRs, S-SMO-CDR, S-SMT-CDR from SGSN and G-CDRs, eG-CDRs from GGSN) by the AGW (SGSN/GGSN/P-GW/SAEGW). In addition, it controls how the information for some of the mandatory fields are reported.

Fields described as optional by the standards but not listed above will always be present in the CDRs, except for Record Extensions (which will never be present).

Important This command can be repeated multiple times with different keywords to configure multiple GTPP attributes.

Example

The following command configures the system to present the time provided in the Duration field of the CDR is reported in milliseconds:

```
gtpp attribute duration-ms
```

gtpp charging-agent

Configures the IP address and port of the system interface within the current context used to communicate with the Charging Gateway Function (CGF).

Product

GGSN

SGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpp charging-agent address ip_address [ port port ]
no gtpp charging-agent
```

no

Removes a previously configured charging agent address.

address *ip_address*

Specifies the IP address of the interface configured within the current context that is used to transmit CDR records (G-CDR/eG-CDR/M-CDR/S-CDR) to the CGF. *ip_address* must be entered using IPV4 dotted-decimal notation.

port *port*

Specifies the Charging Agent UDP port. as an integer from 1 through 65535.

If *port* is not defined, IP will take the default port number 49999.

Important Configuring gtpp charging-agent on port 3386 may interfere with a ggsn-service configured with the same ip address.

Usage Guidelines

This command establishes a Ga interface for the system. For GTPP accounting, one or more Ga interfaces must be specified for communication with the CGF. These interfaces must exist in the same context in which GTPP functionality is configured (refer to the **gtpp** commands in this chapter).

This command instructs the system as to what interface to use. The IP address supplied is also the address by which the GSN is known to the CGF. Therefore, the IP address used for the Ga interface could be identical to one bound to a GSN service (a Gn interface).

If no GSN service is configured in the same context as the Ga interface, the address configured by this command is used to receive unsolicited GTPP packets.

Example

The following command configures the system to use the interface with an IP address of *192.51.100.0* as the accounting interface with port *20000* to the CGF:

```
gtpp charging-agent address 192.51.100.0 port 20000
```

gtpp data-record-format-version

Encodes the data record format version. The version indicates the 3GPP release version.

Product



Important In releases prior to 18, this is applicable only to custom24 and custom35 GTPP dictionaries for S-GW. In 18 and later releases, this command is applicable to all GTPP dictionaries for all products including GGSN, P-GW, S-GW and SGSN.

GGSN

P-GW

SGSN

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] gtpp data-record-format-version` *`string`*

no

Specifies that the default data record format will be encoded based on the GTPP dictionary being used.

gtpp data-record-format-version *string*

Specifies the 3GPP release version to be encoded. *string* must be in the format a.b (for example 10.10). The entry can be from 1 to 1023 alphanumeric characters.

Usage Guidelines

Use this command to support a configurable multiple data record format version *only for custom24 and custom35 dictionaries* in releases prior to 18, and all GTPP dictionaries in release 18 and beyond. The entry can be from 1 to 1023 alphanumeric characters. This is useful when the value of the data record format version is taken according to the dictionary being used. If only the default configuration is used, a version mismatch causes the GTPP request to be discarded while using R10 attributes.

Example

This example configures the data record format version *10.10* to be encoded.

```
gtpp data-record-format-version 10.10
```

gtpp data-request sequence-numbers

Configures the range of sequence numbers to be used in the GTPP data record transfer record (DRT). Use this command to set the start value for the sequence number.

Product

GGSN

SGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpp data-request sequence-numbers start { 0 | 1 }
default gtpp data-request sequence-numbers start
```

default

Default is 0 (zero).

{ 0 | 1 }

Specifies the value of the start sequence number for the GTPP Data Record Transfer Request. Default: 0

- **0**: Designates the start sequence number as 0.
- **1**: Designates the start sequence number as 1.

Usage Guidelines

When the GGSN/P-GW (SAEGW)/SGSN is configured to send GTPP echo request packets, the SGSN always uses 0 as the sequence number in those packets. Re-using 0 as a sequence number in the DRT packets is allowed by the 3GPP standards; however, this CLI command ensures the possibility of inter-operating with CGFs that can not properly handle the re-use of sequence number0 in the echo request packets.

Example

The following command sets the sequence to start at *1*.

```
gtpp data-request sequence-numbers start 1
```

gtpp dead-server suppress-cdrs

Enables or disables CDR archiving when a dead server is detected.



Important This command is customer specific. For more information please contact your local Cisco service representative.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ default | no ] gtpp dead-server suppress-cdrs`

default

Configures the default setting.

Default: Disabled

no

Re-enables CDR archiving.

Usage Guidelines

Use this command to enable/disable CDR archiving when a dead server is detected.With this CLI, once a server is detected as down, requests are purged.Also the requests generated for the period when the server is down are purged.

gtpp deadtime

Configures the amount of time to wait before attempting to communicate with a Charging Gateway Function (CGF) that was previously marked as unreachable.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`gtpp deadtime` *`time`*
`default gtpp deadtime`

default

Configures this command with the default setting.

Default: 120 seconds

time

Specifies the amount of time (in seconds) that must elapse before the system attempts to communicate with a CGF that was previously unreachable. *time* is an integer from 1 through 65535.

Usage Guidelines

If the system is unable to communicate with a configured CGF, after a pre-configured number of failures the system marks the CGF as being down.

This command specifies the amount of time that the system waits prior to attempting to communicate with the downed CGF.

Refer to the **gtpp detect-dead-server** and **gtpp max-retries** commands for additional information on the process the system uses to mark a CGF as down.

Example

The following command configures the system to wait *60* seconds before attempting to re-communicate with a CGF that was marked as down:

```
gtpp deadtime 60
```

gtpp detect-dead-server

Configures the number of consecutive communication failures that could occur before the system marks a Charging Gateway Function (CGF) as down.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp detect-dead-server consecutive-failures *max_number*
default gtpp detect-dead-server consecutive-failures

default

Configures this command with the default setting.

Default: 0

consecutive-failures *max_number*

Specifies the number of failures that could occur before marking a CGF as down. *max_number* is an integer from 0 through 1000.

Usage Guidelines

This command works in conjunction with the **gtpp max-retries** parameter to set a limit to the number of communication failures that can occur with a configured CGF.

The gtpp max-retries parameter limits the number of attempts to communicate with a CGF. Once that limit is reached, the system treats it as a single failure. The gtpp detect-dead-server parameter limits the number of consecutive failures that can occur before the system marks the CGF as down and communicate with the CGF of next highest priority.

If all of the configured CGFs are down, the system ignores the detect-dead-server configuration and attempt to communicate with highest priority CGF again.

Important When the **gtpp detect-dead-server consecutive-failures** CLI command is used in the CDR streaming mode, the CDRs will not be written to the HDD even when all the CGF servers are inactive. The CDR records will be archived at AAA manager and then purged when the archival limit is reached.

If the system receives a GTPP Node Alive Request, Echo Request, or Echo Response message from a CGF that was previously marked as down, the system immediately treats it as being active.

Refer to the **gtpp max-retries** command for additional information.

Example

The following command configures the system to allow *8* consecutive communication failures with a CGF before it marks it as down:

```
gtpp detect-dead-server consecutive-failures 8
```

gtpp dictionary

Designates a dictionary used by GTPP for a specific context.

Product

GGSN

SGSN

PDG/TTG

P-GW

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpp dictionary { custom1 | custom10 | custom11 | custom12 | custom13 |
custom14 | custom15 | custom16 | custom17 | custom18 | custom19 | custom2
 | custom20 | custom21 | custom22 | custom23 | custom24 | custom25 |
custom26 | custom27 | custom28 | custom29 | custom3 | custom30 | custom31
 | custom32 | custom33 | custom34 | custom35 | custom36 | custom37 |
custom38 | custom39 | custom4 | custom40 | custom41 | custom42 | custom43
 | custom44 | custom45 | custom46 | custom47 | custom48 | custom49 |
custom5 | custom50 | custom51 | custom52 | custom53 | custom54 | custom55
 | custom56 | custom57 | custom58 | custom59 | custom6 |  custom60 |
custom7 | custom8 | custom9 | standard }
default gtpp dictionary
```

default

Configures the default dictionary.

custom1

This is a custom-defined dictionary that conforms to TS 32.015 v 3.6.0 for R99. It supports the encoding of IP addresses in text format for G-CDRs.

custom2

Custom-defined dictionary.

custom3

This is a custom-defined dictionary that conforms to TS 32.015 v 3.6.0 for R99 except that it supports the encoding of IP addresses in binary format for G-CDRs.

custom4

This is a custom-defined dictionary that conforms to TS 32.015 v 3.6.0 for R99 except that:

- IP addresses are encoded in binary format.
- The Data Record Format Version information element contains 0x1307 instead of 0x1308.
- QoS Requested is not present in the LoTV containers.
- QoS negotiated is added only for the first container and the container after a QoS change.

custom5

Custom-defined dictionary.

custom6

This is a custom-defined dictionary for eG-CDR encoding.

custom7 ... custom30

These custom-defined dictionary have default behavior or "standard" dictionary.

custom31

This is a custom-defined dictionary for S-CDR encoding that is based on 3GPP TS 32.298 v6.4.1 with a special field appended for the PLMN-ID.

custom33

This ia a custom-defined dictionary for S-CDR encoding that is based on the 3GPP TS 32.298v6.4.1 with the following exceptions:

- Proprietary PLMN-ID field is present.
- It is a SEQUENCE and not a SET.
- Diagnostics and SGSN-Change fields are not supported.
- Indefinite length encoding is used.
- Booleans are encoded as 0x01(3GPP it is 0xff).
- IMEISV shall be sent if available else IMEI should be sent.
- Record Sequence Number is Mandatory.
- APN OI and NI part is length encoded.
- Cause for Record closure should be "RAT Change" instead of "intra-SGSNinter-system".

standard

Default: Enabled

This dictionary conforms to TS 32.215 v 4.6.0 for R4 (and also R5 - extended QoS format).

Usage Guidelines

Use this command to designate specific dictionary used by GTPP for specific context.



Important Note that the following warning message will be displayed whenever an existing GTPP dictionary is being changed or a new GTPP dictionary is configured irrespective of whether or not the calls are active on the system.

Warning: It is not recommended to change the dictionary when the system has active calls.

Are you sure? [Yes|No]: n



Important This change will require user's input on the CLI console for GTPP dictionary configuration / change.

Example

The following command configures the system to use *custom3* dictionary to encode IP address in Binary format in G-CDRs:

gtpp dictionary custom3

gtpp duplicate-hold-time

Configures the number of minutes to hold on to CDRs that are possibly duplicates while waiting for the primary Charging Gateway Function (CGF) to come back up.

Product

GGSN

SGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp duplicate-hold-time *minutes*
default gtpp duplicate-hold-time

default

Configures this command with the default setting.

Default: 60 minutes

minutes

Specifies the number of minutes to hold on to CDRs that may be duplicates whenever the primary CGF is down, *minutes* must be an integer from 1 through 10080.

Usage Guidelines

Use this command to configure how long to hold on to CDRs that are possibly duplicates while waiting for the primary CGF to come back up. If the GGSN/P-GW (SAEGW) determines that the primary CGF is down, CDRs that were sent to the primary CGF but not acknowledged are sent by the GSN to the secondary CGF as "possibly duplicates". When the primary CGF comes back up, the GSN uses GTPP to determine whether the possibly duplicate CDRs were received by the primary CGF. Then the secondary CGF is told whether to release or cancel those CDRs. This command configures how long the system should wait for the primary CGF to come back up. As soon as the configured time expires, the secondary CGF is told to release all of the possibly duplicate CDRs.

Example

Use the following command to set the amount of time to hold on to CDRs to 2 hours (120 minutes);

```
gtpp duplicate-hold-time 120
```

gtpp echo-interval

Configures the frequency at which the system sends GTPP echo packets to configured CGFs.

Product

GGSN

SGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpp echo-interval time
{ default | no } gtpp echo-interval
```

default

Configures the default setting for this command,

Default: 60 seconds

no

Disables the use of the echo protocol except for the scenarios described in the *Usage* section for this command.

time

Specifies the time interval (in seconds) for sending GTPP echo packets as an integer from 60 through 2147483647. Default: 60

Usage Guidelines

The GTPP echo protocol is used by the system to ensure that it can communicate with configured CGFs. The system initiates this protocol for each of the following scenarios:

- Upon system boot
- Upon the configuration of a new CGF server on the system using the **gtpp server** command as described in this chapter

- Upon the execution of the **gtpp test accounting** command as described in the *Exec Mode Commands* chapter of this reference
- Upon the execution of the **gtpp sequence-numbers private-extensions** command as described in this chapter

The echo-interval command is used in conjunction with the gtpp max-retries and gtpp timeout commands as described in this chapter.

In addition to receiving an echo response for this echo protocol, if we receive a GTPP Node Alive Request message or a GTPP Echo Request message from a presumed dead CGF server, we will immediately assume the server is active again.

The alive/dead status of the CGFs is used by the AAA Managers to affect the sending of CDRs to the CGFs. If all CGFs are dead, the AAA Managers will still send CDRs, (refer to the **gtpp deadtime** command), albeit at a slower rate than if a CGF were alive. Also, AAA Managers independently determine if CGFs are alive/dead.

Example

The following command configures an echo interval of *120* seconds:

```
gtpp echo-interval 120
```

gtpp egcdr

Configures the eG-CDR and P-CDR (P-GW CDR) parameters and triggers.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpp egcdr { closure-reason admin-disconnect [ management-intervention |
 normal-release ] | final-record [ [ include-content-ids { all |
only-with-traffic } ] [ closing-cause { same-in-all-partials | unique }
] ] | losdv-max-containers max_losdv_containers | lotdv-max-containers
max_lotdv_containers | dynamic-path ddl-path | rulebase-max-length
rulebase_name_max_length | service-data-flow threshold { interval interval |
volume { downlink bytes [ uplink bytes ] | total bytes | uplink bytes [ downlink
 bytes ] } } | service-idle-timeout { 0 | service_idle_timeout } }
default gtpp egcdr { closure-reason admin-disconnect | dynamic-path |
final-record include-content-ids only-with-traffic closing-cause
same-in-all-partials | losdv-max-containers | lotdv-max-containers |
```

```
service-idle-timeout 0 }
no gtpp egcdr { dynamic-path | rulebase-max-length | service-data-flow
threshold { interval | volume { downlink [ uplink ] | total | uplink [
downlink ] } } }
```

closure-reason admin-disconnect [management-intervention | normal-release]

Controls the configuration of "causeForRecordClosing" in PGW-CDR when a call is cleared from the chassis.

Releases prior to 14.1, when a call is cleared from the chassis the field "causeForRecordClosing" in a PGW-CDR shows "Normal Release". In 15.0 and later releases, the behavior has changed to comply with the 3GPP specifications. That is, the default "causeForRecordClosing" in PGW-CDR will be "Management Intervention".



Important This behavioral change is limited to PGW-CDR Release 8 dictionaries only.

closing-reason: Configures the record closing reason for PGW-CDR.

- **management-intervention**: Specifies to send Management-Intervention as causeForRecordClosing in PGW-CDRs. By default, Management-Intervention will be sent as the record closure reason for PGW-CDRs.
- **normal-release**: Specifies to send Normal Release as causeForRecordClosing in PGW-CDRs.

final-record [[include-content-ids { all | only-with-traffic }] [closing-cause { same-in-all-partials | unique }]]

Enables configuration of the final eG-CDR/P-CDR.

Default: Restores the GTPP eG-CDR/P-CDR final record to the default setting to include content IDs with some data to report are included. Also, sets the closing cause to the default of using the same closing cause for multiple final eG-CDR/P-CDRs.

- **include-content-ids**: Controls which content IDs are being included in the final eG-CDR/P-CDR.
  - **all**: Specifies that all content IDs be included in the final eG-CDR/P-CDR.
  - **only-with-traffic**: Specifies that only content-IDs with traffic be included in the final eG-CDR/P-CDRs.
- **closing-cause**: Configures closing cause for the final eG-CDR/P-CDR.
  - **same-in-all-partials**: Specifies that the same closing cause is to be included for multiple final eG-CDR/P-CDRs
  - **unique**: Specifies that the closing cause for final eG-CDR/P-CDRs is to be unique.

losdv-max-containers *max_losdv_containers*

The maximum number of List of Service Data Volume (LoSDV) containers in one eG-CDR/P-CDR.

max_losdv_containers must be an integer from 1 through 255.

Default: 10

lotdv-max-containers *max_lotdv_containers*

The maximum number of List of Traffic Data Volume (LoTDV) containers in one eG-CDR/P-CDR.

max_lotdv_containers must be an integer from 1 through 8.

Default: 8

dynamic-path *ddl-path*

This keyword activates a new and extensible framework to enable field defined (customer created) eGCDR/PGW-CDR generation. This option enables the user to load the customized or modified dictionary. The dictionary configured through this CLI command takes precedence over existing the **gtpp dictionary** CLI command.

This new framework is implemented to define a GTPP dictionary in a structured format using a "Dictionary Definition Language (DDL)". Using this language, customers can clearly define fields, triggers and behaviors applicable for a particular GTPP dictionary.

DDL file will be parsed at compilation time and metadata will be populated to generate eGCDR and PGW-CDR. This metadata makes the new framework more modular and maintainable. This will help in faster turnaround time in supporting any new enhancements.

When customer wants to add/modify/remove a field, this information has to be updated in DDL. The DDL file is processed dynamically and the field reflects in CDR. This framework works only for eGCDR and PGW-CDR.

ddl-path: Specifies the path of dictionary DDL. The path must be a string of size 0 through 127. This is to support field-loadable ddls. The DDL file will be parsed to populate metadata required to generate eGCDR/PGW-CDR.



Important It is not recommended to enable **gtpp egcdr dynamic-path** when there are active calls.

In this release, both current and new framework are functional to enable field defined (customer created) eGCDR/PGW-CDR generation. By default, the new framework is disabled.

rulebase-max-length *rulebase_name_max_length*

Specifies the maximum character length of charging rulebase name in LOSDVs of eG- CDR/P-CDR.

rulebase_name_max_length must be an integer from 0 through 63. Zero (0) means the rulebase name is added as-is.

Default: None. That is, full (un-truncated) charging rulebase name will go in LOSDVs of eG-CDR/P-CDR.

service-data-flow threshold { interval *interval* | volume { downlink *bytes* [uplink *bytes*] | total *bytes* | uplink *bytes* [downlink *bytes*] } }

Configures the thresholds for closing a service data flow container within an eG-CDR/P-CDR.

- **interval** *interval*: Specifies the time interval, in seconds, to close the eG-CDR/P-CDR if the minimum time duration thresholds for service data flow containers satisfied in flow-based charging.

  interval must be an integer from 60 through 40000000.

  Default: Disabled

- **volume { downlink** *bytes* **[uplink** *bytes* **] | total** *bytes* **| uplink** *bytes* **[downlink** *bytes* **] }**: Specifies the volume octet counts for the generation of the interim G-CDR/P-CDRs to service data flow container in FBC.
  - **downlink** *bytes*: specifies the limit for the number of downlink octets after which the eG-CDR/P-CDR is closed.
  - **total** *bytes*: Specifies the limit for the total number of octets (uplink+downlink) after which the eG-CDR/P-CDR is closed.
  - **uplink** *bytes*: specifies the limit for the number of uplink octets after which the eG-CDR/P-CDR is closed.
  - *bytes* must be an integer from 10000 through 400000000.

A service data flow container has statistics for an individual content ID. When the threshold is reached, the service data flow container is closed.

service-idle-timeout { 0 | *service_idle_timeout* }

Specifies a time period where if no data is reported for a service flow, the service container is closed and added to eG-CDR/P-CDR (as part of LOSDV container list) with service condition change as ServiceIdleOut.

service_idle_timeout must be an integer from 10 through 86400.

0: Specifies no service-idle-timeout trigger.

Default: 0

Usage Guidelines

Use this command to configure individual triggers for eG-CDR/P-CDR generation.

Use the **service-data-flow threshold** option to configure the thresholds for closing a service data flow container within an eG-CDR (eG-CDRs for GGSN and P-CDRs for PGW) during flow-based charging (FBC). A service data flow container has statistics regarding an individual content ID.

Thresholds can be specified for time interval and for data volume, by entering the command twice (once with interval and once with volume). When either configured threshold is reached, the service data flow container will be closed. The volume trigger can be specified for uplink or downlink or the combined total (uplink + downlink) byte thresholds.

When the PDP context is terminated, all service data flow containers will be closed regardless of whether the thresholds have been reached.

An eG-CDR/P-CDR will have at most ten service data flow containers. Multiple eG-CDR/P-CDRs will be created when there are more than ten.

Example

Use the following command to set the maximum number of LoSDV containers to *7*:

```
gtpp egcdr losdv-max-containers 7
```

The following command sets an eG-CDR threshold interval of *6000* seconds:

```
gtpp egcdr service-data-flow threshold interval 6000
```

gtpp error-response

Configures the response when the system receives an error response after transmitting a DRT (data record transfer) request.

Product

GGSN

SGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpp error-response { discard-cdr | retry-request }
default gtpp error-response
```

default

Configures this command with the default setting.

Default: **retry-request**

discard-cdr

Instructs the system to purge the request upon receipt of an error response and not to retry.

retry-request

Instructs the system to retry sending a DRT after receiving an error response. This is the default behavior.

Usage Guidelines

This command configures the system's response to receiving an error message after sending a DRT request.

Example

```
gtpp error-response discard-cdr
```

gtpp group

Configures GTPP server group in a context for the Charging Gateway Function (CGF) accounting server(s) that the system is to communicate with.

Product

ePDG

GGSN

SGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] gtpp group` *`group_name`* **`[ -noconfirm ]`**

group_name

Specifies the name of GTPP server group that is used for charging and/or accounting in a specific context. *group_name* must be an alphanumeric string of 1 through 63 character.

A maximum of eight GTPP server groups (excluding system created default GTPP server group "default") can be configured with this command in a context.

no

Removes the previously configured GTPP group within a context.

When a GTPP group is removed accounting information is not generated for all calls using that group and all calls associated with that group are dropped. A warning message displays indicating the number of calls that will be dropped.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

This feature provides the charging gateway function (CGF) accounting server configurable for a group of servers. Instead of having a single list of CGF accounting servers per context, this feature configures multiple GTPP accounting server groups in a context and each server group is consist of list of CGF accounting servers.

In case no GTPP server group is configured in a context, a server group named "default" is available and all the CGF servers configured in a specific context for CGF accounting functionality will be part of this "default" server group.

Example

The following command configures a GTPP server group named *star1* for CGF accounting functionality. This server group is available for all subscribers within that context.

`gtpp group star1`

gtpp max-cdrs

Configures the maximum number of charging data records (CDRs) included per packet.

Product

GGSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp max-cdrs *max_cdrs* **[wait-time** *wait_time* **]**
default gtpp max-cdrs

default

Configures this command with the default setting.

Default: One CDR per packet; disables **wait-time**

max_cdrs

Specifies the maximum number of CDRs to be inserted in a single packet as an integer from 1 through 255. Default: 1

wait-time ***wait_time***

Specifies the number of seconds the system waits for CDRs to be inserted into the packet before sending it. *wait_time* must be an integer from 1 through 300. Default: Disabled



Important If the **wait-time** expires, the packet is sent as this keyword over-rides *max_cdrs*.

Usage Guidelines

CDRs are placed into a GTPP packet as the CDRs close. The system stops placing CDRs into a packet when either the maximum *max_cdrs* is met, or the **wait-time** expires, or the value for the **gtpp max-pdu-size** command is met.

Example

The following command configures the system to place a maximum of *10* CDRs in a single GTPP packet before transmitting the packet:

```
gtpp max-cdrs 10
```

sgtpp max-pdu-size

Configures the maximum payload size of a single GTPP packet that could be sent by the system.

Product

GGSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp max-pdu-size *pdu_size*
default gtpp max-pdu-size

default

Configures this command with the default setting.

Default:65400 bytes

pdu_size

Specifies the maximum payload size (in octets) of the GTPP packet as an integer from 1024 to65400. The payload includes the CDR and the GTPP header.



Caution This command is effective only when GTPP single-source is configured, otherwise this command has no effect.

Usage Guidelines

The GTPP packet contains headers (layer 2, IP, UDP, and GTPP) followed by the CDR. Each CDR contains one or more volume containers. If a packet containing one CDR exceeds the configured maximum payload size, the system creates and send the packet containing the one CDR regardless.

The larger the packet data unit (PDU) size allowed, the more volume containers that can be fit into the CDR.

The system performs standard IP fragmentation for packets that exceed the system's maximum transmission unit (MTU).

Important The maximum size of an IPv4 PDU (including the IPv4 and subsequent headers) is 65,535. However, a slightly smaller limit is imposed by this command because the system's max-pdu-size doesn't include the IPv4 and UDP headers, and because the system may need to encapsulate GTPP packets in a different/larger IP packet (for sending to a backup device).

Example

The following command configures a maximum PDU size of *2048* octets:

```
gtpp max-pdu-size 2048
```

gtpp max-retries

Configures the maximum number of times the system attempts to communicate with an unresponsive Charging Gateway Function (CGF).

Product

GGSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp max-retries *max_attempts*
default gtpp max-retries

default

Configures this command with the default setting.

Default: 4

max_attempts

Specifies the number of times the system attempts to communicate with a CGF that is not responding. *max_attempts* is an integer from 1 through 15.

Usage Guidelines

This command works in conjunction with the **gtpp detect-dead-server** and **gtpp timeout** parameters to set a limit to the number of communication failures that can occur with a configured CGF.

When the value specified by this parameter is met, a failure is logged. The gtpp detect-dead-server parameter specifies the number of consecutive failures that could occur before the server is marked as down.

In addition, the gtpp timeout command controls the amount of time between re-tries.

If the value for the max-retries is met, the system begins storing CDRs in Random Access Memory (RAM). The system allocates memory as a buffer, enough to store one million CDRs for a fully loaded chassis (a maximum of one outstanding CDR per PDP context). Archived CDRs are re-transmitted to the CGF until they are acknowledged or the system's memory buffer is exceeded.

Refer to the **gtpp detect-dead-server** and **gtpp timeout** commands for additional information.

Example

The following command configures the maximum number of re-tries to be *8*:

```
gtpp max-retries 8
```

gtpp node-id

Configures the GTPP Node ID for all CDRs.

Product

ePDG

GGSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp node-id *node_id*
no gtpp node-id

no

Removes the previous gtpp node ID configuration.

node_id

Specifies the node ID for all CDRs as an alphameric string of 1 through 16 characters.

Usage Guidelines

Use this command to configure the GTPP Node ID for all CDRs.

Example

The following command configures the GTPP Node ID as *test123*:

```
gtpp node-id test123
```

gtpp redirection-allowed

Configures the system to allow or disallow the redirection of CDRs when the primary Charging Gateway Function (CGF) is unavailable.

Product

GGSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpp redirection-allowed
{ default | no } gtpp redirection-allowed
```

default

Configures this command with the default setting. Default: Enabled

no

Deletes the command from the configuration.

Usage Guidelines

This command allows operators to better handle erratic network links, without having to remove the configuration of the backup server(s) via the **no gtpp server** command.

This functionality is enabled by default.

If the no gtpp redirection-allowed command is executed, the system only sends CDRs to the primary CGF. If that CGF goes down, we will buffer the CDRs in memory until the CGF comes back or until the system runs out of buffer memory. In addition, if the primary CGF announces its intent to go down (with a GTPP Redirection Request message), the system responds to that request with an error response.

gtpp redirection-disallowed

This command has been obsoleted and is replaced by the **gtpp redirection-allowed** command.

gtpp server

Configures the Charging Gateway Function (CGF) accounting server(s) with which the system will communicate.

Product

ePDG

GGSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp server *ip_address* **[max** *max_messages* **] [priority** *priority* **] [port** *port* **] [node-alive { enable | disable }] [-noconfirm]**
no gtpp server *ip_address*

no

Deletes a previously configured CGF.

ip_address

Specifies the IP address of the CGF in IPv4 dotted-decimal or IPV6 colon-separated-hexadecimal notation.

max *max_messages*

Default: 256

Specifies the maximum number of outstanding or unacknowledged GTPP packets (from any one AAA Manager task) allowed for this CGF before the system begins buffering the packets.

max_messages can be configured as an integer from 1 through 256.



Important A warning message is displayed if the user tries to configure a value greater than 100 and the max-outstanding is configured as 100. This is because there is an internal limit of up to 100 max outstanding requests that can be configured.

priority *priority*

Default:1000

Specifies the relative priority of this CGF. When multiple CGFs are configured, the priority is used to determine which CGF server to send accounting data to.

priority can be configured as an integer from 1 through 1000. When configuring two or more servers with the same priority you will be asked to confirm that you want to do this. If you use the **-noconfirm** option, you are not asked for confirmation and multiple servers could be assigned the same priority.

port *port*

Default: 3386

Specifies the port the CGF is using. *port* can be configured as an integer from 1 through 65535. Default value for port is 3286.



Important The **port** keyword option has been modified from **udp-port** to make it a generic command. The **udp-port** keyword can still be used, however, it will be in concealed mode and will not be shown in auto-complete or help for the command.

node-alive { enable | disable }

Default: Disable.

This optional keyword allows operator to enable/disable GSN to send Node Alive Request to GTPP Server (i.e. CGF). This configuration can be done per GTPP Server basis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to configure the CGF(s) that the system sends CDR accounting data to.

Multiple CGFs can be configured using multiple instances of this command. Up to 12 CGF scan be configured per system context. Each configured CGF can be assigned a priority. The priority is used to determine which server to use for any given subscriber based on the routing algorithm that has been implemented. A CGF with a priority of "1" has the highest priority.



Important The configuration of multiple CGFs with the same IP address but different port numbers is not supported.

Each CGF can also be configured with the maximum allowable number of unacknowledged GTPP packets. Since multiple AAA Manager tasks could be communicating with the same CGF, the maximum is based on

any one AAA Manager instance. If the maximum is reached, the system buffers the packets Random Access Memory (RAM). The system allocates memory as a buffer, enough to store one million CDRs for a fully loaded chassis (a maximum of one outstanding CDR per PDP context).

Example

The following command configures a CGF with an IP address of *192.51.100.2* and a priority of *5*.

```
gtpp server 192.51.100.2 priority 5
```

The following command deletes a previously configured CGF with an IP address of *100.10.35.7*:

```
no gtpp server 100.10.35.7
```

gtpp source-port-validation

Toggles port checking for node alive/echo/redirection requests from the CGF.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ default | no ] gtpp source-port-validation
```

default

Configures this command with the default setting.

Default: Enabled

no

Disables CGF port checking.Only the IP address will be used to verify CGF requests.

Usage Guidelines

This command is for enabling or disabling port checking on node alive/echo/redirection requests from the CGF. If the CGF sends messages on a non-standard port, it may be necessary to disable port checking in order to receive CGF requests. On the default setting, both IP and port are checked.

Example

The following command disables port checking for CGF requests:

```
no gtpp source-port-validation
```

gtpp storage-server

Configures information for the GTPP back-up storage server.

Product

ePDG

GGSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] gtpp storage-server` *ip-address* **`port`** *port-num*

no

Removes a previously configured back-up storage server.

ip-address

Specifies the IP address of the back-up storage server expressed in IPv4 dotted-decimal notation.

port *port-num*

Specifies the UDP port number over which the GSN communicates with the back-up storage server. Default: 3386

Usage Guidelines

This command configures the information for the server to which GTPP packets are to be backed up to if all the CGFs are unreachable.

One backup storage server can be configured per system context.



Important This command only takes affect if **gtpp single-source** in the Global Configuration Mode is also configured. Additionally, this command is customer specific. Please contact your local sales representative for additional information.

Example

The following command configures a back-up server with an IP address of *192.51.100.1*:

```
gtpp storage-server 192.51.100.1
```

gtpp storage-server local file

Configures the parameters for GTPP files stored locally on the GTPP storage server. This command is available for both ASR 5000 and 5500 platforms.

Product

GGSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpp storage-server local file { compression { gzip | none } | format {
custom1 | custom2 | custom3 | custom4 | custom5 | custom6 | custom7 |
custom8 } | name { format string [ max-file-seq-num seq_number ] | prefix
prefix } | purge-processed-files [ file-name-pattern file_pattern |
purge-interval purge_dur ] | push { encrypted-url url | url url } [
encrypted-secondary-url url | secondary-url url ] [ via-local-context ] |
rotation { cdr-count count | time-interval time [ force-file-rotation ] |
volume mb size } | start-file-seq-num seq_num [ recover-file-seq-num ]  }
default gtpp storage-server local file { compression | format | name {
format | prefix } | purge-processed-files | rotation { cdr-count |
time-interval | volume } | start-file-seq-num }
no gtpp storage-server local file { purge-processed-files | push | rotation
 { cdr-count | time-interval } }
```

default

Configures default setting for the specified parameter.

no

Removes a previously configured parameters for local storage of CDR files on HDD on SMC card.

compression { gzip | none }

Configures the type of compression to be used on the files stored locally.

- **gzip**: Enables Gzip file compression.
- **none**: Disables Gzip file compression -this is the default value.

Default: Disabled

format { *custom-n* }

Configures the file format to be used to format files to be stored locally.

custom1: File format custom1—this is the default value.

custom2: File format custom2.

custom3: File format custom3.

custom4: File format custom4.

custom5: File format custom5.

custom6: File format custom6 with a block size of 8K for CDR files.

custom7: File format custom7 is a customer specific CDR file format.

custom8: File format custom8 is a customer specific CDR file format. It uses *node-id-suffix_date_time_fixed-length-seq-num* format for file naming.

Default: **custom1**

name { format | prefix *prefix* }

Allows the format of the CDR filenames to be configured independently from the file format so that the name format contains the file name with conversion specifications.

prefix — Enter an alphanumeric string of 1 through 127 characters. The string ***must begin*** with the % (percent sign).

- **%y**: = year as a decimal number without century (range 00 to 99).
- **%Y**: year as a decimal number with century.
- **%m**: month as a decimal number (range 01 to 12).
- **%d**: day of the month as a decimal number (range 01 to 31).
- **%H**: hour as a decimal number 24-hour format (range 00 to 23).
- **%h**: hour as a decimal number 12-hour format (range 01 to 12).
- **%M**: minute as a decimal number (range 00 to 59).
- **%S**: second as a decimal number (range 00 to 60). (The range is up to 60 to allow occasional leap seconds.)
- **%Q**: File sequence number. Field width may be specified between the % and the Q. If the natural size of the field is smaller than this width, then the result string is padded (on the left) to the specified width with 0s

- **%N**: No of CDRs in the file. Field width may be specified between the % and the N. If the natural size of the field is smaller than this width, then the result string is padded (on the left) to the specified width with 0s
- **max-file-seq-no**: This can be configured optionally. It indicates the maximum value of sequence number in file name (starts from 1). Once the configured max-file-seq-no limit is reached, the sequence number will restart from 1. If no max-file-seq-no is specified then file sequence number ranges from 1 – 4294967295.

By default the above keyword is not configured (default gtpp storage-server local filename format). In which case the CDR filenames are generated based on the file format as before (maintains backward compatibility).

purge-processed-files [file-name-pattern *file_pattern* | purge-interval *purge_dur*]

Enables the GSN to periodically (every 4 minutes) delete locally processed (*.p) CDR files from the HDD on the SMC card. Default: Disabled

This keyword also deletes the processed push files (tx.*,under $CDR_PATH/TX/tx.*) a well when purging is enabled instead of "*.p:*.P".



Important This option is available only when GTPP server storage mode is configured for local storage of CDRs with the **gtpp storage-server mode local** command.

Optional keyword **file-name-pattern** *file_pattern* provides an option for user to control the pattern of files. *file_pattern* must be mentioned in "*.p:*.P:tx.*" format in a string of size 1 through 127, which is also the default format. Wildcards * and: (synonymous to |) are allowed.

Optional keyword **purge-interval** *purge_dur* provides an option for user to control the purge interval duration (in minutes). *purge_dur* must be an integer from 1 through 259200. Default value 60.

push { encrypted-url *encrypted_url* | url *url* } [encrypted-secondary-url *encrypted_url* | secondary-url *url*] [via-local-context]

Enables push method to transfer local CDR files to remote system.

encrypted-url: Defines use of an encrypted url.

encrypted_url must be an alphanumeric string of 1 through 8192 characters in SFTP format.

url: Location where the CDR files are to be transferred.

url must be an alphanumeric string of 1 through 1024 characters in the format:

scheme://user:password@host

encrypted-secondary-url: Defines use of an encrypted secondary url.

encrypted_url must be an alphanumeric string of 1 through 8192 characters in SFTP format.

secondary-url: Secondary location where the CDR files are to be transferred, in case primary is unreachable.

url must be an alphanumeric string of 1 through 1024 characters in the format:

scheme://user:password@host



Important When a file transfer to primary fails four times, the transfer of files will automatically be failed over to the secondary server. The transfer will switch back to the original primary after 30 minutes, or if there are four transfer failures to the secondary server.

via-local-context: Pushes the CDR files via SPIO in the local context.

Default: Pushes via the group's context.



Important If the push is done through gtpp context, then the push rate is lesser compared to via local context as the HDD is attached to the local context.

rotation { cdr-countcount | time-interval *time* | volume mb *size* }

Specifies rotation related configuration for GTPP files stored locally.

cdr-count *count*: Configures the CDR count for the file rotation as an integer from 1000 through 65000. Default value 10000.

time-interval *time*: Configures the time interval (in seconds) for file rotation as an integer from 30 through 86400. Default value 3600 (1 hour).

volume mb *size*: Configure the file volume (in MB) for file rotation. Enter an integer from 2 to 40. This trigger cannot be disabled. Default value is 4MB.

start-file-seq-num *seq_num* [recover-file-seq-num]

Specifies the start sequence number. The sequence number goes on incrementing until ULONG_MAX (or max-seq-num configured in file name format) and then it would rollover. If **recover-file-seq-num** is configured, every time the system is rebooted (or aaaproxy recovery/ planned/ unplanned packet service card migration), the file sequence number continues from the last sequence number and during rollover it starts from first-sequence number.

seq_num: Configures the sequence number. Enter an integer from 1 through 4294967295.

recover-file-seq-num: Configures the recovery of file sequence number. This is an optional field and if configured, every time the machine rebooted, the file sequence number continues from the last sequence number.

Usage Guidelines

This command configures the parameters for storage of GTPP packets as files on the local server—meaning the hard disk.

Example

The following command configures rotation for every 1.5 hours (5400 seconds) for locally stored files.

```
gtpp storage-server local file rotation time-interval 5400
start-file-seq-num 20 recover-file-seq-num
```

gtpp storage-server max-retries

Configures the maximum number of times the system attempts to communicate with an unresponsive GTPP back-up storage server.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp storage-server max-retries *max_attempts*
default gtpp storage-server max-retries

default

Configures this command with the default setting.

Default: 2

max_attempts

Specifies the number of times the system attempts to communicate with a GTPP back-up storage server that is not responding. *max_attempts* enter an integer from 1 through 15.

Usage Guidelines

This command works in conjunction with the **gtpp storage-server timeout** parameters to set a limit to the number of communication failures that can occur with a configured GTPP back-up storage server.

The **gtpp storage-server timeout** command controls the amount of time between re-tries.

Example

The following command configures the maximum number of re-tries to be *8*:

```
gtpp storage-server max-retries 8
```

gtpp storage-server mode

Configures storage mode, local or remote, for CDRs. Local storage mode is available with ASR 5000 platforms only.

Product

GGSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpp storage-server mode { local | remote | streaming }
default gtpp storage-server mode
```

default

Configures this command with the default setting.

Default: **remote**

local

Default: Disabled

Specifies the use of the hard disk on the SMC for storing CDRs

remote

Specifies the use of an external server for storing CDRs. This is the default value.

streaming

Default: Disabled

Allows the operator to configure "streaming" mode of operation for GTPP group. When this keyword is supplied the CDRs will be stored in following fashion:

- When GTPP link is active with CGF, CDRs are sent to a CGF via GTPP and local hard disk is NOT used as long as every record is acknowledged in time.
- If the GTPP connection is considered to be down, all streaming CDRs will be saved temporarily on the local hard disk and once the connection is restored, unacknowledged records will be retrieved from the hard disk and sent to the CGF.

Usage Guidelines

This command configures whether the CDRs should be stored on the hard disk of the SMC or remotely, on an external server.

Example

The following command configures use of a hard disk for storing CDRs:

```
gtpp storage-server mode local
```

gtpp storage-server timeout

Configures the amount of time that must pass with no response before the system re-attempts to communicate with the GTPP back-up storage server.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp storage-server timeout *duration*
default gtpp storage-server timeout

default

Configures this command with the default setting.

Default: 30 seconds

duration

Specifies the maximum amount of time (in seconds) the system waits for a response from the GTPP back-up storage server before assuming the packet is lost. *duration* is an integer from 30 through 120.

Usage Guidelines

This command works in conjunction with the **gtpp storage-server max-retries** command to establish a limit on the number of times that communication with a GTPP back-up storage server is attempted before a failure is logged. This parameter specifies the time between retries.

Example

The following command configures a retry timeout of *60* seconds:

```
gtpp storage-server timeout 60
```

gtpp suppress-cdrs zero-volume

This command suppresses the CDRs with zero byte data count. The CDRs can be classified as Final-cdrs, Internal-trigger-cdrs, and External-trigger-cdrs. This command allows the selection of CDRs to be suppressed and it is disabled by default.



Important Use of the Zero Volume CDR Suppression feature requires that a valid ECS license key be installed. Contact your Cisco account representative for information on how to obtain a license.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpp suppress-cdrs zero-volume { external-trigger-cdr | final-cdr |
internal-trigger-cdr }
default gtpp suppress-cdrs zero-volume
no gtpp suppress-cdrs zero-volume
```

default

Configures this command with the default setting.

no

Disables suppression of the CDRs with zero byte data count.

Usage Guidelines

This command suppresses the CDRs with zero byte data count. This command provides an option to select the CDRs to be suppressed.

Example

To suppress only final zero volume CDRs use:

```
gtpp suppress-cdrs zero-volume final-cdr
```

To suppress final zero Volume CDRs and interim zero volume CDRs due to internal triggers use:

```
gtpp suppress-cdrs zero-volume final-cdr internal-trigger-cdr
```

To suppress final zero volume CDRs and interim zero volume CDRs due to internal and external triggers use:

```
gtpp suppress-cdrs zero-volume final-cdr internal-trigger-cdr
external-trigger-cdr
```

To suppress interim zero volume CDRs due to internal and external triggers use:

```
gtpp suppress-cdrs zero-volume internal-trigger-cdr external-trigger-cdr
```

To suppress interim zero volume CDRs due to external triggers use:

```
gtpp suppress-cdrs zero-volume external-trigger-cdr
```

gtpp suppress-cdrs zero-volume-and-duration

Suppresses the CDRs created by sessions having zero duration and/or zero volume. By default this mode is disabled.

Product

GGSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp suppress-cdrs zero-volume-and-duration { gcdrs [egcdrs] | egcdrs [gcdrs] }
default gtpp suppress-cdrs zero-volume-and-duration

default

Configures this command with the default setting.

Default: Disabled.

gcdrs [egcdrs]

Suppresses G-CDRs before eG-CDRs.

egcdrs [gcdrs]

Suppresses eG-CDRs before G-CDRs.

Usage Guidelines

Use this command to suppress the CDRs (G-CDRs and eG-CDRs) which were created when zero-duration sessions and zero-volume sessions are encountered due to any reason. By default this command is disabled and system will not suppress any CDR.

Example

The following command configures the system to suppress the eG-CDRs created for a zero duration session or zero volume session:

gtpp suppress-cdrs zero-volume-and-duration egcdrs gcdrs

gtpp timeout

Configures the amount of time that must pass with no response before the system re-attempts to communicate with the Charging Gateway Function (CGF).

Product

GGSN

SGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp timeout *time*
default gtpp timeout

default

Configures this command with the default setting. Default: 20 seconds

time

Specifies the maximum amount of time (in seconds) the system waits for a response from the CGF before assuming the packet is lost. *time* is an integer from 1 through 60.

Usage Guidelines

This command works in conjunction with the **gtpp max-retries** command to establish a limit on the number of times that communication with a CGF is attempted before a failure is logged.

This parameter specifies the time between retries.

Example

The following command configures a retry timeout of *30* seconds:

```
gtpp timeout 30
```

gtpp trigger

This command is left in place for backward compatibility. To disable and enable GTPP triggers you should use the **gtpp trigger** command in GTPP Server Group Configuration Mode.

gtpp transport-layer

Selects the transport layer protocol for the Ga interface for communication between the access gateways (GSNs) and GTPP servers.

Product

GGSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpp transport-layer { tcp | udp }
default gtpp transport-layer
```

default

Configures this command with the default setting.

Default: **udp**

tcp

Default: Disabled

Enables the system to implement TCP as transport layer protocol for communication with GTPP server.

udp

Default: Enabled

Enables the system to implement UDP as transport layer protocol for communication with GTPP server.

Usage Guidelines

Use this command to select the TCP or UDP as the transport layer protocol for Ga interface communication between GTPP servers and AGWs (GSNs).

Example

The following command enables TCP as the transport layer protocol for the GSN's Ga interface.

```
gtpp transport-layer tcp
```

gtpu-service

Creates a GTP-U service or specifies an existing GTP-U service and enters the GTP-U Service Configuration Mode for the current context.

Product

GGSN

P-GW

SAEGW

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpu-service *service_name* **[-noconfirm]**
no gtpu-service *service_name*

gtpu-service *service_name*

Specifies the name of the GTP-U service. If *service_name* does not refer to an existing service, a new service is created if resources allow. *service_name* is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

no gtpu-service *service_name*

Removes the specified GTP-U service from the context.

Usage Guidelines

Enter the GTP-U Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-gtpu-service)#
```

GTP-U Service Configuration Mode commands are defined in the *GTP-U Service Configuration Mode Commands* chapter.

Example

The following command enters the existing GTP-U Service Configuration Mode (or creates it if it does not already exist) for the service named *gtpu-service1*:

gtpu-service gtpu-service1

The following command will remove *gtpu-service1* from the system:

no gtpu-service gtpu-service1

gtpu peer statistics threshold

Specifies the maximum number of GTP-U peers for which statistics will be maintained.

Product

P-GW

SAEGW

S-GW

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

gtpu peer statistics threshold *value*

gtpu peer statistics threshold *value*

Specifies the number of GTP-U peers for which the node will maintain statistics.

Valid entries are from 16000 to 128000.

The default setting is 16000.

The threshold cannot be configured to a lower value than the current value. For example if the threshold value is set to 18000, it can no longer be set to any value below 18000.

Usage Guidelines

Use this command to specify the number of GTP-U peers for which the node will maintain statistics.

Example

The following command specifies that the node will maintain GTP-U peer statistics for 50000 GTP-U peers:

gtpu peer statistics threshold *50000*

ha-service

Creates/deletes a home agent service or specifies an existing HA service for which to enter the Home Agent Service Configuration Mode for the current context.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax Description

ha-service *name* **[-noconfirm]**
no ha-service *name*

no

Indicates the home agent service specified is to be removed.

name

Specifies the name of the HA service to configure. If *name* does not refer to an existing service, the new service is created if resources allow. *name* is an alphanumeric string of 1 through 63 characters.



Important Service names must be unique across all contexts within a chassis.

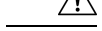
-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Enter the HA Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.



Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Example

The following command will enter, or create and enter, the HA service *sampleService*:

```
ha-service sampleService
```

The following command will remove *sampleService* as being a defined HA service:

```
no ha-service sampleService
```

hexdump-module

Enter the Hexdump Service Configuration Mode to configure hexdump records creation and other related parameters.

Product

ePDG

SaMOG

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

hexdump-module
no hexdump-module

no

Disables creation of hexdump records.

Usage Guidelines

Enter the Hexdump Service Configuration Mode to configure hexdump records creation and other related parameters.

hnbgw-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.

Creates or removes an Home Node B Gateway (HNB-GW) service or configures an existing HNB-GW service and enters the HNB-GW Service Configuration Mode for Femto UMTS access networks configuration in the current context.

Product

HNB-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

hnbgw-service *hnbgw_svc_name* **[-noconfirm]**
no hnbgw-service *hnbgw_svc_name*

no

Removes the specified HNB-GW service from the context.

hnbgw_svc_name

Specifies the name of the HNB-GW service. If *service_name* does not refer to an existing service, the new service is created if resources allow. *hnbgw_svc_name* is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to enter the HNB-GW Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of one HNB-GW service which is further limited to a maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-hnbgw-service)#
```

The commands available in this mode are defined in the *HNB-GW Service Configuration Mode Commands* chapter of *Command Line Interface Reference*.

Caution This is a critical configuration. The HNB-GW service can not be configured without this configuration. Any change to this configuration would lead to restarting the HNB-GW service and removing or disabling this configuration will stop the HNB-GW service.

Example

The following command enters the existing HNB-GW Service Configuration Mode (or creates it if it does not already exist) for the service named *hnb-service1*:

hnbgw-service hnb-service1

The following command will remove *hnb-service1* from the system:

no hnbgw-service hnb-service1

hsgw-service

Creates an HSGW service or specifies an existing HSGW service and enters the HSGW Service Configuration Mode for the current context.

Product HSGW

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

hsgw-service *service_name* **[-noconfirm]**
no hsgw-service *service_name*

no

Removes the specified HSGW service from the context.

service_name

Specifies the name of the HSGW service. If *service_name* does not refer to an existing service, the new service is created if resources allow. *service_name* is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Enter the HSGW Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-hsgw-service)#
```

HSGW Service Configuration Mode commands are defined in the *HSGW Service Configuration Mode Commands* chapter.

Use this command when configuring the following eHRPD components: HSGW.

Example

The following command enters the existing HSGW Service Configuration Mode (or creates it if it does not already exist) for the service named *hsgw-service1*:

```
hsgw-service hsgw-service1
```

The following command will remove *hsgw-service1* from the system:

```
no hsgw-service hsgw-service1
```

hss-peer-service

Creates a Home Subscriber Service (HSS) peer service or configures an existing HSS peer service and enters the HSS Peer Service configuration mode.

Product

MME

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

hss-peer-service *service_name* **[-noconfirm]**
no hss-peer-service *service_name*

no

Removes the specified HSS peer service from the context.

service_name

Specifies the name of the HSS peer service. If *service_name* does not refer to an existing service, a new service is created if resources allow. *service_name* is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Enter the HSS Peer Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

The maximum number of HSS Peer Services that can be created and configured for the SGSN is 16.

The maximum number of HSS Peer Services that can be created and configured for the MME is 64.

Caution On a PSC2 setup, all diamproxy tasks might go in to a warning state if the number of hss-peer-services configured are more than 64 since the memory usage may exceed the allocated value.

Important In some cases, two diameter endpoints (S6a and S13) can be configured for a single HSS Peer Service. To ensure peak system performance, we recommend that the total of all Diameter endpoints should be taken into consideration and limited to 64 endpoints.

Caution A maximum of 256 services (regardless of type) can be configured per system. Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-hss-peer-service)#
```

HSS Peer Service Configuration Mode commands are defined in the *HSS Peer Service Configuration Mode Commands* chapter.

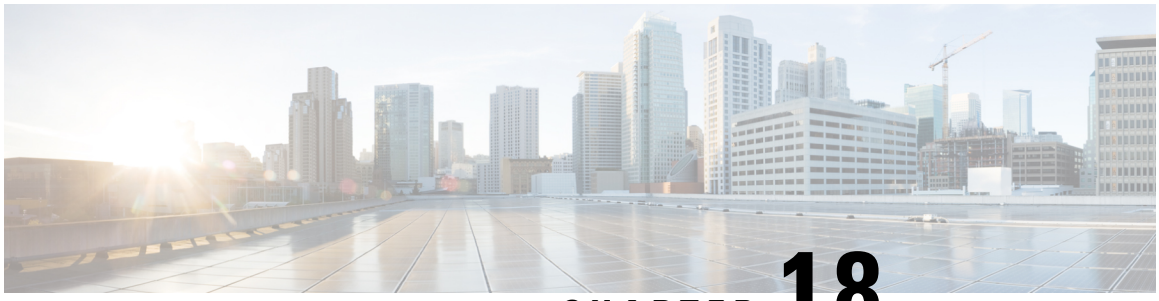
Example

The following command enters the existing HSS Peer Service Configuration Mode (or creates it if it does not already exist) for the service named *hss-peer1*:

hss-peer-service hss-peer1

The following command will remove *hss-peer1* from the system:

no hss-peer-service hss-peer1



CHAPTER 18

Context Configuration Mode Commands I-M

Command Modes

This section includes the commands **ikev1 disable-initial-contact** through **multicast-proxy** service.

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

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

- ignore ssh-ip, on page 495
- ikev1 disable-initial-contact, on page 495
- ikev1 disable-phase1-rekey, on page 496
- ikev1 keepalive dpd, on page 497
- ikev1 policy, on page 498
- ikev2-ikesa, on page 499
- ims-auth-service, on page 502
- ims-sh-service, on page 503
- inspector, on page 504
- interface, on page 508
- ip access-group, on page 510
- ip access-list, on page 511
- ip arp, on page 512
- ip as-path access-list, on page 513
- ip community-list, on page 514
- ip dns-proxy source-address, on page 515
- ip domain-lookup, on page 516
- ip domain-name, on page 517
- ip extcommunity-list, on page 518
- ip forward, on page 519
- ip guarantee, on page 520
- ip identification packet-size-threshold, on page 521

- ip igmp profile, on page 521
- ip localhost, on page 522
- ip name-servers, on page 523
- ip pool, on page 524
- ip prefix-list, on page 539
- ip prefix-list sequence-number, on page 540
- ip route, on page 541
- ip routing maximum-paths, on page 544
- ip routing overlap-pool, on page 545
- ip rri, on page 546
- ip rri-route, on page 547
- ip sri-route, on page 548
- ip vrf, on page 549
- ip vrf-list, on page 550
- ipms, on page 551
- ipne-service, on page 552
- ipsec replay, on page 553
- ipsec transform-set, on page 554
- ipsg-service, on page 555
- ipv6 access-group, on page 557
- ipv6 access-list, on page 557
- ipv6 dns-proxy, on page 558
- ipv6 neighbor, on page 559
- ipv6 pool, on page 560
- ipv6 prefix-list, on page 564
- ipv6 prefix-list sequence-number, on page 566
- ipv6 route, on page 566
- ipv6 route-access-list, on page 569
- ipv6 rri, on page 570
- ipv6 rri-route, on page 571
- ipv6 sri-route, on page 572
- isakmp disable-phase1-rekey, on page 573
- isakmp keepalive, on page 573
- isakmp policy, on page 573
- iups-service, on page 573
- l2tp peer-dead-time, on page 574
- lac-service, on page 575
- lawful-intercept, on page 576
- lawful-intercept dictionary, on page 576
- limit ipsecmgr ikev1 max, on page 576
- lma-service, on page 577
- lns-service, on page 579
- location-service, on page 580
- logging, on page 581
- mag-service, on page 584
- map-service, on page 585

- max-sessions, on page 586
- mipv6ha-service, on page 587
- mme-embms-service, on page 588
- mme-service, on page 590
- mobile-access-gateway, on page 592
- mobile-ip fa, on page 593
- mobile-ip ha assignment-table, on page 594
- mobile-ip ha newcall, on page 595
- mobile-ip ha reconnect, on page 597
- monitor-protocols, on page 598
- mpls bgp forwarding, on page 598
- mpls exp, on page 599
- mpls ip, on page 600
- mseg-service, on page 600
- multicast-proxy, on page 601

ignore ssh-ip

Ignores the SSH IP installation in UP.

Product

CUPS UP

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

ignore-ssh-ip

Usage Guidelines

Use this command to ignore the SSH IP installation in UP.

Example

The following command ignores the SSH IP installation in UP:

ignore-ssh-ip

ikev1 disable-initial-contact

Disables the sending of the INITIAL-CONTACT message in the IKEv1 protocol after the node creates a new Phase1 SA, caused either by Dead Peer Detection or by a rekey.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] ikev1 disable-initial-contact

no

Disables this command, which re-enables the sending of the INITIAL-CONTACT message.

Usage Guidelines

Use this command to disable the sending of the INITIAL-CONTACT message in the IKE v1protocol.

Example

The following command disables the sending of the INITIAL-CONTACT message:

ikev1 disable-initial-contact

ikev1 disable-phase1-rekey

Configures the rekeying of Phase1 SA when the Internet Security Association and Key Management Protocol (ISAKMP) lifetime expires in Internet Key Exchange (IKE) v1 protocol.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] ikev1 disable-phase1-rekey

no

Re-enables Phase 1SAs when the ISAKMP lifetime expires.

Usage Guidelines

Use this command to disable the rekeying of Phase 1 SAs when the ISAKMP lifetime expires in IKE v1 protocol.

Example

The following command disables rekeying of Phase1 SAs when the lifetime expires:

```
ikev1 disable-phase1-rekey
```

ikev1 keepalive dpd

Configures the ISAKMP IPSec Dead Peer Detection (DPD) message parameters for IKE v1 protocol.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] ikev1 keepalive dpd interval *interval* **timeout** *time* **num-retry** *retries*

no

Deletes previously configured IPSec DPD Protocol settings.

dpd interval *interval*

Specifies the time interval (in seconds) at which IPSec DPD Protocol messages are sent. *interval* is an integer from 10 through 3600.

timeout *time*

Specifies the amount of time (in seconds) allowed for receiving a response from the peer security gateway prior to re-sending the message. *time* is an integer from 10 through 3600.

num-retry *retries*

Specifies the maximum number of times that the system should attempt to reach the peer security gateway prior to considering it unreachable. *retries* is an integer from 1 through 100.

Usage Guidelines

Use this command to configure the ISAKMP dead peer detection parameters in IKE v1 protocol.

Tunnels belonging to crypto groups are perpetually kept "up" through the use of the IPSec Dead Peer Detection (DPD) packets exchanged with the peer security gateway.

Important The peer security gateway must support RFC 3706 in order for this functionality to function properly.

This functionality is for use with the Redundant IPSec Tunnel Fail-over feature and to prevent IPSec tunnel state mismatches between the FA and HA when used in conjunction with Mobile IP applications.

Regardless of the application, DPD must be supported/configured on both security peers. If the system is configured with DPD but it is communicating with a peer that does not have DPD configured, IPSec tunnels still come up. However, the only indication that the remote peer does not support DPD exists in the output of the **show crypto isakmp security associations summary dpd** command.

Important If DPD is enabled while IPSec tunnels are up, it will not take affect until all of the tunnels are cleared.

Example

The following command configures IPSec DPD Protocol parameters to have an interval of *15*, a timeout of *10*, to retry each attempt *5* times:

```
ikev1 keepalive dpd interval 15 timeout 10 num-retry 5
```

ikev1 policy

Configures or creates an ISAKMP policy with the specified priority and enters ISAKMP Configuration Mode for IKE v1 protocol.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] ikev1 policy *priority*

no

Removes a previously configured ISAKMP policy for IKE v1 protocol.

priority

Specifies the priority of an ISAKMP policy as an integer from 0 through 100. ISAKMP policies for IKE v1 protocol with lower priority numbers take precedence over policies with higher priorities. "0" is the highest priority. Default: 0

Usage Guidelines

Use this command to create ISAKMP policies to regulate how IPSec key negotiation is performed for IKE v1 protocol.

Internet Security Association Key Management Protocol (ISAKMP) policies are used to define Internet Key Exchange (IKE) SAs. The IKE SAs dictate the shared security parameters (i.e. which encryption parameters to use, how to authenticate the remote peer, etc.) between the system and a peer security gateway.

During Phase 1 of IPSec establishment, the system and a peer security gateway negotiate IKESAs. These SAs are used to protect subsequent communications between the peers including the IPSec SA negotiation process.

Multiple ISAKMP policies can be configured in the same context and are used in an order determined by their priority number.

Example

Use the following command to create an ISAKMP policy with the priority *1* and enter the ISAKMP Configuration Mode:

```
ikev1 policy 1
```

ikev2-ikesa

Creates a new, or specifies an existing, IKEv2 security association parameters and enters the IKEv2 Security Association Configuration Mode.



Important In Release 20, 21.0 and 21.1, HeNBGW is not supported. This command must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

HeNBGW

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] ikev2-ikesa { auth-method-set *auth_method_set_name* **| certificate policy** *policy_name* **| ddos { blacklist ip-address** *ipv4_address | ipv6_address* **| [**

init-flood | udp-error] { source-based | system-based } [threshold-upper *threshold_upper_value* **[threshold-lower** *threshold_lower_value* **[poll-timer-duration** *poll_timer_duration_value* **]]] } | dh-group { [1 | 14 | 2 | 5] + { | reuse } } | transform-set** *transform_set_name* **}**

{ default | no } ikev2-ikesa dh-group reuse

default

Sets the IKEv2 IKESA Diffie-Hellman related parameter to its default value.

Default: 14

no

Removes the entered IKEv2 security association parameters.

auth-method-set *auth_method_set_name*

Configure an IKEv2 IKE Security Association Auth-Method Set. Applicable for IKEv2 subscriber-mode based products, This object encapsulates various Authentication methods.

auth_method_set_name is the context level name to be used for the IKEv2 IKE Security Association Authentication methods Set, which is a string of size 1 to 127.

certificate policy *policy_name*

certificate: Configures certificate related configuration to be associated to crypto template.

policy: Configures certificate policy to be used for certificate related auth method.

policy_name is the context level name to be used for the IKEv2 Security Association Cert Policy, which is a string of size 1 to 127.

ddos

Configures the IKEv2 DDoS mitigation Parameters.

blacklist ip-address*ipv4_address* | *ipv6_address*

Configures the source IPv4 or IPv6 address to be blacklisted.

init-flood

Configures the IKEv2 DDoS mitigation parameters for INIT Floods.

udp-error

Configures the IKEv2 DDoS mitigation parameters for UDP errors.

dh-group

Configures the IKEv2 IKESA Diffie-Hellman related parameters.

1

Configures the Diffie-Hellman Group 1, 768-bit MODP Group.

14

Configures the Diffie-Hellman 14, 2048-bit MODP Group.

2

Configures the Diffie-Hellman 2, 1024-bit MODP Group.

5

Configures the Diffie-Hellman 5, 1546-bit MODP Group.

reuse

Configures the reuse responders key-pair for DH group(s).

+

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

source-based threshold-upper *threshold_upper_value* **threshold-lower** *threshold_lower_value* **poll-timer-duration** *poll_timer_duration_value*:

Configures the IKEv2 DDoS mitigation parameters for INIT Floods applicable at source IP address level.

threshold-upper *threshold_upper_value*: Configures upper threshold value for INIT floods, after which alarm will be raised. *threshold_upper_value* must be an integer from 100 to 4294967295. Default: 10000.

threshold-lower *threshold_lower_value*: Configures lower threshold value for INIT floods, after which alarm will be cleared. *threshold_lower_value* must be an integer from 50 to 4294967294. Default: 5000.

poll-timer-duration *poll_timer_duration_value*: Configures IKEv2 DDoS INIT Floods timer duration in seconds. *poll_timer_duration_value* must be an integer from 30 to 3600. Default: 60 seconds.

system-based threshold-upper *threshold_upper_value* **threshold-lower** *threshold_lower_value* **poll-timer-duration** *poll_timer_duration_value*:

Configures the IKEv2 DDoS mitigation parameters for INIT Floods applicable at system level.

threshold-upper *threshold_upper_value*: Configures the upper threshold value for INIT floods, after which alarm will be raised. *threshold_upper_value* must be an integer from 1000 to 4294967295. Default: 100000.

threshold-lower *threshold_lower_value*: Configures the lower threshold value for INIT floods, after which alarm will be cleared. *threshold_lower_value* must be an integer from 500 to 4294967294. Default: 50000.

poll-timer-duration *poll_timer_duration_value*: Configures the IKEv2 DDoS INIT floods timer duration in seconds. *poll_timer_duration_value* must be an integer from 60 to 3600. Default: 60 seconds.

transform-set *transform_set_name*

Configure an IKEv2 IKE Security Association Transform Set. This object encapsulates various IKEv2 IKE algorithm configurations which are required for establishing and IKEv2 IKE Security Assocation with a remote peer.

transform_set_name is the context level name to be used for the IKEv2 IKE Security Association Transform Set, which is a string of size 1 to 127.

Usage Guidelines

Use this command to create a new or enter an existing IKEv2 security association parameters set. A list of up to four separate transform-sets and three separate authentication method sets can be created.

Entering the command **transform-set** *transform_set_name* results in the following prompt:

```
[context_name]hostname(cfg-ctx-ikev2ikesa-tran-set)#
```

IKEv2 Security Association Configuration Mode commands are defined in the *IKEv2 Security Association Configuration Mode Commands* chapter.

Example

The following command configures an IKEv2 security association transform set called *ikesa3* and enters the IKEv2 Security Association Configuration Mode:

```
ikev2-ikesa transform-set ikesa3
```

ims-auth-service

This command enables the creation, configuration or deletion of an IMS authorization service in the current context.

Product

GGSN

HA

IPSG

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

ims-auth-service *auth_svc_name* **[-noconfirm]**
{ no | default } ims-auth-service *auth_svc_name*

no

Deletes the specified IMS authorization service within the current context.

default

Restores default state of IMS authorization service, disabled for a specific context.

auth_svc_name

Specifies name of the IMS authorization service as a unique alphanumeric string of 1 through 63 characters.

In releases prior to 18, a maximum of 16 authorization services can be configured globally in the system. There is also a system limit for the maximum number of total configured services. In 18 and later releases, up to a maximum of 30 IMS authorization service profiles can be configured within the system.

Important Service names must be unique across all contexts within the system.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines Use this command to create/configure/delete an IMS authorization service for Gx interface support in the current context.

Entering this command results in the following prompt:

[*context_name*]*hostname*(config-imsa-service)

IMS authorization Service Configuration commands are described in the *IMS Authorization Service Configuration Mode Commands* chapter.

Important Whenever a new ims-auth-serv is configured using an endpoint that is used by another ims-auth-serv, then the diabase callbacks are overwritten with values of the new IMSA service. This is a limitation on the system to register only one application per endpoint. So, multiple IMSA services registering with same endpoint may not work properly. If such scenario occurs, configure a different endpoint name for the IMSA service being used and then remove and re-configure the IMSA service used.

Example

The following command configures an IMS authorization service named *ims_interface1* within the current context:

```
ims-auth-service ims_interface1
```

ims-sh-service

Creates the specified IP Multimedia Subsystem (IMS) Sh service name to allow configuration of an Sh service.

Product PDIF

SCM

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
ims-sh-service name
no ims-sh-service name
```

no

Removes a previously configured IMS-Sh-service.

name

Specifies the name of the IMS-Sh-service to be configured as an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines The IMS-Sh-service is named in the pdif-service and/or cscf-service. Use this command to enter the IMS Sh Service Configuration Mode.

Entering this command results in the following prompt:

[*context_name*]*hostname*(config-ims-sh-service)#

IMS Sh Service Configuration Mode commands are defined in the *IMS Sh Service Configuration Mode Commands* chapter in this guide.

Example

The following example creates or enters an IMS Sh service named *ims-1*:

```
ims-sh-service ims-1
```

inspector

Configures a context-level inspector account within the current context.

Product All

Privilege Security Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
inspector user_name [ encrypted ] [ nopassword ] password password [ ecs | noecs ] [ expiry-date date_time ] [ li-administration ] [ noconsole ] [ noecs ] [ timeout-absolute abs_seconds ] [ timeout-min-absolute abs_minutes ] [ timeout-idle timeout_duration ] [ timeout-min-idle idle_minutes ][ exp-grace-interval days][ exp-warn-interval days][ no-exp-grace-interval ][ no-exp-warn-interval ]
no inspector user_name
```

no

Removes a previously configured inspector account.

user_name

Specifies a name for the context-level inspector account as an alphanumeric string of 1 through 32 characters.

[encrypted] password *password*

Specifies the password to use for the user which is being given context-level inspector privileges within the current context. The encrypted keyword indicates the password specified uses encryption.

password is 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 system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the password keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

[nopassword]

This option allows you to create an inspector without an associated password. Enable this option when using ssh public keys (**authorized key** command in SSH Configuration mode) as a sole means of authentication. When enabled this option prevents someone from using an inspector password to gain access to the user account.

ecs | noecs

Default: **noecs**

ecs: Permits the specific user to access ACS-specific configuration commands.

noecs: Prevents the specific user to access ACS-specific configuration commands.

expiry-date *date_time*

Specifies the date and time that this account expires. Enter the date and time in the format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss.

Where YYYY is the year, MM is the month, DD is the day of the month, HH is the hour, mm is minutes, and ss is seconds.

li-administration

Refer to the *Lawful Intercept Configuration Guide* for a description of this parameter.

noconsole

Disables user access to a Console line.



Note The Global Configuration mode **local-user allow-aaa-authentication noconsole** command takes precedence in a normal (non-Trusted) StarOS build. In this case, all AAA-based users cannot access a Console line.

timeout-absolute *abs_seconds*

This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.

Specifies the maximum amount of time (in seconds) the context-level inspector may have a session active before the session is forcibly terminated. *abs_seconds* must be an integer from 0 through 300000000. The value 0 disables the absolute timeout. Default: 0

timeout-min-absolute *abs_minutes*

Specifies the maximum amount of time (in minutes) the context-level inspector may have a session active before the session is forcibly terminated. *abs_minutes* must be an integer from 0 through 525600 (365 days). The value 0 disables the absolute timeout. Default: 0

timeout-idle *timeout_duration*

This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.

Specifies the maximum amount of idle time (in seconds) the context-level inspector may have a session active before the session is terminated. *timeout_duration* must be an integer from 0 through 300000000. The value 0 disables the idle timeout. Default: 0

timeout-min-idle *idle_minutes*

Specifies the maximum amount of idle time (in minutes) the context-level inspector may have a session active before the session is terminated. *idle_minutes* must be an integer from 0 through 525600 (365 days). The value 0 disables the idle timeout. Default: 0

Usage Guidelines

Create new context-level inspector or modify existing inspector's options, in particular, the timeout values.

Inspector users have minimal read-only privileges. Refer to the *Command Line Interface Overview* chapter for more information.



Important A maximum of 128 administrative users and/or subscribers may be locally configured per context.

[max-age *days*]

Defines the maximum age of a user password before it has to be changed. **max-age** is the replacement for **expiry-date**.

[no-max-age]

This parameter ensures that password never expires (these are non expiring passwords).

exp-warn-interval *days*

Impends password expiry warning interval in days. There is no default value at per user level. If any of the value is specified, Context global values are considered.

For example:

```
inspector trexpac111 password pass@1234
```

In the previous example, there are no values for expiry, grace, and warn are provided. In this case, Global values for both of them will be considered.

[no-exp-warn-interval]

Disables impending password expiry warnings .

exp-grace-interval *days*

Specifies password expiry grace interval in days. Default = 3 days after expiry.

[no-exp-grace-interval]

Disables grace period of expired password.

Example

The following command creates a context-level inspector account named *user1*:

```
inspector user1 password secretPassword
```

The following command removes a context-level inspector account named *user1*:

```
no inspector user1
```

Example

The following command shows the notifications you will receive if the password is not reset before the expiration date:

inspector *user_name* **password** *password* **[max-age** *days***][password-exp-grace-interval** *days***][password-exp-grace-interval** *days***]**

```
login: xxx
password: xxx
1. <Normal>
# <you are logged in>

2. <When in warning period>
Warning: Your password is about to expire in 0 days.
We recommend you to change password after login.
Logins are not allowed without acknowleding this.
Do you wish to continue [y/n] (times out in 30 seconds) :

3.<when in grace period>
Your password has expired
Current password:
New password:
Repeat new password:

4. <after the grace period>
Password Expired (even beyond grace period, if configured). Contact Security Administrator
 to reset password
```

interface

Creates or deletes an interface or specifies an existing interface. By identifying an interface, the mode changes to configure this interface in the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

interface *name* **[broadcast | loopback | point-to-point | tunnel | unnumbered]**
no interface *name*

no

Removes the specified interface.

name

Specifies the name of the interface to configure. If *name* does not refer to an existing interface, the new interface is created if resources allow. *name* is an alphanumeric string of 1 through 79 characters.

broadcast

Creates an Ethernet broadcast (IP) interface and enters the Ethernet Configuration Mode. Default: Enabled

Important Refer to the *Ethernet Interface Configuration Mode Command* chapter for more information.

loopback

Creates an internal IP address that is always UP, is not bound to any physical card/port, and can be reached by any interface configured in the current context. As a loopback interface uses all available physical ports, this type of interface is particularly useful for load-balancing. The interface must be configured for loopback when configuring Interchassis Session Recovery (ICSR). A total of 256 loopback interfaces can be configured. Default: Disabled

This loopback option is not used to setup a diagnostic test port so it should not be confused with the loopback option used in the various card/port configuration modes.

Important Refer to the *Loopback Interface Configuration Mode Command* chapter for more information.

point-to-point

Creates a permanent virtual connection (PVC) in the current context and enters the PVC Configuration Mode. Currently, this type of interface is only used with an optical (ATM) line card.



Important Refer to the *PVC Interface Configuration Mode Command* chapter for more information.

tunnel

Creates a tunnel interface to support the various tunnel interfaces. Currently only IPv6-over-IPv4 and GRE tunnel interfaces are supported.



Important Refer to the *Tunnel Interface Configuration Mode Commands* chapter for more information.

unnumbered

Creates an unnumbered IP interface within the 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.



Important Refer to the *Unnumbered Interface Configuration Mode Commands* chapter for more information.

Usage Guidelines

Use this command to enter or create the interface configuration mode for an existing interface or for a newly defined interface. This command is also used to remove an existing interface when it longer is needed.



Important If no keyword is specified, broadcast is assumed and the interface is Ethernet by default.

For IPv6-over-IPv4 or GRE tunneling, you need to specify the interface type as **tunnel**.

Example

The following command enters the Ethernet Interface Configuration Mode creating the interface *sampleService*, if necessary:

```
interface sampleInterface
```

The following command removes *sampleService* as being a defined interface:

```
no interface sampleInterface
```

The following command enters the Tunnel Interface Configuration Mode creating the interface *GRE_tunnel1*, if necessary:

```
interface GRE_tunnel1 tunnel
```

ip access-group

Configures an access group with an Access Control List (ACL) for IP traffic for the current context. The Context-level ACL is applied only to outgoing packets.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
ip access-group name [ in | out ] [ priority_value ]
no ip access-group name [ in | out ]
```

no

Indicates the specified ACL rule is to be removed from the group.

name

Specifies the ACL rule to be added/removed from the group.

In Release 8.1 and later, *name* is an alphanumeric string of 1 through 47 characters.

In Release 8.0, *name* is an alphanumeric string of 1 through 79 characters.



Important Up to eight ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 256-rule limit for the context.

in | out

The **in** and **out** keywords are deprecated and are only present for backward compatibility. The Context-level ACL are applied only to outgoing packets.

priority_value

Specifies the priority of the access group. 0 is the highest priority. If *priority_value* is not specified, the priority is set to 0. *priority_value* must be an integer from 0 through 4294967295. Default: 0

If access groups in the list have the same priority, the last one entered is used first.

Usage Guidelines

Use this command to add IP access lists (refer to the **ip access-list** command) configured with in the same context to an ACL group.

Refer to the *Access Control Lists* appendix of the *System Administration Guide* for more information on ACLs.

Example

The following commands add *sampleGroup* to the context-level ACL with a priority of *0*:

```
ip access-group sampleGroup 0
```

ip access-list

Create, configure, or delete an IP Access List in the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

ip access-list *name*
{ default | no } ip access-list *name*

default

Sets the context's default access control list to that specified by *name*.

no

Removes the specified access list.

name

Specifies the access list name.

name is an alphanumeric string of 1 through 47 characters.

If the named access list does not exist, it is created, and the CLI mode changes to the ACL Configuration Mode, wherein the access list can be configured.

If the named access list already exists, the CLI mode changes to the ACL Configuration Mode, wherein the access list can be reconfigured.

Usage Guidelines

Executing this command enters the ACL Configuration Mode in which rules and criteria are defined for the ACL.

Important A maximum of 256 rules (21.4 and higher releases) or 128 rules (releases prior to 21.4) can be configured per ACL. The maximum number of ACLs that can be configured per context is limited by the amount of available memory in the VPN Manager software task; it is typically less then 200.

Refer to the *Access Control Lists* appendix of the *System Administration Guide* for more information on ACLs.

Example

The following command creates an access list named *sampleList*, and enters the ACL Configuration Mode:

```
ip access-list sampleList
```

ip arp

Configures the allocation retention priority (ARP) options for the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
ip arp ip_address mac_address [ vrf vrf_name ]
no ip arp ip_address mac_address
```

no

Removes the ARP configuration data for the specified IP address from the configuration.

ip_address

Specifies the IP address for which to configure the ARP options where *ip_address* is an IP address expressed in IPv4 dotted-decimal notation.

mac_address

Specifies the media-specific access control layer address for the IP address. *mac_address* must be specified as a an 6-byte hexadecimal number with each byte separated by a colon, for example., "AA:12:bb:34:f5:0E".

vrf *vrf_name*

Associates a Virtual Routing and Forwarding (VRF) context with this static ARP entry.

vrf_name is name of a preconfigured virtual routing and forwarding (VRF) context configured in *Context Configuration Mode* via the **ip vrf** command.

Usage Guidelines

Manage the IP address mapping which is a logical/virtual identifier to the more lower layer addressing used for address resolution in ICMP messages.

For tunnel-based interface, network IP pool can have overlapping ip-addresses across Verve. To manage it adding a preconfigured VRF context is required to associate with an static ARP entry. By default, the ARP is added in the given context. If the VRF name is specified, then the ARP is added to the VRF ARP table.

Example

The following commands set the IP and MAC address for the current context then remove it from the configuration:

```
ip arp 10.2.3.4 F1:E2:D4:C5:B6:A7
no ip arp 10.2.3.4
```

The following commands set the IP and MAC address for a VRF context *vrf1* in the configuration:

```
ip arp 10.2.3.4 F1:E2:D4:C5:B6:A7 vrf vrf1
```

ip as-path access-list

Defines Border Gateway Protocol (BGP) Autonomous System (AS) Path access lists.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] ip as-path access-list` *`list_name`* **`[ { deny | permit } `** *`reg_expr`* **`]`**

no

Remove the specified regular expression from the AS path access list.

list_name

Specifies the name of an AS path list as an alphanumeric string of 1 through 79 characters.

{ deny | permit }

deny: Denies access to AS paths that match the regular expression.

permit: Allows access to AS paths that match the regular expression.

reg_expr

A regular expression to define the AS paths to match. *reg_expr* is an alphanumeric string of 1 through 254 characters.

Important The **?** (question mark) character is not supported in regular expressions for this command.

Usage Guidelines Use this command to define AS path access lists for the BGP router in the current context. The chassis supports a maximum of 64 access lists per context.

Example

The following command creates an AS access list named *ASlist1* and permits access to AS paths:

```
ip as-path access-list ASlist1 permit
```

ip community-list

Configures filtering via a BGP community list. To filter by a BGP community, you must then match the community in a route-map.

Product All products supporting BGP routing

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
ip community-list { named named_list | standard identifier } { deny | permit
 } { internet | local-AS | no-advertise | no-export | value AS-community_number
 AS-community_number AS-community_number ... }
{ internet | local-AS | no-advertise | no-export | value AS-community_number
 AS-community_number AS-community_number ...}
{ internet | local-AS | no-advertise | no-export | value AS-community_number
 AS-community_number AS-community_number ...}
no ip community-list { named named_list | standard identifier } { deny |
permit } { internet | local-AS | no-advertise | no-export | value
AS-community_number }
```

no

Entering **no ip community-list** with a permit/deny clause deletes the matching community-list entry. Entering **no ip community-list** without a permit/deny clause deletes all the entries belonging to a 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.

{ deny | permit }

Specifies whether this community will deny or permit access to a specified destination.

{ internet | local-AS | no-advertise | no-export | value *AS-community_number*

Specifies the destinations to deny or permit 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.
- **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 AS community numbers separated by spaces.

Usage Guidelines

Configures filtering via a BGP community list. To filter by a BGP community, you must then match the community in a route-map.

Multiple community-list entries can be attached to a community-list by adding multiple permit or deny clauses for various community strings. Up to 64 community-lists can be configured in a context.

The communities-list is a way to group destinations into communities and apply routing decisions based on the communities. This method simplifies the configuration of a BGP speaker that controls distribution of routing information.

A community is a group of destinations that share some common attribute. Each destination can belong to multiple communities. Autonomous system administrators define to which communities a destination belongs.

Example

The following command specifies that community list number 5 will permit access to AS destination 200:5.

```
ip community-list standard 5 permit value 200:5
```

ip dns-proxy source-address

Enables the proxy DNS functionality and identifies this context as the destination context for all redirected DNS requests.



Important This command must be entered in the destination context for the subscriber. If there are multiple destination contexts for different subscribers, the command must be entered in each context.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **`[ no ] ip dns-proxy source-address`** *ip_address*

no

Removes the address in this context as a destination for redirected DNS packets.

ip_address

Specifies an interface in this context used for redirected DNS packets. *ip_address* must be entered using IPv4 dotted-decimal notation.

Usage Guidelines Use this command to identify the interface in this context where redirected DNS packets are sent to the home DNS. The system uses this address as the source address of the DNS packets when forwarding the intercepted DNS request to the home DNS server. For a more detailed explanation of the proxy DNS intercept feature, see the **proxy-dns intercept-list** command.

Example

The following command identifies an interface with an address of *209.165.200.255* in a destination context where the system forwards all intercepted DNS requests:

```
ip dns-proxy source-address 209.165.200.255
```

ip domain-lookup

Enables or disables domain name lookup via domain name servers for the current context.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
ip domain-lookup
no ip domain-lookup
```

no

Disables domain name lookup.

Usage Guidelines

Domain name look up is necessary if the subscribers configured for the context are to be allowed to use logical host names for services which requires the host name resolution via DNS.

Example

```
ip domain-lookup
no ip domain-lookup
```

ip domain-name

Configures or removes a logical domain name for the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] ip domain-name *name*

no

Indicates the logical domain name for the current context is to be removed.

name

Specifies the logical domain name to use for domain name server address resolution. *name* is an alphanumeric string of 1 through 1023 characters formatted to be a valid IP domain name.

Usage Guidelines

Set a logical domain name if the context is to be accessed by logical domain name in addition to direct IP address.

Example

```
ip domain-name sampleName.org
```

ip extcommunity-list

Configures route target filtering via a BGP extended community list. To filter by a BGP extended community, you must then match the extended community in a route-map.

Product

All products supporting BGP routing

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
ip extcommunity-list { named named_list | standard identifier } { deny |
permit } rt rt_number rt_number rt_number ...
no ip community-list { named named_list | standard identifier } { deny |
permit } rt rt_number
```

no

Entering **no ip extcommunity-list** with a permit/deny clause deletes the matching extended community-list entry. Entering **no ip extcommunity-list** without a permit/deny clause deletes all the entries belonging to an extended community-list.

named *named_list*

Specifies the name of an extended community list as an alphanumeric string of 1 through 79 characters.

standard *identifier*

Specifies the name of an extended community list as an integer from 1 through 99.

{ deny | permit }

Specifies whether this community will deny or permit access to a specific route target.

rt *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

Configures filtering via a BGP extended community list. To filter by a BGP extended community, you must then match the community in a route-map.

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.

Multiple extended community-list entries can be attached to an extended community-list by adding multiple permit or deny clauses for various extended community strings. Up to 64 extended community-lists can be configured in a context.

Example

The following command specifies that extended community list number 78 will deny access to route target 200:5:

```
ip extcommunity-list standard 78 deny rt 200:20
```

ip forward

Configures an IP forwarding policy to forward outgoing pool packets whose flow lookup fails to the default-gateway.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] ip forward outbound unused-pool-dest-address default-gateway
```

no

Disables forwarding to the default gateway.

outbound unused-pool-dest-address default-gateway

Enables forwarding to the default gateway.

Usage Guidelines

Use this command to set an IP forwarding policy that forwards outgoing pool packets whose flow lookup fails to the default gateway. By default, the behavior is to either send an ICMP Unreachable message or to discard the packet depending on the configuration of the IP pool.

Pool packets coming from the line card or MIO card whose flow lookup fails are discarded or ICMP unreachable is sent irrespective of whether this command is configured or not.



Note While this CLI is available on the ASR 5500, its functionality is not supported. Therefore, if the CLI is configured, it does not affect or alter the IP forwarding behaviour.

Example

To enable this functionality, enter the following command:

```
ip forward outbound unused-pool-dest-address default-gateway
```

To disable this functionality, enter the following command:

```
no ip forward outbound unused-pool-dest-address default-gateway
```

ip guarantee

Enables and disables local switching of framed route packets.

Product

GGSN

P-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[no] ip guarantee framed-route local-switching
```

no

Disables local switching of framed route packets.

framed-route local-switching

Enables local switching of framed route packets. By default, this functionality is disabled.

Usage Guidelines

Use this command to enable and disable local switching of framed route packets. This functionality will be applicable only when there are some NEMO/framed route sessions in a context.

Example

The following command enables local switching of framed route packets:

```
ip guarantee framed-route local-switching
```

ip identification packet-size-threshold

Configures the packet size above which system will assign unique IP header identification.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

ip identification packet-size-threshold *size*
default ip identification packet-size-threshold

default

Restores default value of 576 bytes to IP packet size for fragmentation threshold.

size

Specifies the size of IP packet in bytes above which system will assign unique IP header identification for system generated IP encapsulation headers (such as MIP data tunnel). *size* is an integer from 0 through 2000. Default: 576

Usage Guidelines

This configuration is used to set the upper limit of the IP packet size. All packets above that size limit will be considered "fragmentable", and an unique non-zero identifier will be assigned.

Example

The following commands set the IP packet size to 1024 bytes as threshold. above this limit system will assign unique IP header identification for system generated IP encapsulation headers:

```
ip identification packet-size-threshold 1023
```

ip igmp profile

Configures an Internet Group Management Protocol (IGMP) profile and moves to the IGMP Profile Configuration mode.

Product

PDSN

GGSN

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] ip igmp profile *name*

no

Removes the specified IGMP profile.

name

Specifies the name of an IGMP profile as an alphanumeric string of 1 through 63 characters. If this is not the name of an existing profile, you are prompted to create the new profile.

Usage Guidelines

Configure and existing IGMP profile or create a new one. When this command is executed you are moved to the IGMP Profile Configuration mode. For additional information, refer to the *IGMP Profile Configuration Mode Commands* chapter.

Example

```
ip igmp profile default
```

ip localhost

Configures or removes the static local host logical name to IP address mapping for the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] ip localhost *name ip_address*

no

Specifies that the static mapping must be removed.

name

Specifies the logical host name (DNS) for the local machine on which the current context resides. *name* is an alphanumeric string of 1 through 1023 characters formatted to be a valid IP host name.

ip_address

Specifies the IP address for the static mapping. *ip_address* must be expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage Guidelines

Avoid excessive DNS lookups across the network by statically mapping the logical host name to the local host's context.

Example

```
ip localhost localHostName 10.2.3.4
no ip localhost localHostName 10.2.3.4
```

ip name-servers

Modifies the list of domain name servers the current context may use for logical host name resolution.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
ip name-servers ip_address secondary_ip_address[third_ip_address]
no ip name-servers ip_address
```

no

Indicates the name server specified is to be removed from the list of name servers for the current context.

ip_address

Specifies the IP address of a domain name server using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

secondary_ip_address

Specifies the IP address of a secondary domain name server using either IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

third_ip_address

Specifies the IP address of a third domain name server using either IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. (VPC only)

Usage Guidelines

Manage the list of name servers the current context may use in resolving logical host names.

Note When this CLI configuration is changed, the DNS client is reinitialized and the **cache ttl negative** value is reset to the default value if **no cache ttl negative** is configured for the DNS client in the context.. Therefore, check and reconfigure the **no cache ttl negative** CLI after the **ip name-servers** CLI configuration is changed on the node.

The DNS can be specified at the Context level in Context configuration as well as at the APN level in APN Configuration Mode with **dns** and **ipv6 dns** commands, or it can be received from AAA server.

When DNS is requested in PCO configuration, the following preference will be followed for DNS value:

1. DNS Values received from LNS have the first preference.
2. DNS values received from RADIUS Server has the second preference.
3. DNS values locally configured with APN with **dns** and **ipv6 dns** commands has the third preference.
4. DNS values configured at context level has the last preference.

Important The same preference would be applicable for the NBNS servers to be negotiated via ICPC with the LNS.

Example

```
ip name-servers 10.2.3.4
```

ip pool

Enables creation, configuration or deletion of IP address pools in the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

ip pool *pool_name* { *ip_address/subnet_mask* | *ip_address_mask_combo* | **range** *start_ip_address end_ip_address* } [**address-hold-timer** *address_hold_timer*] [**address-quarantine-timer** *seconds*] [**advertise-if-used**] [**alert-threshold** [**group-available** | **pool-free** | **pool-hold** | **pool-release** | **pool-used** | **pool-usable** | **pool-usable-final**] *low_thresh* [**clear** *high_thresh*]] [**explicit-route-advertise**] [**group-name** *group_name*] [**include-nw-bcast**] [**napt-users-per-ip-address** *users_per_ip* [**alert-threshold** { { **pool-free** | **pool-hold** | **pool-release** | **pool-used** } *low_thresh* [**clear** *high_thresh*] } +] [

max-chunks-per-user *max_chunks_per_user* [**nat-binding-timer** *nat_binding_timer*] [**nat-pkt-drop-threshold** *high_thresh* [**clear** *low_thresh*]] [**nexthop-forwarding-address** *ip_address*] [**on-demand**] [**port-chunk-size** *port_chunk_size*] [**port-chunk-threshold** *port_chunk_threshold*] [**send-nat-binding-update**] +] [**nat** *priority*] [**nat-one-to-one** [**alert-threshold** { { **pool-free** | **pool-hold** | **pool-release** | **pool-used** } *low_thresh* [**clear** *high_thresh*] } +] [**nat-binding-timer** *nat_binding_timer*] [**nat-pkt-drop-threshold** *high_thresh* [**clear** *low_thresh*]] [**nexthop-forwarding-address** *ip_address*] [**on-demand**] [**send-nat-binding-update**] +] [**nat-realm users-per-nat-ip-address** *users* [**on-demand** [**address-hold-timer** *address_hold_timer*]]] [**nexthop-forwarding-address** *ip_address* [**overlap vlanid** *vlan_id*] [**respond-icmp-echo** *ip_address*]] [**nw-reachability server** *server_name*] [**policy allow-static-allocation**] [**framed-route-vrf-list** *vrf_list_name*] [**pool-route** *ip_address/ip_mask*] [**private** *priority*] [**public** *priority*] [**resource** *priority*] [**send-icmp-dest-unreachable**] [**skip-nat-subscriber-ip-check**] [**srp-activate**] [**subscriber-gw-address** *ip_address*] [**static**] [**suppress-switchover-arps**] [**tag** { **none** | **pdif-setup-addr** }] [**unicast-gratuitous-arp-address** *ip_address*] [**vrf** *vrf_name* { [**mpls-label input** *in_label_value* | **output** *out_label_value1* [*out_label_value2*] }] [**framed-route-vrflist**] +

no ip pool *pool_name* **[address-hold-timer] [address-quarantine-timer] [advertise-if-used] [alert-threshold [[group-available] [pool-free] [pool-hold] [pool-release] [pool-used] +] [explicit-route-advertise] [group-name] [include-nw-bcast] [nexthop-forwarding-address [respond-icmp-echo]] [nw-reachability server] [policy allow-static-allocation] [framed-route-vrf-list] [send-icmp-dest-unreachable] [skip-nat-subscriber-ip-check] [srp-activate] [subscriber-gw-address] [suppress-switchover-arps] [tag { none | pdif-setup-addr }] [unicast-gratuitous-arp-address] + [send-nat-binding-update] [framed-route-vrflist]**

no

Removes the specified IP address pool from the current context's configuration, or disables the specified option(s) for the specified IP pool.

no alert-threshold

This command without any optional keywords disables all alert thresholds.

name

Specifies the logical name of the IP address pool. *name* must be an alphanumeric string of 1 through 31 characters.



Important An error message displays if the **ip** *pool name* and the *group name* in the configuration are the same. An error message displays if the **ip** *pool name* or *group name* are already used in the context.

Important Adding the IP Pool command and the Busyout command of the same IP Pool at the same time creates a race condition. To avoid the issues, run the IP Pool command and Busyout command separately.

ip_address

Specifies the beginning IP address of the IP address pool using IPv4 dotted-decimal.

subnet_mask

Specifies the IP address mask bits to determine the number of IP addresses in the pool. *ip_mask* must be specified using IPv4 dotted-decimal notation.

1 bits in the *ip_mask* indicate that bit position in the *ip_address* must also have a value of 1.

0 bits in the *ip_mask* indicate that bit position in the *ip_address* does not need to match – the bit can be either a 0 or a 1.

For example, if the IP address and mask are specified as *172.168.10.0* and *255.255.255.224*, respectively, the pool will contain IP addresses in the range *172.168.10.0* through *172.168.10.31* for a total of 32 addresses.

Note

- The valid prefix length for IPv6 pool is 32 to 63.
- The static and dynamic pools have further restrictions on prefix length.
  - Pool size length <= 24 (for a static pool) => valid prefix length is from 39 to 63.
  - Pool size length <= 20 (for a dynamic pool) => valid prefix length is from 43 to 63
- Further, each platform has a restriction on the maximum number of dynamic IPv6 addresses and maximum number of static IPv6 addresses supported per context.

ip_address_mask_combo

Specifies a combined IP address subnet mask bits to indicate what IP addresses the route applies to. *ip_address_mask_combo* must be specified using CIDR notation where the IP address is specified using IPv4 dotted-decimal notation and the mask bits are a numeric value which is the number of bits in the subnet mask.

range *start_ip_address end_ip_address*

Specifies the IP addresses for the IP pool as a range of addresses.

start_ip_address specifies the beginning of the range of addresses for the IP pool.

end_ip_address specifies the end of the range of addresses for the IP pool.

The IP address range must be specified using IPv4 dotted-decimal notation.

For example, if *start_ip_address* is specified as *172.168.10.0* and *end_ip_address* is specified as *172.168.10.31* the IP pool will contain addresses in the range *172.168.10.0* through *172.168.10.31* for a total of 32 addresses.

private [*priority*]

Address pool may only be used by mobile stations which have requested an IP address from a specified pool. When private pools are part of an IP pool group, they are used in a priority order according to the precedence setting. *priority* must be an integer from 0 through 10 with 0 being the highest priority. The default value is 0.

public [*priority*]

Address pool is used in priority order for assigning IP addresses to mobile stations which have not requested a specific address pool. *priority* must be an integer from 0 through 10 with 0 being the highest priority. The default value is 0.

static

Designates local IP address pool to statically assign pooled addresses.

Important The keyword **static** must be used for DHCP served IP addresses.

tag { none | pdif-setup-addr }

Default: **none**

none: default tag for all IP address pools

pdif-setup-addr:pool with this tag should only be used for PDIF calls.

address-hold-timer *seconds*

When this is enabled, and an active subscriber is disconnected, the IP address is held or considered still in use, and is not returned to the free state until the address-hold-timer expires. This enables subscribers who reconnect within the length of time specified (in seconds) to obtain the same IP address from the IP pool.

seconds is the time in seconds and must be an integer from 0 through 31556926.

Important *For releases prior to 20.0*, a change made to the IP pool hold timer takes immediate effect on existing addresses currently on hold. Timeouts are adjusted to align with the new value. *For releases after 20.0*, the new timeout value will only be applied to addresses which are put on hold in the future. Timeouts for addresses currently in the hold state are not modified. They will timeout using the original timeout value.

Important Currently, the address-hold-timer only supports IPv4 addresses.

address-quarantine-timer *seconds*

Specifies the timer value in seconds for an address quarantine timer as an integer from 20 through 86400. This timer cannot be configured with an address-hold-timer in the same pool.

The IP pool address-quarantine-timer is a mechanism to busy out a released IP address for a specified interval. This prevents an IP address from being reused until the quarantine timer expires.

Each IP pool can be configured with a timer value that determines how long a recently released address will be held in quarantine before being freed. When the timer has expired, the address is returned to the list of free addresses, to be allocated again to a new subscriber. Any address that has been released, but for which the address-quarantine-timer has not expired, is still considered to be in use for the purposes of allocation. If a subscriber tries to reconnect while the address-quarantine timer is armed, even though it is the same subscriber ID, the subscriber does not get the same address.

advertise-if-used

Advertises to the peer routes only if addresses are being used in pool.

alert-threshold { group-available | pool-free | pool-hold | pool-release | pool-used | pool-usable | pool-usable-final } *low_thresh* [clear *high_thresh*]

Default: All thresholds are disabled.

Configures IP address pool-level utilization thresholds. These thresholds take precedence over context-level IP pool thresholds.

group-available: Set an alert based on the available percentage of IP addresses for the entire IP pool group.

pool-free: Set an alert based on the percentage of IP addresses that are unassigned in this IP pool.

pool-hold: Set an alert based on the percentage of IP addresses from this IP pool that are on hold.

pool-release: Set an alert based on the percentage of IP addresses from this IP pool that are in the release state.

pool-used: This command sets an alert based on the percentage of IP addresses that have been assigned from this IP pool.

pool-usable: This command sets IP pool usable pre threshold state as either free or release.

pool-usable-final: Thiss command sets the IP pool usable final threshold state as either free or release.



Important Refer to the **threshold available-ip-pool-group** and **threshold monitoring** commands in this chapter for additional information on IP pool utilization thresholding.

low_thresh: The IP pool utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer between 0 and 100.

clear *high_thresh*: The IP pool utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm is generated. It may be configured as an integer between 0 and 100.



Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

group-name *group_name*

Assigns one or more preconfigured IP pools to the IP pool group. *group_name* is case sensitive and must be an alphanumeric string of 1 through 31 characters. One or more IP pool groups are assigned to a context and one IP pool group consists one or more IP pool(s).

IP pool group name is used in place of an IP pool name. When specifying a desired pool group in a configuration the IP pool with the highest precedence is used first. When that IP pool's addresses are exhausted the pool with the next highest precedence is used.

include-nw-bcast

Allows pools to include the classful network and broadcast addresses that are usually excluded when a pool crosses the classful network boundaries.

To remove the **include-nw-bcast** option from the ip pool, use the **no ip pool test include-nw-bcast** command.

napt-users-per-ip-address *users_per_ip* [alert-threshold { { pool-free | pool-hold | pool-release | pool-used } *low_thresh* [clear *high_thresh*] } +] [max-chunks-per-user *max_chunks_per_user* [nat-binding-timer *nat_binding_timer* port-chunk-hold-timer *port_chunk-hold_timeout*] [nat-pkt-drop-threshold *high_thresh* [clear *low_thresh*]] [nexthop-forwarding-address *ip_address*] [on-demand] [port-chunk-size *port_chunk_size* [min-port-chunk-per-user *chunks*]] [port-chunk-threshold *port_chunk_threshold*] [send-nat-binding-update] +

Important In UMTS deployments this keyword is available in 9.0 and later releases. In CDMA deployments this keyword is available in 8.3 and later releases.

Important In UMTS deployments, on upgrading from Release 8.1 to Release 9.0, and in CDMA deployments, on upgrading from Release 8.1 to 8.3, all NAT realms configured in Release 8.1 using the **nat-realm** keyword must be reconfigured using either the **nat-one-to-one** (for one-to-one NAT realms) or the **napt-users-per-ip-address** (for many-to-one NAT realms) keywords.

Configures many-to-one NAT realms.

- *users_per_ip*: Specifies how many users can share a single NAT IP address.

  In 18 and earlier releases, *users_per_ip* must be an integer from 2 through 2016.

  In 19 and later releases: *users_per_ip* must be an integer from 2 through 8064.

- **alert-threshold**: Specifies the alert threshold for the pool:

Important Thresholds configured using the **alert-threshold** keyword are specific to the pool that they are configured in. Thresholds configured using the **threshold ip-pool-*** commands in the Context Configuration Mode apply to all IP pools in that context, and override the threshold configurations set within individual pools.

- **pool-free**: Percentage free alert threshold for this pool
- **pool-hold**: Percentage hold alert threshold for this pool

- **pool-release**: Percentage released alert threshold for this pool
- **pool-used**: Percentage used alert threshold for this pool
- *low_thresh*: The IP pool utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. *low_thresh* must be an integer from 0 through 100.
- **clear** *high_thresh*: The IP pool utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm is generated. *high_thresh* must be an integer from 0 through 100.



Important The *high_thresh* value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

- **max-chunks-per-user** *max_chunks_per_user*: Specifies the maximum number of port chunks to be allocated per subscriber in the many-to-one NAT pool.

  In 18 and earlier releases: *max_chunks_per_user* must be an integer from 1 through 2016.

  In 19 and later releases: *max_chunks_per_user* must be an integer from 1 through 8064.

  Default: 1

- **min-port-chunk-per-user***min_port-chunk_per_user*: Configures NAT Port minimum number of chunks per user for many-to-one NAT pool.

  In 21.23 and later releases: *max_chunks_per_user* must be an integer from 1 through 100.

- **nat-binding-timer** *binding_timer*: Specifies NAT Binding Timer for the NAT pool. *timer* must be an integer from 0 through 31556926. If set to 0, is disabled. Default: 0
- **port-chunk-hold-timer** *port_chunk-hold_timeout*: Configures timeout in seconds. The freed port chunk is reused in a napt IP pool. If either the value is set to 0 or this is not configured, then **nat-binding-timer** becomes effective. The **port-chunk-hold-timer** must be an integer from 0 through 31556926. By Default, it is disabled. Enable the port chunk hold timer with a non-zero value.



Note

- Configure NAT binding timer value while enabling port chunk hold timer feature.
- If the NAT binding timer is disabled and port-chunk-hold timer is configured, then all NAT port chunks will be released after port chunk hold timer expiry and NAT IP address will never be freed.
- Specify the value of the port chunk hold timeout as lesser than the NAT binding timeout value.
- Do not configure the port chunk hold timer to lesser than 2MSL .

- **nat-pkt-drop-threshold** *high_thresh* **[clear** *low_thresh* **]**: Specifies the NAT packet drop threshold in percentage (%).

high_thresh specifies the high NAT packet drop percentage threshold, and must be an integer from 0 through 100. Default: 0

clear *low_thresh* specifies the low NAT packet drop percentage threshold, and must be an integer from 0 through 100. Default: 0

- **nexthop-forwarding-address** *address*: Specifies the nexthop forwarding address for this pool. *address* must be an IPv4 or IPv6 address. If configured for a NAT pool, packets that are NATed using that NAT pool will be routed based on the configured nexthop address.



Important The **nexthop-forwarding-address** support for NAT IP pools is functional only in later releases of Release 9.0 and in 10.0 and later releases.



Important

- The minimum port chunk per user is only applicable to NAPT single-ip.
- **min-port-chunk-per-user** and **port-chunk-threshold** are mutually exclusive.

- **on-demand**: Specifies allocating IP when matching data traffic begins.
- **port-chunk-size** *size*: Specifies NAT port chunk size (number of NAT ports per chunk) for many-to-one NAT pool.

  In 18 and earlier releases: *size* must be an integer from 32 through 32256 (in multiples of 32).

  In 19 and later releases: *size* must be an integer from 8 through 32256 (in multiples of 8).



Important The **port-chunk-size** configuration is only available for many-to-one NAT pools.



Important The **port-chunk-size** must be a minimum of *64* with systems configured as an A-BG or P-CSCF.

- **port-chunk-threshold** *chunk_threshold*: Specifies NAT port chunk threshold in percentage of number of chunks for many-to-one NAT pool. *chunk_threshold* must be an integer from 1 through 100. Default: 100%



Important The **port-chunk-threshold** configuration is only available for many-to-one NAT pools.

- **send-nat-binding-update**: Specifies sending NAT binding updates to AAA for this realm. Default: Disabled



Important **send-nat-binding-update** is supported for both one-to-one and many-to-one realms.

The following IP pool configuration keywords can also be used in the many-to-one NAT pool configuration:

- **group-name** *group_name*: Specifies the pool group name. The grouping enables to bind discontiguous IP address blocks in individual NAT IP pools to a single pool group.

  This keyword is available for NAT pool configuration only in Release 10.0 and later.

  NAT pool and NAT pool group names must be unique.

  group_name is an alphanumeric string of 1 through 31 characters that is case sensitive.

- **srp-activate**

  Activates the IP pool for Interchassis Session Recovery (ICSR).

nat *priority*

Designates the IP address pool as a Network Address Translation (NAT) address pool.

priority specifies the priority of the NAT pool. 0 is the highest priority. If *priority* is not specified, the priority is set to 0.

Must be a value from 0 (default) to 10.

Important This functionality is currently supported for use with systems configured as an A-BG or P-CSCF.

nat-one-to-one [alert-threshold { { pool-free | pool-hold | pool-release | pool-used } *low_thresh* [clear *high_thresh*] } +] [nat-binding-timer *nat_binding_timer*] [nat-pkt-drop-threshold *high_thresh* [clear *low_thresh*]] [nexthop-forwarding-address *ip_address*] [on-demand] [send-nat-binding-update] +

Important In UMTS deployments this keyword is available in Release 9.0 and later releases. In CDMA deployments this keyword is available in Release 8.3 and later releases.

Important In UMTS deployments, on upgrading from Release 8.1 to Release 9.0, and in CDMA deployments, on upgrading from Release 8.1 to Release 8.3, all NAT realms configured in Release 8.1 using the **nat-realm** keyword must be reconfigured using either the **nat-one-to-one** (for one-to-one NAT realms) or the **napt-users-per-ip-address** (for many-to-one NAT realms) keywords.

Configures one-to-one NAT realm.

- **alert-threshold**: Specifies alert threshold for this pool:

Important Thresholds configured using the **alert-threshold** keyword are specific to the pool in which they are configured. Thresholds configured using the **thresholdip-pool *** commands in the Context Configuration Mode apply to all IP pools in the context, and override the threshold configurations set within individual pools.

- **pool-free**: Percentage free alert threshold for this pool

- **pool-hold**: Percentage hold alert threshold for this pool
- **pool-release**: Percentage released alert threshold for this pool
- **pool-used**: Percentage used alert threshold for this pool
- *low_thresh*: The IP pool utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. *low_thresh* must be an integer from 0 through 100.
- **clear** *high_thresh*: The IP pool utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm is generated. *high_thresh* must be an integer from 0 through 100.



Important The *high_thresh* value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

- **nat-binding-timer** *nat_binding_timer*: Specifies NAT Binding Timer for the NAT pool. *binding_timer* must be an integer from 0 through 31556926. If set to 0, is disabled.



Important For many-to-one NAT pools, the default NAT Binding Timer value is 60 seconds. For one-to-one NAT pools, it is 0. By default, the feature is disabled—the IP addresses/ port-chunks once allocated will never be freed.

- **nat-pkt-drop-threshold** *high_thresh* **[clear** *low_thresh* **]**: Specifies the NAT packet drop threshold in percentage (%).

  high_thresh specifies the high NAT packet drop percentage threshold, and must be an integer from 0 through 100. Default: 0

  clear *low_thresh* specifies the low NAT packet drop percentage threshold, and must be an integer from 0 through 100. Default: 0

- **nexthop-forwarding-address** *ip_address*: Specifies the nexthop forwarding address for this pool. *address* must be an IPv4 or IPv6 address. If configured for a NAT pool, packets that are NATed using that NAT pool will be routed based on the configured nexthop address.



Important The **nexthop-forwarding-address** support for NAT IP pools is functional only in later releases of Release9.0 and in Release 10.0 and later releases.

- **on-demand**: Specifies allocating IP address when matching data traffic begins.
- **send-nat-binding-update**: Specifies sending NAT binding updates to AAA for this realm. Default: Disabled



Important **send-nat-binding-update** is supported for both one-to-one and many-to-one realms.

The following IP pool configuration keywords can also be used in the one-to-one NAT pool configurations:

- **address-hold-timer** *address_hold_timer*
- **group-name** *group_name*: specifies the pool group name. The grouping enables to bind discontiguous IP address blocks in individual NAT IP pools to a single pool group. NAT pool and NAT pool group names must be unique. *group_name* is an alphanumeric string of 1 through 31 characters that is case sensitive. This keyword is available for NAT pool configuration only in StarOS 10.0 and later releases.
- **srp-activate**:Activates the IP pool for Interchassis Session Recovery (ICSR).

nat-realm users-per-nat-ip-address *users* [on-demand [address-hold-timer *address_hold_timer*]]

Important In UMTS deployments, the **nat-realm** keyword is only available in Release 8.1.

Important In Release 8.1, the NAT On-demand feature is not supported.

Important This functionality is currently supported for use with systems configured as an A-BG or P-CSCF.

Designates the IP address pool as a Network Address Translation (NAT) realm pool.

users-per-nat-ip-address *users*: specifies the number of users sharing a single NAT IP address as an integer from 1 through 5000.

on-demand: Specifies to allocate IP when matching data traffic begins.

address-hold-timer *address_hold_timer*: Specifies the address hold timer (in seconds) for this pool as an integer from 0 through 31556926. If set to 0, the address hold timer is disabled.

Important Currently, the address-hold-timer only supports IPv4 addresses.

nexthop-forwarding-address *ip_address*

A subscriber that is assigned an IP address from this pool is forwarded to the next hop gateway with the specified IP address. *ip_address*: Specifies the nexthop forwarding address for this pool. *address* must be an IPv4 or IPv6 address.

overlap vlan id *vlan_id*

When a nexthop forwarding address is configured, this keyword can be configured to enable over-lapping IP address pool support and associates the pool with the specified virtual LAN (VLAN). *vlan_id* is the identification number of a VLAN assigned to a physical port and can be configured to any integer from 1 through 4095.

For more information on configuring VLANs, refer to the *System Administration Guide*.



Important This functionality is currently supported for use with systems configured as an HA, or as a PDSN for Simple IP, or as a GGSN. This keyword can only be issued for pools of type private or static and must be associated with a different nexthop forwarding address and VLAN. A maximum of 256 over-lapping pools can be configured per context and a maximum of 256 over-lapping pools can be configured per HA or simple IPPDSN. For GGSNs, the total number of pools is limited by the number of VLANs defined but the maximum number per context is 256. Additional network considerations and configuration outside of the system maybe required.

nw-reachability server *server_name*

Binds the name of a configured network reachability server to the IP pool and enables network reachability detection for the IP pool. This takes precedence over any network reachability server settings in a subscriber configuration.

server_name: Specifies the name of a network reachable server that has been defined in the current context, expressed as an alphanumeric string of 1 through 16 characters.



Important Also see the following commands for more information: Refer to the **policy nw-reachability-fail** command in the HA Configuration Mode to configure the action that should be taken when network reachability fails. Refer to the **nw-reachability server** command in this chapter to configure network reachability servers. Refer to the **nw-reachability-server** command in the Subscriber Configuration Mode to bind a network reachability server to a specific subscriber.

respond-icmp-echo *ip_address*

Pings the first IP address from overlapping IP address pools.



Important In order for this functionality to work, all of the pools should contain an initial IP address that can be pinged.

resource

Specifies this IP pool as a resource pool. The IP addresses in resource pools may have IP addresses that also exist in other resource pools. IP addresses from a resource pool should not be used for IP connectivity within the system where the pool is defined. These IP addresses should be allocated for sessions which are L3 tunneled through the system (IP-in-IP or GRE). It is possible for resource pools in the same context to have overlapping addresses when the terminating network elements for the L3 tunnels are in different VPNs. Default: Disabled

Also refer to the *Subscriber Configuration Mode Commands* chapter for a description of the **l3-to-l2-tunnel address-policy** command.

send-icmp-dest-unreachable

When enabled, this generates an ICMP destination unreachable PDU when the system receives a PDU destined for an unused address within the pool.

Default: Disabled

skip-nat-subscriber-ip-check

When enabled, this is configured to skip private IP address check for non-NAT pools. This can be configured only for non-NAT pools during call-setup if NAT is enabled for the subscriber. If NAT is disabled, this value is not considered.

Default: Disabled (subscriber IP check is done).

explicit-route-advertise

When enabled, the output of **show ip pool verbose** includes the total number of explicit host routes. Default: Enabled

srp-activate

Activates the IP pool for Interchassis Session Recovery (ICSR).

subscriber-gw-address*ip_address*

Configures the subscriber gateway address for this pool.



Important Using this keyword might give a message as "busyout configured". This indicates that one ip address is reserved as subscriber-gw-address and not the entire pool.

suppress-switchover-arp

Suppress corresponding gratuitous ARP generation when a line card or MIO card switchover occurs. Default: Disabled

unicast-gratuitous-arp-address *ip_address*

Perform a unicast gratuitous ARP to the specified IP address rather than broadcast gratuitous ARP when gratuitous ARP generation is required. Default: Perform broadcast gratuitous ARP.

vrf *vrf_name* { [mpls-label input *in_label_value* | output *out_label_value1* [*out_label_value2*] }

Associates a preconfigured Virtual Routing and Forwarding (VRF) instance with this IP pool and configures MPLS label parameters.



Important This command must be used with next-hop parameters.

vrf_name is name of a preconfigured virtual routing and forwarding (VRF) context configured in Context Configuration Mode through **ip vrf** command.

- *in_label_value* is the MPLS label that identifies the inbound traffic destined for this pool.
- *out_label_value1* and *out_label_value2* identify the MPLS labels to be added to the outgoing packets sent for subscribers from this pool. Where *out_label_value1* is the inner output label and *out_label_value2* is the outer output label.

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

By default, the pools configured are bound to the default VRF unless specified with a VRF name.

Important You cannot have overlapping pool addresses using the same VRF. Also you cannot have two pools using different VRFs but the same in-label irrespective of whether or not the pools overlap. The pool must be private or static in-order to be associated with a certain VRF. If the VRF with such a name is not configured, you are prompted to add the VRF before configuring a pool.

policy allow-static-allocation

Configures static address allocation policy for dynamic IP pool. This keyword enables a dynamic IP pool to accept a static address for allocation.

Important In static allocation scenario, the pool group name is returned by AAA in the attribute **SN1-IP-Pool-Name**, and the IP address to use will be returned in the **Framed-IP-Address** attribute.

framed-route-vrf-list*vrf_list_name*

Configures a vrf-list in order for NVSE VRF authorization.

pool-route *ip_address/ip_mask*

Configures the IP pool route instead of generating by-default. The address followed by the **pool-route** keyword can be an IPv4 or IPv6 address with the mask value.

+

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

Usage Guidelines

Define one or more pools of IP addresses for the context to use in assigning IPs to mobile stations. This command is also useful in resizing existing IP pools to expand or contract the number of addresses allocated. If you resize an IP pool, the change is effective immediately.

When using the **ip pool** command to resize an IP pool, the type must be specified since by default the command assumes the type as public. In other words, the CLI syntax to resize an IP pool is the same syntax used to create the pool. See examples below.

```
ip pool pool1 100.1.1.0/24 static
```

The syntax to resize that pool would be:

```
ip pool pool1 100.1.1.0/25 static
```

A pool which is deleted will be marked as such. No new IP addresses will be assigned from a deleted pool. Once all assigned IP addresses from a deleted pool have been released, the pool, and all associated resources, are freed.

Important If an IP address pool is matched to a ISAKMP crypto map and is resized, removed, or added, the corresponding security association must be cleared in order for the change to take effect. Refer to the **clear crypto** command in the Exec mode for information on clearing security associations.

Over-lapping IP Pools: The system supports the configuration of over-lapping IP address pools within a particular context. Over-lapping pools are configured using either the resource or overlap keywords.

The **resource** keyword allows over-lapping addresses tunneled to different VPN end points.

The **overlap** keyword allows over-lapping addresses each associated with a specific virtual LAN (VLAN) configured for an egress port. It uses the VLAN ID and the nexthop address to determine how to forward subscriber traffic with addresses from the pool thus resolving any conflicts with overlapping addresses.

Note that if an overlapping IP Pool is bound to an IPSec Tunnel (refer to the **match ip pool** command in the *Crypto Group Configuration Mode* chapter), that tunnel carries the traffic ignoring the nexthop configuration. Therefore, the IPSec Tunnel takes precedence over the nexthop configuration. (Thus, one can configure the overlapping IP Pool with fake VLAN ID and nexthop and still be able to bind it to an IPSec Tunnel for successful operation.

The **overlap** keyword allows over-lapping addresses each associated with a specific VLAN can only be issued for pools of type private or static and must be associated with a different nexthop forwarding address and VLAN. A maximum of 128 over-lapping pools can be configured per context and a maximum of 256 over-lapping pools can be configured per system.



Important Overlapping IP address functionality is currently supported for use with systems configured as an HA for Mobile IP, or as a PDSN for Simple IP, or as a GGSN. For deployments in which subscriber traffic is tunneled from the FA to the HA using IP-in-IP, a separate HA service must be configured for each over-lapping pool.

IP Pool Address Assignment Method: IP addresses can be dynamically assigned from a single pool or from a group of pools. The addresses are placed into a queue in each pool. An address is assigned from the head of the queue and, when released, returned to the end. This method is known as least recently used (LRU).

When a group of pools have the same priority, an algorithm is used to determine a probability for each pool based on the number of available addresses, then a pool is chosen based on the probability. This method, over time, allocates addresses evenly from the group of pools.



Important Note that setting different priorities on each individual pool in a group can cause addresses in some pools to be used more frequently.



Important In NAT IP pool configurations, the minimum number of public IP addresses that must be allocated to each NAT pool must be greater than or equal to the number of Session Managers (SessMgrs) available on the system. On the ASR 5000, it is >= 84 public IP addresses. This can be met by a range of 84 host addresses from a single Class C. The remaining space from the Class C can be used for other allocations.

Example

The following commands define a private IP address pool, a public IP address pool, and a static address pool, respectively.

```
ip pool samplePool1 1.2.3.0 255.255.255.0 private
ip pool samplePool2 1.3.0.0 255.255.0.0 public
ip pool samplePool3 1.4.5.0 255.255.255.0 static
```

The following command defines a private IP pool specified with a range of IP addresses. The pool has 101 addresses.

```
ip pool samplePool4 range 10.5.5.0 10.5.5.100 private
```

The following command sets the address hold timer on the pool to *60* minutes (*3600* seconds):

```
ip pool samplePool4 address-hold-timer 3600
```

The following command removes the IP address pool from the configuration:

```
no ip pool samplePool1
```

The following command creates a static IP pool:

```
ip pool pool1 100.1.1.0/24 static
```

The following command resizes the static IP pool created in the previous example:

```
ip pool pool1 100.1.1.0/25 static
```

ip prefix-list

Creates an IP prefix list for filtering routes.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

ip prefix-list name *list_name* **[seq** *seq_number* **] { deny | permit } { any |** *network_address*/*net_mask* **[ge** *ge_value* **] [le** *le_value* **]**
no ip prefix-list *list_name* **[seq** *seq_number* **] { deny | permit } { any |** *network_address*/*net_mask* **[ge** *ge_value* **] [le** *le_value* **]**

no

Delete the specified prefix-list entry.

name *list_name*

Specifies a name for the prefix list as an alphanumeric string of 1 through 79 characters.

seq *seq_number*

Assigns the specified sequence number to the prefix list entry as an integer from 1 through 4294967295.

deny

Specifies prefixes to deny.

permit

Specifies prefixes to permit.

any

Matches any prefix.

network_address/net_mask **[ge** ***ge_value*** **] [le** ***le_value*** **]**

Specifies the prefix to match.

network_address/net_mask: the IP address and the length, in bits, of the network mask that defines the prefix. The IP address and mask must be entered in IPv4dotted-decimal notation. When neither **ge** (greater than or equal to) or **le** (less than or equal to) are specified an exact match is assumed.

ge *ge_value*: Specifies the minimum prefix length to match as an integer from 0 through 32. If only the ge value is specified, the range is from the ge value to 32. The ge value must be greater than *net_mask* and less than the le value.

le *le_value*: Specifies the maximum prefix length to match as an integer from 0 through 32. If only the le value is specified, the range is from the *net_mask* to the le value. The le value must be less than or equal to 32.

The following equation describes the conditions that ge and le values must satisfy:

net_mask < *ge_value* < *le_value* <= **32**

Usage Guidelines Use this command to filter routes by their IP prefix.

Example

```
ip prefix-list name prelist10 seq 5 permit 192.168.100.0/8 ge 12 le 24
```

ip prefix-list sequence-number

Enables or disables the inclusion of IP prefix list sequence numbers in the configuration file. This option is enabled by default.

Product PDSN

HA

GGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] ip prefix-list sequence-number

no

Disables the listing of IP prefix list sequence numbers in the configuration file.

Usage Guidelines

Use this command to enable and disable the inclusion of IP prefix list sequence numbers in the configuration file.

Example

To disable the inclusion of IP prefix list sequence numbers in the configuration file, enter the following command:

no ip prefix-list sequence-number

ip route

Adds or removes routing information from the current context's configuration.

Product

All

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] ip route { *ip_address*/*ip_mask* | *ip_address ip_mask* } { *gateway_ip_address* | next-hop *next_hop_ip_address* | point-to-point | tunnel } *egress_intrfc_name* [cost *cost*] [fall-over bfd multihop *mhsess_name*] [precedence *precedence*] [vrf *vrf_name* [cost *value*] [fall-over bfd multihop *mhsess_name*] [precedence *precedence*] +

[no] ip route static bfd *if_name remote-endpt_ipv4_address*

[no] ip route static multihop bfd *mhbfd_sess_name local_endpt_ipaddr remote_endpt_ipaddr*

[no] ip route kernel ip_address/ip_address_mask_combo *egress_intrfc_name* **cost** *number*

[no] ip route kernel ip_address/ip_address_mask_combo *egress_intrfc_name* **cost** *number* **blackhole**

no

Indicates the route specified by this options is to be removed from the configuration.

kernel

Allows static route in the kernel routing table options.

ip_address/ip_mask* | *ip_address/ip_mask

Specifies a destination IP address or group of addresses that will use this route.

ip_address/ip_mask: Specifies a combined IP address subnet mask bits to indicate what IP addresses to which the route applies. *ip_address* must be entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. *ip_mask/* is entered using CIDR notation; the mask bits are a numeric value which is the number of bits in the subnet mask.

ip_address/ip_mask: Specifies an IP address and the networking (subnet) mask pair which is used to identify the set of IP addresses to which the route applies. *ip_address* must be specified using the standard IPv4 dotted decimal notation. *ip_mask* must be specified using the standard IPv4 dotted decimal notation as network mask for subnets.

The mask as specified by *ip_mask* or resulting from *ip_address/ip_mask* is used to determine the network for packet routing.

0's in the resulting mask indicate the corresponding bit in the IP address is not significant in determining the network for packet routing.

1's in the resulting mask indicate the corresponding bit in the IP address is significant in determining the network.

ip_address/ip_address_mask_combo

Specifies a combined IP address subnet mask bits to indicate what IP addresses the route applies to. *ip_address_mask_combo* must be specified using CIDR notation where the IP address is specified using IPv4 dotted-decimal notation and the mask bits are a numeric value, which is the number of bits in the subnet mask.

***gateway_ip_address* | next-hop *next_hop_ip_address* | point-to-point | tunnel**

Specifies which device or network to use when forwarding packets.

gateway_ip_address: Specifies the IP address of the network gateway to which to forward packets. The address must be entered in IPv4 dotted-decimal notation (###.###.###.###).

next-hop *next_hop_ip_address*: Specifies the next-hop IP address to which packets are to be forwarded. The address must be entered in IPv4 dotted-decimal notation and IPv6 address in colon-separated-hexadecimal notation.

point-to-point: Specifies that the egress port is an ATM point-to-point interface.

tunnel: Sets the static route for this egress interface as tunnel type, such as IPv6-over-IPv4 or GRE.

egress_intrfc_name

Specifies the name of the egress (out-bound) interface name in the current context as an alphanumeric string of 1 through 79 characters. For a blackhole route, the default is "*", that is, a wildcard interface.

cost *cost*

Specifies the relative cost of the route. *cost* must be an integer from 0 through 255 where 255 is the most expensive. Default: 0

cost *number*

Defines the number of hops to the next gateway. The cost must be an integer from 0 through 255 where 255 is the most expensive. The default is 0.

blackhole

Defines blackhole route to install in the kernel to block or drop packets.

fall-over bfd multihop *mhsess_name*

Enables fall-over BFD functionality for the specified multihop session. The **fall-over bfd** option uses BFD to monitor neighbor reachability and liveliness. When enabled it will tear down the session if BFD signals a failure. Specify *mhsess_name* as an alphanumeric string of 1 through 19 characters.

precedence *precedence*

Specifies the selection order precedence for this routing information. *precedence* must be an integer from 1 through 254 where 1 is the highest precedence. Default: 1

vrf *vrf_name*

Associates a Virtual Routing and Forwarding (VRF) context with this static route configuration.

vrf_name is the name of a preconfigured VRF context configured in *Context Configuration Mode* via the **ip vrf** command.

static bfd *if_name remote-endpt_ipv4_address*

Creates a static IP route that will be associated with Bidirectional Forwarding Detection (BFD). For additional information, see the *BFD Configuration Mode Commands* chapter.

if_name: Specifies the name of the interface to which the static BFD neighbor is bound as an alphanumeric string of 1 through 79 characters.

remote_endpt_ipv4_address: Specifies the gateway address of the BFD neighbor in IPv4 dotted-decimal notation.

static multihop bfd *mhbfd_sess_name local_endpt_ipaddr remote_endpt_ipaddr*

Creates a static multihop BFD route with local and remote endpoints.

mhbfd_sess_name: Specifies the multihop BFD session name as an alphanumeric string of 1 through 79 characters.

local_endpt_ipaddress: Specifies the local endpoint address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

remote_endpt_ipaddress: Specifies the remote endpoint address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage Guidelines

Use this command to configure IP route parameters. precedence and cost options for the route selections such that routes of the same precedence are grouped together then lowest cost is selected first. This results in route's being selected first by lower precedence then the cost is used if multiple route's are defined with the same precedence.

This command also configures static IP routes when implementing Bidirectional Forwarding Detection (BFD).

Important A maximum of 1,200 static routes may be configured per context.

Virtual Routing and Forwarding (VRF) context can be associated with static IP route for BGP/MPLS, GRE, or IPSec tunnel support.

Important SNMP traps are generated when BFD sessions go up and down (BFDSessUp and BFDSessDown).

Use the **ip route kernel ip_address/ip_address_mask_combo interface** *interface_name* **cost** *number* to add the special route to any of two packet processing interfaces (SF cards) defined in the context configuration. Use the **[no] ip route kernel ip_address/ip_address_mask_combo interface** *interface_name* **cost** *number* **blackhole** to block or drop packets going out of the node.

Example

The following command adds a route using the combined IP address and subnet mask form:

```
ip route 10.2.3.0/32 192.168.1.2 egressSample1 precedence 160
```

The following configures route options for a route specified using the distinct IP address and subnet mask form:

```
ip route 10.2.3.4 255.224.0.0 10.1.2.3 egressSample2 cost 43
```

The following deletes the two routes configured above:

```
no ip route 209.165.200.224/32 192.51.1.2 egressSample1 precedence 160
no ip route 209.165.200.224 255.224.0.0 209.165.200 egressSample2 cost
43
```

The following command adds a route using the combined IP address and subnet mask form and specifies the egress interface as tunnel type:

```
ip route 209.165.200.224/32 tunnel egressSample1 precedence 160 vrf vrf1
```

ip routing maximum-paths

Enables Equal Cost Multiple Path (ECMP) routing support and specifies the maximum number of ECMP paths that can be submitted by a routing protocol in the current context.

Product All products that support Cost Multiple Path (CMP)

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

ip routing maximum-paths [*max_num*]
[default | no] ip routing maximum-paths

default

Resets the command to its default setting of 4.

no

Disables ECMP for the current context.

max_num

The maximum number of ECMP paths that can be submitted by a routing protocol. *max_num* must be an integer within the following ranges:

- For ASR5000: 1 through 10
- For ASR5500: 1 through 24
- For VPC-DI: 1 through 32 (*for Releases prior to 21.4*
- For VPC-DI: 1 through 64 (*for Release 21.4+*

Default: 4

Usage Guidelines

Use this command to enable ECMP for routing and set the maximum number of ECMP paths that can be submitted by a routing protocol.

Example

To enable ECMP and set the maximum number of paths that may be submitted by a routing protocol in the current context to *10*, enter the following command:

```
ip routing maximum-paths 10
```

To disable ECMP in the current context, enter the following command:

```
no ip routing maximum-paths
```

ip routing overlap-pool

Configures the routing behavior for overlap-pool addresses.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description `[ no | default ] ip routing overlap-pool`

default

Resets the command to its default setting of disabled.

no

Disables the routing behavior for overlap-pool addresses for the current context.

Usage Guidelines Use this command configuration to advertise overlap-pool addresses in dynamic routing protocols when overlap pools are configured using vlan-ids. If the "iprouting overlap-pool" is configured, then the overlap-addresses are added as interface addresses and advertised.

ip rri

Configures Reverse Route Injection (RRI) egress clear port IPv4 parameters. (VPC-VSM only)

Product SecGW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **ip rri {** *ip_address* **| next-hop** *nexthop_address* **} interface** *interface_name* **[vrf** *vrf_name* **]**
no ip rri { *ip_address* **| next-hop** *nexthop_address* **} interface** *interface_name* **[vrf** *vrf_name* **]**

no

Disables the specified RRI egress parameters.

ip_address

Specified in IPv4 dotted-decimal notation.

next-hop ***nexthop_address***

Next hop address specified in IPv4 dotted-decimal notation. The next hop IP address is not required for point-to-point and tunnel interfaces.

interface ***interface_name***

Specifies the name of an existing egress interface as an alphanumeric string of 1 through 79 characters.

vrf *vrf_name*

Specifies the name of an existing VRF as an alphanumerical string of 1 through 63 characters.

Usage Guidelines

Use this command to configure RRI regress clear port IPv4 parameters.

Example

```
ip rri 209.165.200.225 interface rri02
```

ip rri-route

Configures High Availability (HA) IPv4 routing parameters for Reverse Route Injection (RRI). (VPC-VSM only)

Product

SecGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

ip rri-route network-mode { L2 | L3 } { *clear_loopback_ip* | rri-ip *virtual_ip_address* } { *ip_address* | next-hop *nexthop_address* } interface *interface_name* [vrf *vrf_name*]

no ip rri-route network-mode { L2 | L3 } { *clear_loopback_ip* | rri-ip *virtual_ip_address* } { *ip_address* | next-hop *nexthop_address* } interface *interface_name* [vrf *vrf_name*]

no

Disables the specified RRI route.

network-mode { L2 | L3 }

Specifies the RRI route network mode type as Layer 2 (L2) or Layer 3 (L3).

clear_loopback_ip

Specifies the loopback address for clear traffic in IPv4 dotted-decimal notation.

rri-ip *virtual_ip_address*

Specifies the use of a virtual IP address on both Primary and Secondary for RRI. *virtual_ip_address* is expressed in IPv4 dotted-decimal notation.

ip_address

Specified in IPv4 dotted-decimal notation.

next-hop *nexthop_address*

Next hop address specified in IPv4 dotted-decimal notation. The next hop IP address is not required for point-to-point and tunnel interfaces.

interface *interface_name*

Specifies the name of an existing egress interface as an alphanumeric string of 1 through 79 characters.

vrf *vrf_name*

Specifies the name of an existing VRF as an alphanumerical string of 1 through 63 characters.

Usage Guidelines

Use this command to configure HA IPv4 routing parameters for RRI.

Example

```
ip rri-route network-mode L3 rri-ip 209.165.200.225 next-hop
209.165.200.227 interface rriroute04
```

ip sri-route

Configures Layer 3 (L3) High Availability (HA) IPv4 routing parameters for Service Route Injection (SRI). (VPC-VSM only)

Product

Important The **ip sri-route** CLI command is deprecated, and not supported in 19.0 and later releases.

SecGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
ip sri-route sri-ip network_address next hop nexthop_address interface interface_name
  [ vrf vrf_name ]
no ip sri-route sri-ip network_address next hop nexthop_address interface
interface_name  [ vrf vrf_name ]
```

no

Disables the specified SRI route.

sri-ip *network_address*

Specifies the IPv4 address associated with the SRI route.

next hop *nexthop_address*

Next hop address specified in IPv4 dotted-decimal notation. The next hop IP address is not required for point-to-point and tunnel interfaces.

interface *interface_name*

Specifies the name of an existing egress interface as an alphanumeric string of 1 through 79 characters.

vrf *vrf_name*

Specifies the name of an existing VRF as an alphanumerical string of 1 through sixty-three characters.

Usage Guidelines

Use this command to configure L3 HA routing parameters for SRI.

Example

```
ip sri-route sri-ip 10.1.1.21 next-hop 10.1.1.23 interface sri23
```

ip vrf

Creates a Virtual Routing and Forwarding (VRF) context instance, assigns a VRF identifier, and configures the VRF parameters for BGP/MPLS VPN, GRE tunnel, and IPSec interface configuration.



Important IKEv2 ACL VRF is not supported.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

ip vrf *vrf_name*
no ip vrf

no

Disables IP Virtual Routing and Forwarding (VRF) parameters.

vrf_name

Specifies the name of the virtual routing and forwarding interface as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to create a VRF context and assign a VRF identifier for BGP/MPLS VPN, IPSec, GRE tunnel configuration in this context instance. This command is used when the system works as a BGP router with MPLS VPN and binds an MPLS VPN to the system or to facilitate GRE or IPSec tunnelling. The addresses assigned to this interface are visible in the VRF routing table.

This command switches the command mode to IP VRF Context Configuration Mode:

```
[context_name>]host_name(config-context-vrf)#
```

If required, this command creates an IP VRF Context Configuration Mode instance.

When using this command please note of the following:

- A VRF context instance must be created and configured before referring, associating, or binding the same with any command or mode.
- If the interface binding to a VRF context instance is changed or any IP address assigned to the interface is deleted, a warning is displayed.
- All interfaces bound with a VRF context instance will be deleted when that VRF is removed/deleted.
- An interface can be bound to only one VRF context instance.
- A maximum of 100 VRF context instances can be configured on a system.

Refer to the *IP VRF Context Configuration Mode Commands* chapter for parameter configuration.

Example

The following command configures the virtual routing and forwarding context instance *vrf1* in a context:

```
ip vrf vrf1
```

ip vrf-list

Creates a VRF list and adds VRFs to the list. The VRFs must have been previously created via the **ip vrf** command.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
ip vrf-list list_name permit vrf_name
no ip vrf-list list_name [ permit vrf_name ]
```

no

Deletes a VRF list or delete VRFs from this list. If **permit** and *vrf-name* are not specified, the entire list of VRFs is deleted. Otherwise, the specified VRF(s) is deleted from the list.

list_name

Specifies the name of the VRF list as an alphanumerical string of 1 through 63 characters.

vrf_name

Specifies the name of the virtual routing and forwarding interface as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Create a VRF list and add VRFs to the list. The VRFs must have been previously created via the **ip vrf** command. This command supports multiple VRFs over NEMO.

Example

The following command creates a VRF list named *corp103* and adds a VRF named *vrf3567*:

```
ip vrf-list corp103 permit vrf3567
```

ipms

Enables/disables/manages an intelligent packet monitoring system (IPMS) client service and enters the IPMS Client Configuration Mode within the current context.

Product

IPMS

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] ipms [ -noconfirm ]
```

no

Deletes a previously configured IPMS client service.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Caution If this keyword option is used with **no ipms** command, the IPMS client service will be deleted with all active/inactive IPMS sessions without prompting any warning or confirmation.

Usage Guidelines

Use this command to enable/disable/manage the IPMS client service within a context and configure certain functionality. This command enables and allows the configuration of service enabling the system to function as an IPMS-enabled Access Gateway in a network. This command is also used to remove previously configured IPMS client service.

A maximum of 1 IPMS client can be configured per system.

Important The IPMS is a license enabled external application support. Refer to the *IPMS Installation and Administration Guide* for more information on this product.

Refer to the *IPMS Installation and Administration Guide* and *IPMS Configuration Mode* chapter of this reference for additional information.

Example

The following command creates an IPMS client service name within the context:

ipms

ipne-service

Create and/or configure an IPNE service.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] ipne-service *ipne_service*

no

Included as a prefix of the command, **no** causes the system to disable IPNE service when it has been created with this command and removes the IPNE service definition from the MME's configuration.

ipne_service

Enter 1 to 63 alphanumeric characters to create a unique name for an IPNE service instance.

Usage Guidelines

This command creates an instance of an IPNE service in the context.It is recommended that the IPNE Service be configured in the same context in which the MME Service has been configured.

This command also accesses the commands in the IPNE service configuration mode to configure the IPNE service.

If an IPNE service is to be removed and the service has active handles, then the handles are deleted using a timer-based approach and then the IPNE service is removed.

Example

Create an IPNE service called *IPNEserv1*:

```
ipne-service IPNEserv1
```

Use a command similar to the following to disable and remove the IPNE service configuration for the IPNE service called *ipneserv*.

```
no ipne-service ipneserv
```

ipsec replay

Configures IKEv2 IPSec specific anti-replay.

Product

ePDG

PDIF

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] ipsec replay [ window-size window_size ]
```

no

Disables this option.

replay

Configures IKEv2 IPSec anti-replay.

window-size *window_size*

Configures anti-replay window size.

window_size is the window size 32, 64 (default), 128, 256, 384, 512 , an integer value between 32..512

Usage Guidelines Use this command to configure IKEv2 IPSec specific anti-replay.

Example

The following command sets the window size to 256:

```
ipsec replay window-size 256
```

ipsec transform-set

Creates a new or specifies an existing IPSec transform set and enters the IPSec Transform Set Configuration Mode for the current context.

Product ePDG

PDIF

SCM

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] ipsec transform-set transform_set_name
```

no

Removes an existing transform set from the system.

transform-set *name*

Specifies the name of a new or existing transform set as an alphanumeric string of 1 through 127 characters.

Usage Guidelines Use this command to Configure IKEv2 IPsec child security association transform set parameters. Up to four transform-sets can be created.

Entering this command results in the following prompt:

[*context_name*]*hostname*(cfg-ctx-ipsec-tran-set)#

This command applies to IKEv2. Please check **crypto ipsec transform-set** command for ipsec transform-set configuration for IKEv1.

Example

The following command configures an IPSec transform set called *ipsec12* and enters the IPSec Transform Set Configuration Mode:

ipsec transform-set *ipsec12*

ipsg-service

This command allows you to create/modify/delete an IP Services Gateway (IPSG) service in the current context.

Product

eWAG

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

ipsg-service *ipsg_service_name* **[mode { radius-server [ewag] | radius-snoop }] [-noconfirm]**
no ipsg-service *ipsg_service_name* **[mode { radius-server [ewag] | radius-snoop }]**

no

If previously configured, deletes the specified IPSG service.

ipsg_service_name

Specifies the name of the IPSG service.

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

Important Service names must be unique across all contexts within a chassis.

mode { radius-server [ewag] | radius-snoop }

Configures the IPSG to perform as either a RADIUS server or as a device to extract user information from RADIUS accounting request messages (snoop). If the optional keyword **mode** is not entered, the system defaults to **radius-server**.

- **radius-server**:Creates the named IPSG RADIUS Server service in the current context and/or enters the IPSG RADIUS Server Configuration Mode.

- **radius-server ewag**: Enables the eWAG service (IPSG service in eWAG mode), and enters the IPSG RADIUS Server Configuration Mode, which is common for the eWAG and IPSG services.
- **radius-snoop**:Creates the named IPSG RADIUS Snoop service in the current context and/or enters the IPSG RADIUS Snoop Configuration Mode.

-noconfirm

Specifies to execute the command without additional prompt or confirmation.

Usage Guidelines

Use this command to create/configure/delete an IPSG service.

A maximum of one IPSG service can be configured per context.

IPSG service commands are defined in the *IPSG RADIUS Snoop Configuration Mode Commands* chapter and the *IPSG RADIUS Server Configuration Mode Commands* chapters.

A maximum of 256 services (regardless of type) can be configured per system.



Caution A large number of services greatly increases the complexity of system management and may impact overall system performance (i.e., resulting from system handoffs). Do not configure a large number of services unless your application requires it. Contact your Cisco account representative for more information.



Important IP Services Gateway functionality is a license-controlled feature. A valid feature license must be installed prior to configuring an IPSG service. Contact your Cisco account representative for more information.

On entering the command with the **radius-server** mode or without any mode, the CLI prompt changes to:

[*context_name*]*hostname*(config-ipsg-service-radius-server)#

On entering the command with the **radius-snoop** mode, the CLI prompt changes to:

[*context_name*]*hostname*(config-ipsg-service-radius-snoop)#

For more information about the IP Services Gateway, refer to the *IP Services Gateway Administration Guide*.

Example

The following command configures an IPSG RADIUS Snoop service named *ipsg1* and enters the IPSG RADIUS Snoop Configuration Mode:

```
ipsg-service ipsg1 mode radius-snoop
```

The following command enables the eWAG service (IPSG service in eWAG mode), and enters the IPSG RADIUS Server Configuration Mode, which is common for the eWAG and IPSG services:

```
ipsg-service ipsg2 mode radius-server ewag
```

ipv6 access-group

Configures the IPv6 Access group.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

ipv6 access-group *group name* **{** *priority_value* **}**

group_name

Specifies the name of the access group as an alphanumeric string of 1 through 79 characters.

priority_value

Specifies the priority of the access group. 0 is the highest priority. If *priority_value* is not specified the priority is set to 0. *priority_value* must be an integer from 0 through 4294967295. Default: 0

If access groups in the list have the same priority, the last one entered is used first.

Usage Guidelines

Use this command to specify IPv6 access group name and priority. Use a lower value to indicate a higher priority for the group.

Example

```
ipv6 access-group group_1
```

ipv6 access-list

Create, configure, or delete an IPv6 Access List in the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description `[ no ] ipv6 access-list name`

no

Removes the specified access list.

name

Specifies the access list name.

name is an alphanumeric string of 1 through 47 characters.

If the named access list does not exist, it is created, and the CLI mode changes to the ACL Configuration Mode, wherein the access list can be configured.

If the named access list already exists, the CLI mode changes to the ACL Configuration Mode, wherein the access list can be reconfigured.

Usage Guidelines Executing this command enters the IPv6 ACL Configuration Mode in which rules and criteria are defined for the ACL.

Important A maximum of 256 rules can be configured per ACL. The maximum number of ACLs that can be configured per context is limited by the amount of available memory in the VPN Manager software task; it is typically less then 200.

Refer to the *Access Control Lists* appendix of the *System Administration Guide* for more information on ACLs.

Example

```
ipv6 access-list samplelist
no ipv6 access-list samplelist
```

ipv6 dns-proxy

Configures the domain name server proxy for the context.

Product PDSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description `[ no ] ipv6 dns-proxy source-ipv4-address ip_address`

no

Removes the predefined IP address for local interface in the destination context.

ip_address

Specifies the IPv4 address of one of the local interface in the destination context to configure the IPv6 DNS proxy where *ip_address* must be specified using IPv4 dotted-decimal notation.

Usage Guidelines The IPv6 DNS proxy source IPv4 address is used as the source IP address for the DNS proxy transaction.

Example

The following command provides an example of configuring a IPv6 DNS proxy of *192.168.23.1*:

```
ipv6 dns-proxy source-ipv4-address 192.168.23.1
```

ipv6 neighbor

Adds a static IPv6 neighbor entry into the neighbor discovery table.

Product PDIF

Privilege Administrator, Security Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **`[ no ] ipv6 neighbor`** *`ipv6_address hardware_address`*

no

Removes the specified address.

ipv6_address hardware_address

ipv6_address is the IP address of node to be added to the table.

hardware_address is the associated 48-bit MAC address.

Usage Guidelines Add a static IPv6 neighbor entry into the neighbor discovery table.



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

Example

Add the ipv6 address *fe80::210:83ff:fef7:7a9d::/24* and associated 48 bit MAC address *0:10:83:f7:7a:9d* to the table.

```
ipv6 neighbor fe80::210:83ff:fef7:7a9d::/24 0:10:83:f7:7a:9d
```

ipv6 pool

Modifies the current context's IP address pools by adding, updating or deleting a pool. This command also resizes an existing IP pool.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

ipv6 pool *name* **{ 6to4 local-endpoint** *ipv4_address* **[default-relay-router** *router_address* **] | alert threshold | group-name** *name* **| policy { allow-static-allocation | dup-addr-detection } | prefix** *ip_address/len* **[6to4-tunnel local-endpoint** *ip_address* **| default-relay-router** *router_address* **] | range** *start_addressend_address* **| suppress-switchover-arps } [prefix-length** *prfx_length* **] [private** *priority* **] [public** *priority* **] [shared** *priority* **] [static** *priority* **] [group-name** *name* **] [vrf** *vrf-name* **]**
no ipv6 pool *name*

no

Deletes the previously configured IPv6 pool.

name

Specifies the logical name of the IP address pool as an alphanumeric string of 1 through 31 characters.

Important Adding the IPv6 Pool command and the Busyout command of the same IPv6 Pool at the same time creates a race condition. To avoid the issues, run the IPv6 Pool command and Busyout command separately.

6to4-tunnel local-endpoint *ip_address*

Specifies the IPv4 address of the local interface to be used for IPv6-to-IPv4 compatible pool address construction.

alert threshold { 6to4 local-endpoint *ipv4_address* | alert threshold | group-available | group-name *name* | policy { allow-static-allocation | dup-addr-detection } | pool-free | pool-used | pool-usable | pool-usable-final | prefix | range *start_address end_address* }

Default: All thresholds are disabled.

Configures IP address pool-level utilization thresholds. These thresholds take precedence over context-level IPv6 pool thresholds.

- **6to4**: Sets an alert based on the IPv6 Pool for an IPv6-to-IPv4 compatible address type.
- **alert-threshold**: Sets an alert based on the percentage free alert threshold for this group.
- **group-available**: Sets an alert based on the percentage free alert threshold for this group.
- **group-name**: Sets an alert based on the IPv6 Pool Group.
- **policy allow-static-allocation**: Sets an alert based on the address allocation policy.
- **pool-free**: Sets an alert based on the percentage free alert threshold for this pool.
- **pool-used**: Sets an alert based on the percentage used alert threshold for this pool.
- **pool-usable**: This command sets IP pool usable pre threshold state as either free or release.
- **pool-usable-final**: Thiss command sets the IP pool usable final threshold state as either free or release.
- **prefix**: Sets an alert based on the IPv6 Pool address prefix.
- **range**: Sets an alert based on the IPv6 address pool range of addresses.
- **suppress-switchover-arps**: Sets an alert based on the Suppress Gratuitous ARPs when performing a line card or an MIO switchover.

group name *name*

IPv6 Pool Group.

The following options are available:

- **6to4**: IPv6 Pool for IPv6-to-IPv4 compatible address type
- **alert-threshold**: Percentage free alert threshold for this group
- **group-name**: IPv6 Pool Group
- **policy**: Configure an address allocation policy
- **prefix**: IPv6 Pool address prefix
- **range**: Configures IPv6 address pool to use a range of addresses
- **suppress-switchover-arps**: Suppress gratuitous ARPs when performing a line card or an MIO switchover.

ipv4_address

Specifies the beginning IPv4 address of the IPv4 address pool. *ipv4_address* must be specified using IPv4 dotted-decimal notation.

default-relay-router *router address*

Specifies the default relay router for the tunnel.

policy allow-static-allocation

Allows a dynamic pool to accept a static address allocation.

The following options are available:

- **6to4**: IPv6 Pool for IPv6- to-IPv4 compatible address type
- **alert-threshold**: Percentage free alert threshold for this group
- **group-name**: IPv6 Pool Group
- **policy**: Configure an address allocation policy
- **prefix**: IPv6 Pool address prefix
- **range**: Configure IPv6 address pool to use a range of addresses
- **suppress-switchover-arps**: Suppress gratuitous ARPs when performing a line card or an MIO switchover

policy dup-addr-detection

This command is valid for IPv6 shared pools only (Sample syntax: **ipv6 pool** *name* **prefix** *ip_address/len* **shared policy dup-addr-detection**). When this policy is enabled, the IPv6 shared pool allows a prefix to be shared in different call sessions with different interface IDs for an IPv6 address. This allows the tracking of interface IDs per prefix and the detection of duplicate IDs.

With this policy disabled, the IPv6 shared pool will allow a prefix to be shared across different call sessions. The interface ID is not considered for any duplicate address detection. Default: Disabled

The following options are available:

- **6to4**: IPv6 pool for IPv6-to-IPv4 compatible address type
- **alert-threshold**: Percentage free alert threshold for this group
- **group-name**: IPv6 pool group
- **policy**: Configure an address allocation policy
- **prefix**: IPv6 pool address prefix
- **range**: Configures IPv6 address pool to use a range of addresses
- **suppress-switchover-arps**: Suppress gratuitous ARPs when performing a line card or an MIO switchover

prefix *ip_address/len*

Specifies the beginning IPv6 address of the IPv6 address pool. *ip_address/len* must be specified using IPv6 colon-separated-hexadecimal. *len* is an integer that indicates the number bits of prefix length.



Important If the **prefix** *ip_address/len* specified is less than /40, then a **prefix-length** *prfx_length* must be specified. Options are 48, 52, or 58 bits of **prefix-length**.



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

range *start_address end_address*

Configures an IPv6 address pool to use a range of addresses.

start_address specifies the beginning of the range of addresses for the IPv6 pool. It must be specified using IPv6 colon-separated-hexadecimal notation.

end_address specifies the end of the range of addresses for the IPv6 pool. It must be specified using IPv6 colon-separated-hexadecimal notation.

suppress-switchover-arps

Suppresses gratuitous ARPs when performing a line card switchover.

The following options are available:

- **6to4**: IPv6 Pool for IPv6-to-IPv4 compatible address type
- **alert-threshold**: Percentage free alert threshold for this group
- **group-name**: IPv6 Pool Group
- **policy**: Configure an address allocation policy
- **prefix**: IPv6 Pool address prefix
- **range**: Configures IPv6 address pool to use a range of addresses
- **suppress-switchover-arps**: Suppress gratuitous ARPs when performing a line card or an MIO switchover

prefix-length *prfx_length*

Specifies a configured length of prefixes. *prfx_length* can be 48, 52, 56 or 64 bits of prefix (Default = 64). This option supports S-GW/P-GW validation of fixed-length addresses via DHCPv6 (TS 29.274 – 7.2.2 and 8.14).



Important If the **prefix** *ip_address/len* specified is less than /40, then a **prefix-length** *prfx_length* must be specified. Options are 48, 52, or 58 bits of **prefix-length**.



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

private *priority* | public *priority* | shared *priority* | static *priority*

Default: **public**

private *priority*: Specifies that the address pool may only be used by mobile stations which have requested an IP address from a specified pool. When private pools are part of an IP pool group, they are used in a priority order according to the precedence setting. *priority* must be an integer from 0 through 10 with 0 being the highest. The default is 0.

public *priority*: Specifies that the address pool is used in priority order for assigning IP addresses to mobile stations which have not requested a specific address pool. *priority* must be an integer from 0 through 10 with 0 being the highest and with a default of 0.

shared *priority*: Specifies that the address pool that may be used by more than one session at any time. *priority* must be an integer from 0 through 10 with 0 being the highest and with a default of 0.

static *priority*: Specifies that the address pool is used for statically assigned mobile stations. Statically assigned mobile stations are those with a fixed IP address at all times. *priority* must be an integer from 0 through 10 with 0 being the highest and with a default of 0.

group-name *name*

Groups the IPv6 pools into different groups. The subscribers/domain can be configured with the group-name instead of the prefix-pool names. *name* is the name of the group by which the IPv6 pool is to be configured expressed as an alphanumeric string of 1 through 79 characters.

vrf *vrf-name*

Associates the pool with the VRF specified as an alphanumeric string of 1 through 63 characters. By default the configured IPv6 pool will be associated with the global routing domain.

Usage Guidelines

Use this command to modify the current context's IP address pools by adding, updating or deleting a pool. Also use this command to resize an existing IP pool.

Example

The following command adds an IPv6 pool named *ip6Star*:

```
ipv6 pool ip6Star
```

ipv6 prefix-list

Creates an IPv6 prefix list for filtering routes.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

ipv6 prefix-list name *list_name* **[seq** *seq_number* **] { deny | permit } { any |** *network_address*/*net_mask* **[ge** *ge_value* **] [le** *le_value* **]**
no ipv6 prefix-list *list_name* **[seq** *seq_number* **] { deny | permit } { any |** *network_address*/*net_mask* **[ge** *ge_value* **] [le** *le_value* **]**

no

Delete the specified prefix-list entry.

name *list_name*

Specifies a name for the prefix list as an alphanumeric string of 1 through 79 characters.

seq *seq_number*

Assigns the specified sequence number to the prefix list entry as an integer from 1 through 4294967295.

deny

Specifies prefixes to deny.

permit

Specifies prefixes to permit.

any

Matches any prefix.

***network_address*/*net_mask* [ge *ge_value*] [le *le_value*]**

Specifies the prefix to match.

network_address/*net_mask*: the IPv6 address and the length, in bits, of the network mask that defines the prefix. The IP address and mask must be entered in IPv6 colon-separated-hexadecimal notation. When neither **ge** (greater than or equal to) or **le** (less than or equal to) are specified an exact match is assumed.

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

ge *ge_value*: Specifies the minimum prefix length to match as an integer from 0 through 128. If only the ge value is specified, the range is from the ge value to 128. The ge value must be greater than *net_mask* and less than the le value.

le *le_value*: Specifies the maximum prefix length to match as an integer from 0 through 128. If only the le value is specified, the range is from the *net_mask* to the le value. The le value must be less than or equal to 128.

The following equation describes the conditions that ge and le values must satisfy:

net_mask < *ge_value* < *le_value* <= **128**

Usage Guidelines Use this command to filter routes by their IPv6 prefix.

Example

```
ipv6 prefix-list name prelistv6-10 seq 5 permit 2002::123.45.67.89/32
```

ipv6 prefix-list sequence-number

Enables or disables the inclusion of IPv6 prefix list sequence numbers in the configuration file. This option is enabled by default.

Product PDSN

HA

GGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] ipv6 prefix-list sequence-number
```

no

Disables the listing of IPv6 prefix list sequence numbers in the configuration file.

Usage Guidelines Use this command to enable and disable the inclusion of IPv6 prefix list sequence numbers in the configuration file.

Example

To disable the inclusion of IPv6 prefix list sequence numbers in the configuration file, enter the following command:

```
no ipv6 prefix-list sequence-number
```

ipv6 route

Configures a static IPv6 route to the next-hop router.

Product All

Privilege Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] ipv6 route *ipv6_address*/*prefix_length* **{ interface** *name* **| next-hop** *ipv6_address* **interface** *name* **} [cost** *cost*] **[fall-over bfd multihop** *mhsess_name* **] [precedence** *precedence* **] [vrf** *vrf_name* **[cost** *value* **] [fall-over bfd multihop** *mhsess_name* **] [precedence** *precedence* **]**
[no] ipv6 route static bfd *if_name remote-endpt_ipv6address*
[no] ipv6 route static multihop bfd *mhbfd_sess_name local_endpt_ipv6addr remote_endpt_ipv6addr*

no

Removes the specified static route.

ipv6_address/prefix_length

Specifies a destination IPv6 address or group of addresses that will use this route.

ipv6_address/prefix_length must be specified using IPv6 colon-separated-hexadecimal with 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.

interface *name*

Specifies the name of the interface on this system associated with the specified route or next-hop address. *name* must be an existing interface name on the system expressed as an alphanumeric string of 1 through 79 characters.

next-hop *ipv6_address*

The IPv6 address of the directly connected next hop device in IPv6 colon-separated-hexadecimal notation.

cost *cost*

Defines the number of hops to the next gateway as an integer from 0 through 255. Default: 0

fall-over bfd multihop *mhsess_name*

Enables fall-over BFD functionality for the specified multihop session. The **fall-over bfd** option uses BFD to monitor neighbor reachability and liveliness. When enabled it will tear down the session if BFD signals a failure. Specify *mhsess_name* as an alphanumeric string of 1 through 19 characters.

precedence *precedence*

Indicates the administrative preference of the route. A low precedence specifies that this route takes preference over the route with a higher precedence. *precedence* must be an integer from 1 through 254. Default: 1

vrf *vrf_name*

Associates a Virtual Routing and Forwarding (VRF) context with this static route configuration.

vrf_name is the name of a preconfigured VRF context configured in *Context Configuration Mode* via the **ip vrf** command.

static bfd *if_name remote-endpt_ipv6address*

Creates a static IP route that will be associated with Bidirectional Forwarding Detection (BFD). For additional information, see the *BFD Configuration Mode Commands* chapter.

if_name: Specifies the name of the interface to which the static BFD neighbor is bound as an alphanumeric string of 1 through 79 characters.

remote_endpt_ipv6address: Specifies the gateway address of the BFD neighbor in IPv6 colon-separated-hexadecimal notation.

static multihop bfd *mhbfd_sess_name local_endpt_ipv6addr remote_endpt_ipv6addr*

Creates a static multihop BFD route with local and remote endpoints.

mhbfd_sess_name: Specifies the multihop BFD session name as an alphanumeric string of 1 through 79 characters.

local_endpt_ipv6addr: Specifies the local endpoint address in IPv6 colon-separated-hexadecimal notation.

remote_endpt_ipv6addr: Specifies the remote endpoint address in IPv6 colon-separated-hexadecimal notation.

Usage Guidelines

Use this command to configure IPv6 route parameters, precedence and cost options for the route selections such that routes of the same precedence are grouped together then lowest cost is selected first. This results in route's being selected first by lower precedence then the cost is used if multiple route's are defined with the same precedence.

This command also configures static IP routes when implementing Bidirectional Forwarding Detection (BFD).

Important A maximum of 1,200 static routes may be configured per context.

Virtual Routing and Forwarding (VRF) context can be associated with static IP route for BGP/MPLS, GRE, or IPSec tunnel support.

Important SNMP traps are generated when BFD sessions go up and down (BFDSessUp and BFDSessDown).

Example

T the following example configures a static route with IPv6 prefix/length *2001:0db8:3c4d:0015:0000:0000:abcd:ef12/24* to the next hop interface *egress1*:

```
ipv6 route 2001:0db8:3c4d:0015:0000:0000:abcd:ef12/24 interface egress1
```

ipv6 route-access-list

Configures an IPv6 route access list for filtering routes.

Product

GGSN

HA

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

ipv6 route-access-list named *list_name* **] { deny | permit }** *network_address*/*net_mask* **[exact-match]**
no ipv6 prefix-list *list_name* **] { deny | permit } { any |** *network_address*/*net_mask* **[exact-match]**

no

Delete the specified prefix-list entry.

name *list_name*

Specifies a name for the prefix list as an alphanumeric string of 1 through 79 characters.

deny

Specifies prefixes to deny.

permit

Specifies prefixes to permit.

***network_address*/*net_mask* [exact-match]**

Specifies the prefix to match.

network_address/*net_mask*: the IPv6 address and the length, in bits, of the network mask that defines the prefix. The IP address and mask must be entered in IPv6 colon-separated-hexadecimal 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.

exact-match *le_value*: Specifies that only an exact match will initiate access list deny/permit function.

Usage Guidelines Use this command to filter routes by their IPv6 prefix.

Example

```
ipv6 route-access-list name routelistv6 seq 5 permit 2002::123.45.67.89/24
```

ipv6 rri

Configures Reverse Route Injection (RRI) egress clear port IPv6 parameters. (VPC-VSM only)

Product SecGW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
ipv6 rri { ipv6_address | next-hop nexthop_address } interface interface_name [
vrf vrf_name ]
no ipv6 rri { ipv6_address | next-hop nexthop_address } interface interface_name
[ vrf vrf_name ]
```

no

Disables the specified RRI egress route.

ipv6_address

Specified in IPv6 colon-separated-hexadecimal notation.

next-hop *nexthop_address*

Next hop address specified in IPv6 colon-separated-hexadecimal notation. The next hop IP address is not required for point-to-point and tunnel interfaces.

interface *interface_name*

Specifies the name of an existing egress interface as an alphanumeric string of 1 through 79 characters.

vrf *vrf_name*

Specifies the name of an existing VRF as an alphanumerical string of 1 through 63 characters.

Usage Guidelines Use this command to configure IPv6 RRI egress clear port IPv6 parameters.

Example

```
ipv6 rri 2001:4A2B::1f3F interface rri03
```

ipv6 rri-route

Configures High Availability (HA) IPv6 routing parameters for Reverse Route Injection (RRI). (VPC-VSM only)

Product

SecGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

ipv6 rri-route network-mode { L2 | L3 } { *clear_loopback_ip* | rri-ip *virtual_ipv6_address* } { *ipv6_address* | next-hop *nexthop_address* } interface *interface_name* [vrf *vrf_name*]
no ipv6 rri-route network-mode { L2 | L3 } { *clear_loopback_ip* | rri-ip *virtual_ipv6_address* } { *ipv6_address* | next-hop *nexthop_address* } interface *interface_name* [vrf *vrf_name*]

no

Disables the specified RRI route.

network-mode { L2 | L3 }

Specifies the RRI route network mode type as Layer 2 (L2) or Layer 3 (L3).

clear_loopback_ip

Specifies the loopback address for clear traffic in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

rri-ip *virtual_ipv6_address*

Specifies the use of a virtual IP address on both Primary and Secondary for RRI. *virtual_ipv6_address* is expressed in IPv6 colon-separated-hexadecimal notation.

ipv6_address

Specified in IPv6 colon-separated-hexadecimal notation.

next-hop *nexthop_address*

Next hop address specified in IPv6 colon-separated-hexadecimal notation. The next hop IP address is not required for point-to-point and tunnel interfaces.

interface *interface_name*

Specifies the name of an existing egress interface as an alphanumeric string of 1 through 79 characters.

vrf *vrf_name*

Specifies the name of an existing VRF as an alphanumerical string of 1 through 63 characters.

Usage Guidelines

Use this command to configure HA IPv6 routing parameters for RRI.

Example

```
ipv6 rri-route network-mode L3 rri-ip 2001:4A2B::1f3F
```

ipv6 sri-route

Configures Layer 3 (L3) High Availability (HA) IPv6 routing parameters for Service Route Injection (SRI). (VPC-VSM only)

Product

SecGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

ipv6 sri-route sri-ip *network_address* **next hop** *nexthop_address* **interface** *interface_name* **[vrf** *vrf_name* **]**
no ipv6 sri-route sri-ip *network_address* **next hop** *nexthop_address* **interface** *interface_name* **[vrf** *vrf_name* **]**

no

Disables the specified SRI route.

sri-ip *network_address*

Specifies the IPv6 address associated with the SRI route.

next hop *nexthop_address*

Next hop address specified in IPv6 colon-separated-hexadecimal notation. The next hop IP address is not required for point-to-point and tunnel interfaces.

interface *interface_name*

Specifies the name of an existing egress interface as an alphanumeric string of 1 through 79 characters.

vrf *vrf_name*

Specifies the name of an existing VRF as an alphanumerical string of 1 through 63 characters.

Usage Guidelines

Use this command to configure L3 HA IPv6 routing parameters for SRI.

Example

```
ipv6 sri-route sri-ip 2001:4A2B::1f3F interface sri23
```

isakmp disable-phase1-rekey

This command is deprecated. Use **ikev1 disable-phase1-rekey** command to configure the parameters for Phase1 SA rekeying when ISAKMP lifetime expires for IKE v1 protocol.

isakmp keepalive

This command is deprecated. Use **ikev1 keepalive dpd** command to configure ISAKMP IPSec Dead Peer Detection (DPD) message parameters for IKE v1 protocol.

isakmp policy

This command is deprecated. Use **ikev1 policy** command to create/configure an ISAKMP policy with the specified priority for IKE v1 protocol.

iups-service

Creates an Iu-PS service instance and enters the Iu-PS Service Configuration Mode. This mode defines the configuration and usage of Iu-PS interfaces between the SGSN and the RNCs in the UMTS radio access network (UTRAN). It defines both the control plane (GTP-C) and the data plane (GTP-U) between these nodes.



Important For details about the commands and parameters for this mode, check the *IuPS Service Configuration Mode Commands* chapter.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **`[ no ] iups-service`** *`srvc_name`*

no

Remove the configuration for the specified Iu-PS service from the configuration for the current context.

srvc_name

Specifies the IuPS service name as a unique alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines Use this command to create, edit, or remove an Iu-PS service. Add up to eight definitions to be used with a single SGSN service so the SGSN can support multiple PLMNs.

Example

The following command creates an Iu-PS service named *iu-ps1*:

```
iups-service iu-ps1
```

The following command removes the Iu-PS service named *iu-ps1*:

```
no iups-service iu-ps1
```

l2tp peer-dead-time

Configures a delay when attempting to tunnel to a specific peer which is initially unreachable due to reasons such as a network issue or temporarily having reached its capacity.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

l2tp peer-dead-time *seconds*
default l2tp peer-dead-time

default

Rests the command to its default setting of 60.

seconds

Specifies the interval (in seconds) to wait before attempting to tunnel to a specific peer which is initially unreachable as an integer from 5 through 64,000. Default: 60

Usage Guidelines

The time to wait before trying to establish a tunnel to a known peer after the initial attempt was unsuccessful.

Example

The following example configures the delay in attempting to tunnel to a temporarily unreachable peer. The delay is set to *120* seconds in this example.

```
l2tp peer-dead-time 120
```

lac-service

Enters the LAC Service Configuration Mode, or is used to add or remove a specified L2TP Access Concentrator (LAC) service.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] lac-service *name*

no

Removes the specified lac-service from the current context.

name

Specifies the name of a LAC service to configure, add, or remove as an alphanumeric string of 1 through 63 characters that is case-sensitive.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines Enter the LAC Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Example

To add a new LAC service named *LAC1* and enter the LAC Service Configuration Mode, enter the following command:

```
lac-service LAC1
```

To configure an existing LAC service named *LAC2*, enter the following command:

```
lac-service LAC2
```

To delete an existing LAC service named *LAC3*, enter the following command:

```
no lac-service LAC3
```

lawful-intercept

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

lawful-intercept dictionary

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

limit ipsecmgr ikev1 max

Use this command to limit the parameter for this context.

Product IPSec

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

limit ipsecmgr ikev1 max*max_value*

default limit ipsecmgr ikev1 max

default

Sets/Restores default value assigned for specified parameter.

limit

Limits the parameter for this context.

ipsecmgr

To limit ipsecmgr manager settings.

ikev1

Specifies IKEv1 tasks.

max ***max_value***

Specifies maximum ipsecmgr IKEv1 tasks. *max_value* must be an integer from 1 to 176.

Example

Use the following command to limit number of IPSec managers within a context to 23.

limit ipsecmgr ikev1 max*23*

lma-service

Creates an Local Mobility Anchor (LMA) service or specifies an existing LMA service and enters the LMA Service Configuration Mode for the current context.

Product

P-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

lma-service *service_name* **[-noconfirm]**
no lma-service *service_name*

no

Removes the specified LMA service from the context.

service_name

Specifies the name of the LMA service. If *service_name* does not refer to an existing service, the new service is created if resources allow.

service_name is an alphanumeric string of 1 through 63 characters.



Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Enter the LMA Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.



Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-lma-service)#
```

LMA Service Configuration Mode commands are defined in the *LMA Service Configuration Mode Commands* chapter.

Use this command when configuring the following eHRPD and PMIP SAE components: P-GW (SAEGW).

Example

The following command enters the existing LMA Service Configuration Mode (or creates it if it does not already exist) for the service named *lma-service1*:

```
lma-service lma-service1
```

The following command will remove *lma-service1* from the system:

```
no lma-service lma-service1
```

Ins-service

Enters the LNS Service Configuration Mode, or is used to add or remove a specified L2TP Network Server (LNS) service.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] lns-service` *name*

no

Removes the specified lac-service from the current context.

name

Specifies the name of a LNS service to configure, add or remove as an alphanumeric string of 1 through 63 characters that is case-sensitive.



Important Service names must be unique across all contexts within a chassis.

Usage Guidelines

Enter the LNS Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.



Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Example

To add a new LNS service named *LNS1* and enter the LNS Service Configuration Mode, enter the following commands:

```
lns-service LNS1
```

To configure an existing LNS service named *LNS2*, enter the following command:

lns-service LNS2

To delete an existing LNS service named *LNS3*, enter the following command:

no lns-service LNS3

location-service

Creates a location service configuration instance or configures an existing location service configuration and enters the Location Service Configuration Mode. LoCation Services (LCS) are used to determine the geographic location of a UE.

Product

MME

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

location-service *service_name* **[-noconfirm]**
no location-service *service_name*
slr emergency unauth-imsi

no

Removes the specified location service configuration instance from the context.

service_name

Specifies the name of the location service configuration instance. If *service_name* does not refer to an existing service, the new service is created if resources allow.

service_name is an alphanumeric string of 1 through 63 characters.



Important Service names must be unique across all contexts within a chassis.

unauth-imsi

Allows MME to send unauthorized IMSI in LRR message when available.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Enter the Location Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing Service Configuration instance.

Location Service Configuration Mode commands are defined in the *Location Service Configuration Mode Commands* chapter.

A maximum of 16 location service instances can be configured per system.

Entering this command results in the following prompt:

```
[context_name]hostname(config-location-service)#
```

Example

The following command enters the existing Location Service Configuration Mode (or creates it if it does not already exist) for the service named *location-service1*:

```
location-service location-service1
```

The following command will remove *location-service1* from the system:

```
no location-service location-service1
```

logging

Modifies the logging options for a specified system log server for the current context.

Product

All

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] logging syslog *ip_address* **[event-verbosity { min | concise | full } | facility** *facilities* **| msg-format { rfc3164 | rfc5424 } | pdu-data { none | hex | hex-ascii } | pdu-verbosity** *pdu_level* **| port** *number* **rate** *value* **] { first-console }**

no

Indicates that internal logging is to be disabled for the options specified.

syslog *ip_address*

Specifies the IP address of a system log server on the network in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

event-verbosity { min | concise | full }

Specifies the level of detail to use in logging of events. Detail level must be one of the following:

- **min**: Displays minimal detail.
- **concise**:Displays summary detail.
- **full**: Displays full detail.

facility *facilities*

Default: **local7**

Specifies the local facility for which the system logging server's logging options shall be applied. Local facility must be one of the following:

- **local0** — Pertains to syslog severity level of 0, Emergency
- **local1** — Pertains to syslog severity level of 1, Alert
- **local2** — Pertains to syslog severity level of 2, Critical
- **local3** — Pertains to syslog severity level of 3, Error
- **local4** — Pertains to syslog severity level of 4, Warning
- **local5** — Pertains to syslog severity level of 5, Notice
- **local6** — Pertains to syslog severity level of 6, Informational
- **local7** — Pertains to syslog severity level of 7, Debug

If local facility is not specified, then **local7** is applied by default.

Multiple system log servers can share the logging options of a given local facility. This allows for the logical grouping of system log servers and the options which affect all of those associated with the same local facility.

msg-format { rfc3164 | rfc5424 }

Configures the message format for each system log server as per RFC3164 or RFC5424. Default: rfc3164.

pdu-data { none | hex | hex-ascii }

Specifies output format for packet data units when logged. Format must be one of the following:

- **none**: Displays data in raw format.
- **hex**: Displays data in hexadecimal format.
- **hex-ascii**:Displays data in hexadecimal and ASCII format (similar to a main-frame dump).

pdu-verbosity *pdu_level*

Specifies the level of verboseness to use in logging of packet data units as a value from 1 through 5, where 5 is the most detailed.

port *number*

Specifies an alternate port number for the system log server. Default: 514.

number must be an integer value from 1 through 65535.

rate *value*

Specifies the rate at which log entries are allowed to be sent to the system log server. No more than the number specified by *value* will be sent to a system log server within any given one-second interval.

value must be an integer from 0 through 100000. Default: 1000

first-console

Enables the first serial port as the debug console for event log collection.

Note that on a VPC-DI that has a CF and SF card, the CF card on the first serial port is configured as the debug console. The second serial port is configured as the CLI console.



Note The CF card on the VPC-DI and VPC-SI can be configured as the VGA, which also provides the CLI console.

On the SF card, the first serial port is configured as the debug console. The second serial port cannot be configured as the CLI console because there is no support for this console on the SF card.



Note The **logging first-console** CLI command does not enable or disable system logs such as crash logs, system printed logs, and so on, which are always enabled.

Usage Guidelines

Set the log servers to enable remote review of log data.

Example

The following sets the logging for events to the maximum for the local7 facility:

```
logging syslog 10.2.3.4 event-verbosity full
```

The following command sets the logging for packet data units to level 3 and sets the output format to the main-frame style hex-ascii for the local3 facility:

```
logging syslog 10.2.3.4 facility local3 pdu-data hex-ascii pdu-verbosity
 3
```

The following sets the rate of information for the local1 facility:

```
logging syslog 10.2.3.4 facility local1 rate 100
```

The following disables internal logging to the system log server specified:

```
no logging syslog 10.2.3.4
```

The following configure the first serial port as the debug console:

```
logging first-console
```

mag-service

Creates a Mobile Access Gateway (MAG) service or specifies an existing MAG service and enters the MAG Service Configuration Mode for the current context.

Product

HSGW

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

mag-service *service_name* **[-noconfirm]**
no mag-service *service_name*

no

Removes the specified MAG service from the context.

service_name

Specifies the name of the MAG service. If *service_name* does not refer to an existing service, the new service is created if resources allow.

service_name is an alphanumeric string of 1 through 63 characters.



Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Enter the MAG Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.



Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your Cisco service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-mag-service)#
```

MAG Service Configuration Mode commands are defined in the *MAG Service Configuration Mode Commands* chapter.

Use this command when configuring the following eHRPD and PMIP SAE components: HSGW and S-GW.

Example

The following command enters the existing MAG Service Configuration Mode (or creates it if it does not already exist) for the service named *mag-service1*:

mag-service mag-service1

The following command will remove *mag-service1* from the system:

no mag-service mag-service1

map-service

Creates a Mobile Application Part (MAP) Service instance and enters the MAP Service Configuration mode to define or edit the MAP service parameters.

MAP is the SS7 protocol that provides the application layer required by some of the nodes in GPRS/UMTS networks to communicate with each other in order to provide services to mobile phone users. MAP is used by the serving GPRS support node (SGSN) to access SS7 network nodes such as a home location register (HLR) or a radio access network (RAN).

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

map-service *srvc_name*
no map-service *srvc_name*

no

Remove the specified MAP service from the configuration for the current context.

srvc_name

Specifies the name of the MAP service as a unique alphanumeric string of 1 through 63 characters.



Important Service names must be unique across all contexts within a chassis.

Usage Guidelines Use this command to create, edit, or remove a MAP service configuration.



Important For details about the commands and parameters, check the *MAP Service Configuration Mode Commands* chapter.

Example

The following command creates a MAP service named *map_1*:

```
map-service map_1
```

The following command removes the configuration for a MAP service named *map_1* from the configuration for the current context:

```
no map-service map_1
```

max-sessions

Configures the maximum simultaneous sessions allows for corresponding users.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
max-sessions number { administrator name user_name | config-administrator
name user_name | inspector name user_name | operator name user_name }
no max-sessions { administrator name user_name | config-administrator name
 user_name | inspector name user_name | operator name user_name }
default max-sessions { administrator name user_name | config-administrator
 name user_name | inspector name user_name | operator name user_name }
```

max-sessions *number*

Specifies the maximum number of simultaneous CLI sessions. It must be an alphanumeric integer from 1 to 100. **Default**: No limit.

administrator

Configures login user with security administrator rights for specific content. A username must follow the **administrator** keyword.

config-administrator

Configures login user with configuration administrator rights for specific content. A username must follow the **config-administrator** keyword.

inspector

Configures login user with inspector rights for specific content. A username must follow the **inspector** keyword.

operator

Configures login user with operator rights for specific content. A username must follow the **operator** keyword.

name *user_name*

Specifies the username. *user_name* specifies the security username. It must be an string size from 1 to 32.

no

Removes the configured maximum number of simultaneous CLI sessions. This option returns the user to the default setting. If the user does not exist, then an error message appears stating: 'Failure: User x has not been configured. Configure it first!'.

default

Removes the configured maximum number of simultaneous CLI sessions and returns the user to the default number. **Default**: No limit.

Usage Guidelines

This command allows administrative users the ability configure the maximum simultaneous sessions allowed for corresponding users.

Example

The following command allows an administrator the ability to configure 4 simultaneous sessions for user 5.

max-sessions 4 administrator name 5

mipv6ha-service

Creates a Mobile IPv6 Home Agent (MIPv6-HA) service instance and enters the MIPv6 HA Service Configuration mode to define or edit the MIPv6-HA service parameters.

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

mipv6ha-service *srvc_name*
no mipv6ha-service *srvc_name*

no

Remove the specified MIPv6-HA service from the configuration for the current context.

srvc_name

Specifies the name of the MIPv6-HA service as a unique alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines

Use this command to create, edit, or remove a MIPv6-HA service configuration.

Important For details about the commands and parameters, check the *MIPv6 HA Service Configuration Mode Commands* chapter.

Example

The following command creates a MIPv6-HA service named *mipv6ha_1*:

```
mipv6ha-service mipv6ha_1
```

The following command removes the configuration for a MIPv6-HA service named *mipv6ha_1* from the configuration for the current context:

```
no mipv6ha-service mipv6ha_1
```

mme-embms-service

Creates an MME-eMBMS service or configures an existing MME-eMBMS service. As well, this command enters the MME-eMBMS Service configuration mode. MME-eMBMS service handles the MME's Multimedia Broadcast/Multicast Service (MBMS) functional for Evolved Packet Core (EPC) networks in the current context.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
mme-embms-service service_name [ -noconfirm ]
no mme-embms-service service_name
```

no

Removes the specified MME-eMBMS service from the context.

service_name

Specifies the name of the MME-eMBMS service. If *service_name* does not refer to an existing service, the new service is created if resources allow.

service_name is an alphanumeric string of 1 through 63 characters.



Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Enter the MME-eMBMS Service configuration mode to access the commands needed to setup or modify either a newly defined service or an existing service. This command is also used to remove an existing MME-eMBMS service from the MME's configuration.

A maximum of 8 MME-eMBMS services can be configured on a system which is further limited to a maximum of 256 services (regardless of type) can be configured per system.



Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-mme-embms-service)#
```

MME Service Configuration Mode commands are defined in the *MME Service Configuration Mode Commands* chapter.

Example

The following command enters the existing MME-eMBMS Service configuration mode (or creates it if it does not already exist) for the service named *embms1*:

```
mme-embms-service embms1
```

The following command will remove *embms1* from the system:

```
no mme-embms-service embms1
```

mme-service

Creates an Mobility Management Entity (MME) service or configures an existing MME service and enters the MME Service Configuration Mode for Evolved Packet Core (EPC) networks in the current context.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
mme-service service_name [ -noconfirm ]
  n1-mode 5gs-interworking-with-n26 [ sgw-selection { s5-or-s8 | s11 [
ue-usage-type  ue-usage-type-val [ ue-usage-type-val+ ] ]} ]
     [ no ] n1-mode 5gs-interworking-with-n26
     [ no ] n1-mode 5gs-interworking-with-n26 sgw-selection s11 [
ue-usage-type  ue-usage-type-val [ue-usage-type-val+ ] ]
  [ release-s1-s11-on-timer-expiry-upon-clr ]
  no mme-service service_name [ release-s1-s11-on-timer-expiry-upon-clr ]
  [ no ] delete-old-on-duplicate-enodeb-detection
  [ no ] oldtac-dsr-attach-over-attach
```

no

Removes the specified MME service from the context.

service_name

Specifies the name of the MME service. If *service_name* does not refer to an existing service, the new service is created if resources allow.

service_name is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

n1-mode 5gs-interworking-with-n26 [sgw-selection { s5-or-s8 | s11 [ue-usage-type ue-usage-type-val [ue-usage-type-val+]]}]

n1-mode: Configures interworking with 5Gs for UEs supporting N1 mode.

5gs-interworking-with-n26: Enables 5GS-EPS interworking with N26 interface.

no: Disables 5GS-EPS interworking with N26 interface.

sgw-selection: Allows dynamic S-GW selection based on either s11 or s5-or-s8. Defaults to s5-or-s8. Value under the Call Control Profile takes precedence over value under the MME service.

- **s5-or-s8**: Dynamic S-GW selection based on the s5-or-s8 interface.
- **s11**: Dynamic S-GW selection based on the s11 interface.
- **ue-usage-type**: Specifies upto eight UE usage type integer values in the range 128–255.

release-s1-s11-on-timer-expiry-upon-clr

MME to wait for timer expiry after receiving a Cancel Location Request (CLR) from the HSS for EPS to 5GS Mobility registration procedure before releasing S1 and S11.

[no] release-s1-s11-on-timer-expiry-upon-clr

MME releases resources instantly when CLR is received.

[no] delete-old-on-duplicate-enodeb-detection

The **mmedemux** deletes the old stale path and establishes a new path. By default it is disabled.



Note The **delete-old-on-duplicate-enodeb-detection** CLI is a critical parameter, which will restart the mme service and remove active sessions.

no : The **mmedemux** retains the old eNodeB path.

[no] oldtac-dsr-attach-over-attach

Configures the MME to send old TAC Id in delete session request for old sessions in attach over attach scenario.

no: Disables the CLI **oldtac-dsr-attach-over-attach**.

Usage Guidelines

Enter the MME Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 8 MME service can be configured on a system which is further limited to a maximum of 256 services (regardless of type) can be configured per system.

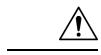


Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-mme-service)#
```

MME Service Configuration Mode commands are defined in the *MME Service Configuration Mode Commands* chapter.



Caution This is a critical configuration. The MME service cannot be configured without this configuration. Any change to this configuration would lead to restarting the MME service and removing or disabling this configuration will stop the MME service.

Example

The following command enters the existing MME Service Configuration Mode (or creates it if it does not already exist) for the service named *mme-service1*:

```
mme-service mme-service1
```

The following command will remove *mme-service1* from the system:

```
no mme-service mme-service1
```

The following **no n1-mode 5gs-interworking-with-n26sgw-selections ue-usage-type 130** CLI command indicates that if the N1 mode is configured and sgw-interface is configured with s11 and ue-usage-type in the MME Service, then Ue-usage 130 gets removed using the **no** option.

mobile-access-gateway

Controls whether duplicate MAG sessions are allowed in HSGW. By default, duplicate sessions are rejected.

Product

HSGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
mobile-access-gateway newcall duplicate-session { purge | reject }
[ default | no ] mobile-access-gateway newcall duplicate-session
```

default | no

Disables the feature. New session create request is discarded.

newcall duplicate-session { purge | reject }

Determines new call related behavior on context when duplicate MAG sessions are requested in HSGW (Mobile Access Gateway).

purge: Enables the feature. Old MAG session is deleted and new session create request is rejected, but on retry the new call comes up.

reject: Disables the feature. Rejects new call with duplicate session create request; new session create request is discarded.

Usage Guidelines

This command controls whether duplicate MAG sessions are allowed in HSGW.

When enabled, HSGW rejects new session create request initially and creates new call on retry.

When disabled, HSGW rejects new call and new session create request is discarded.

Example

The following command allows duplicate MAG sessions in HSGW on this context:

mobile-access-gateway newcall duplicate-session purge

mobile-ip fa

Configures settings that effect all FA services in the current context.

Product

FA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
mobile-ip fa { multiple-dynamic-reg-per-nai | newcall
duplicate-home-address { accept | reject } }
{ default | no } mobile-ip fa { multiple-dynamic-reg-per-nai | newcall
duplicate-home-address }
```

default

Configures the default setting for the specified parameter.

- **multiple-dynamic-reg-per-nai**:All FA services in the current context can not simultaneously setup multiple dynamic home address registrations that have the same NAI.
- **newcall duplicate-home-address**: **reject**

no

- **multiple-dynamic-reg-per-nai**: Disables all FA services in the current context from simultaneously setting up multiple dynamic home address registrations that have the same NAI.
- **newcall duplicate-home-address**:Resets this option to its default of reject.

multiple-dynamic-reg-per-nai

This keyword allows all FA services in the current context to simultaneously setup multiple dynamic home address registrations that have the same NAI.

newcall duplicate-home-address { accept | reject }

- **accept**: The new call is accepted and the existing call is dropped.
- **reject**: The new call is rejected with an Admin Prohibited code.

Usage Guidelines

Use this command to set the behavior of all FA services in the current context.

Example

To configure all FA services to accept new calls and drop the existing call when the new call requests an IP address that is already in use by an existing call, enter the following command:

```
mobile-ip fa newcall duplicate-home-address accept
```

To enable all FA services in the current context to allow all FA services in the current context to simultaneously setup multiple dynamic home address registrations that have the same NAI, enter the following command:

```
mobile-ip fa multiple-dynamic-reg-per-nai
```

mobile-ip ha assignment-table

Creates a Mobile IP HA assignment table and enters Mobile IP HA Assignment Table Configuration Mode.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

mobile-ip ha assignment-table *atable_name* **[-noconfirm]**
no mobile-ip ha assignment-table *atable_name*

no

This keyword deletes the specified assignment table

atable_name

Specifies the name of the MIP HA assignment table to create or edit as an alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to create a new MIP HA assignment table or edit an existing MIP HA assignment table.



Important A maximum of eight MIPHA assignment tables can be configured per context with a maximum of 8 MIP HA assignment tables across all contexts.



Important A maximum of 256 non-overlapping hoa-ranges can be configured per MIP HA Assignment table with a maximum of 256 non-overlapping hoa-ranges across all MIP HA Assignment tables.

Example

The following command creates a new MIP HA assignment table name *MIPHAtable1* and enters MIP HA Assignment Table Configuration Mode without asking for confirmation from the user:

```
mobile-ip ha assignment-table MIPHAtable1
```

mobile-ip ha newcall

Configures the behavior of all HA services when duplicate home addresses and duplicate IMSI sessions occur for new calls.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
mobile-ip ha newcall { duplicate-home-address { accept | reject } |
duplicate-imsi-session { allow | disallow | global-disallow } |
wimax-session-overwrite { allow | disallow }
```

{ default | no } mobile-ip ha newcall { duplicate-home-address | duplicate-imsi-session | wimax-session-overwrite }

default

Configures the default setting for the specified parameter.

- **duplicate-home-address**: **reject**—sets HA services to reject a new call that requests an IP address that is already assigned.
- **duplicate-imsi-session**: **allow**—sets HA services to accept new calls that have the same IMSI as a call that is already active.
- **wimax-session-overwrite:disallow**—disable session overwrite feature for WiMax mobile-ip calls on the HA.

no

Configures the default setting for the specified parameter.

duplicate-home-address { accept | reject }

Configures the HA to either accept or reject new calls if the new call requests a static IP home address that is already assigned to an existing call from an IP address pool in the same destination context.

- **accept**: The new call is accepted and the existing call is dropped.
- **reject**: The new call is rejected with an Admin Prohibited code.

duplicate-imsi-session { allow | disallow | global-disallow }

Configures the HA to either permit or not permit multiple sessions for the same IMSI.

- **allow**: Allows multiple sessions for the same IMSI.
- **disallow**: If a mobile node already has an active session and a new sessions is requested using the same IMSI, the currently active session is dropped and the new session is accepted.
- **global-disallow**: Enables HA services in this context to accept a new session and disconnect any other session(s) having the same IMSI being processed in this context. In addition, a request is sent to all other contexts containing HA services to do the same.



Important In order to ensure a single session per IMSI across all contexts containing HA services, the global-disallow option must be configured in every context.

wimax-session-overwrite { allow | disallow }

Use this command to enable or disable the overwrite feature for WiMAX mobile ip (MIPv4) calls on the HA.

Usage Guidelines

Use this command to set the behavior of all HA services for new calls.

Example

To configure all HA services to accept new calls when the new call requests a static IP that is already assigned from an IP pool in the same destination context, enter the following command:

```
mobile-ip ha newcall duplicate-home-address accept
```

To configure all HA services to drop an active call and accept a new one that uses the same IMSI, enter the following command:

```
mobile-ip ha newcall duplicate-imsi-session disallow
```

mobile-ip ha reconnect

Sets the behavior of all HA services to reconnect dropped calls.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] mobile-ip ha reconnect [ static-homeaddr [ dynamic-pool-allocation
 ] ] }
```

static-homeaddr

Specifies that the home address as a static IP address.

dynamic-pool-allocation

Allows a dynamic pool to accept a static address allocation.

Usage Guidelines

Use this command to reset the HA behavior for new calls.

Example

```
mobile-ip ha reconnect
mobile-ip ha reconnect static-homeaddr
mobile-ip ha reconnect static-homeaddr dynamic-pool-allocation
no mobile-ip ha reconnect
no mobile-ip ha reconnect static-homeaddr
```

monitor-protocols

Enters the Monitor Protocols configuration mode.

Product

CUPS

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

monitor-protocols

Usage Guidelines

The Monitor Protocols configuration mode contains commands used to configure protocol monitoring groups (relationships) between the current device and a remote peer.

Configure monitor protocol groups on both the CP and UP and within the same context as the CUPS Sx interface.

mpls bgp forwarding

Globally enables Multi protocol Label Switching (MPLS) Border Gateway Protocol (BGP) forwarding.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

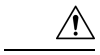
[no] mpls bgp forwarding

no

Disables MPLS BGP forwarding.

Usage Guidelines

Use this command to globally enable the MPLS BGP forwarding. By enabling this command, the BGP VPNv4 routes need not have an underlying LSP to forward the IP packets. If this command is not enabled, then the nexthop for the BGP routes must be reachable via LDP.



Caution This command should always be enabled when nexhtop is not reachable thorough LSP.

Example

The following command enables the MPLS BGP forwarding on the system:

```
mpls bgp forwarding
```

mpls exp

Sets the default behavior as Best Effort using a zero value in the 3-bit MPLS EXP (Experimental) header. This setting overrides the value sent by the mobile subscriber.

Product

eHRPD

GGSN

PDSN (HA)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] mpls exp *<value>*

no

Reverts back to the default behavior, which is to copy the DSCP from the mobile subscriber packet to the EXP header of the packet, if there is no explicit configuration for DSCP to EXP.

<value>

Specifies the MPLS EXP header value as an integer from 0 through 7. Higher value indicates higher priority.

Usage Guidelines

Set the default behavior as Best Effort using a zero value in the 3-bit MPLS EXP header. This value applies to all the VRFs in the context. The default behavior is to copy the DSCP value of mobile subscriber traffic to the EXP header, if there is no explicit configuration for DSCP to EXP (via the **mpls map-dscp-to-exp dscp** <*n*> **exp** <*m*> command).

This command disables the default behavior and sets the EXP value to the configured <value>.

Example

The following command sets the MPLS EXP header value to 2:

```
mpls exp 2
```

mpls ip

Globally enables the Multiprotocol Label Switching (MPLS) forwarding of IPv4 packets along normally routed paths.

Product

GGSN

HA

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] mpls ip

no

Disables MPLS forwarding of IPv4 packets configured on the system. **no mpls ip** stops dynamic label distribution on all the interfaces regardless of interface configuration.

Usage Guidelines

Globally enables the MPLS forwarding of IPv4 packets along normally routed paths for the entire context.

It does not start label distribution over an interface until MPLS has been enabled for the interface as well. Refer to the *Ethernet Interface Configuration Mode Commands* chapter for additional information.



Caution This feature is not enabled by default.

Example

Following command enables (but does not start) MPLS forwarding of IPv4 packets along normally routed paths:

```
mpls ip
```

mseg-service

This command is not supported in this release.

multicast-proxy

Creates, configures or deletes a multicast proxy host configuration.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] multicast-proxy { igmp interface *ip_address* **range-start** *start_ip_address* **range-end** *end_ip_address* **| listen address** *listen_ip_address* **port** *port_number* **protocol** *protocol_number* **sessmgr** *instance* **}**

no

If previously configured, deletes the specified multicast proxy parameter from the current context.

igmp interface *ip_address* range-start *start_ip_address* range-end *end_ip_address*

Specifies the IP address and range of associated addresses for this Internet Group Management Protocol (IGMP) interface.

ip_address is the IP address of this interface expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

range-start *start_ip_address* is the start point for the multicast address range expressed in IPv4dotted-decimal or IPv6 colon-separated-hexadecimal notation.

range-end *end_ip_address* is the end point for the multicast address range expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. *end_ip_address*

listen address *listen_ip_address* port *port_number* protocol *protocol_number* sessmgr *instance*

Configures this context as a multicast proxy listener.

listen_ip_address is the IP address that will be listened to, expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

port *port_number* is the port number which will be listened to. If this is not provided, the listener will receive all packets from the *listen_ip_address*. *port_number* is an integer from 1 through 65535.

protocol *protocol_number* is the IANA protocol number associated with the port number. If this is not provided, the listener will receive all packets from the *listen_ip_address* and *port_number*. *protocol_number* is an integer from 1 through 255.

sessmgr *instance* session manager instance that will do the listening. *instance* is an integer from 1 through 270.

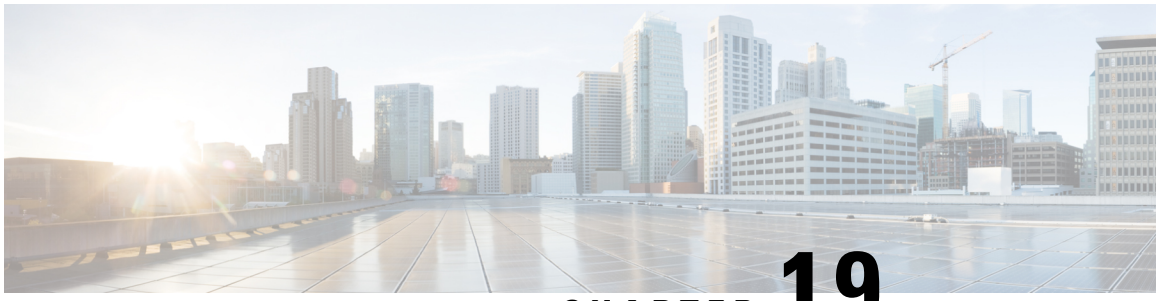
Usage Guidelines

Use this command to create/configure/delete a multicast proxy host configuration.

Example

The following command creates an IGMP multicast host configuration:

```
multicast proxy igmp interface 192.51.1.34 range-start 255.0.0.0 range-end
 255.0.0.1
```



CHAPTER 19

Context Configuration Mode Commands N-R

Command Modes

This section includes the commands **nw-reachability server** through **router** service.

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

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

- nw-reachability server, on page 605
- network-requested-pdp-context activate, on page 606
- network-requested-pdp-context gsn-map, on page 608
- network-requested-pdp-context hold-down-time, on page 609
- network-requested-pdp-context interval, on page 610
- network-requested-pdp-context sgsn-cache-time, on page 610
- operator, on page 611
- optimize pdsn inter-service-handoff, on page 615
- password, on page 615
- pcc-af-service, on page 618
- pcc-policy-service, on page 620
- pcc-service, on page 621
- pcc-sp-endpoint, on page 623
- pdg-service, on page 624
- pdif-service, on page 625
- pdsn-service, on page 626
- pdsnclosedrp-service, on page 627
- pgw-service, on page 628
- policy, on page 629
- policy-group, on page 630
- policy-map, on page 631
- ppp, on page 632

- ppp magic-number, on page 637
- ppp statistics, on page 638
- proxy-dns intercept-list, on page 639
- rac-profile, on page 640
- radius accounting, on page 640
- radius accounting algorithm, on page 643
- radius accounting apn-to-be-included, on page 644
- radius accounting billing-version, on page 645
- radius accounting gtp trigger-policy, on page 646
- radius accounting ha policy, on page 647
- radius accounting interim volume, on page 648
- radius accounting ip remote-address, on page 649
- radius accounting keepalive, on page 650
- radius accounting rp, on page 651
- radius accounting server, on page 654
- radius algorithm, on page 658
- radius allow, on page 659
- radius attribute, on page 660
- radius authenticate null-username, on page 662
- radius authenticate apn-to-be-included, on page 663
- radius authenticator-validation, on page 663
- radius change-authorize-nas-ip, on page 664
- radius charging, on page 667
- radius charging accounting algorithm, on page 668
- radius charging accounting server, on page 669
- radius charging algorithm, on page 671
- radius charging server, on page 672
- radius deadtime, on page 674
- radius detect-dead-server, on page 675
- radius dictionary, on page 677
- radius group, on page 678
- radius ip vrf, on page 678
- radius keepalive, on page 679
- radius max-outstanding, on page 681
- radius max-retries, on page 682
- radius max-transmissions, on page 683
- radius mediation-device, on page 684
- radius probe-interval, on page 684
- radius probe-max-retries, on page 685
- radius probe-message, on page 686
- radius probe-timeout, on page 686
- radius server, on page 687
- radius strip-domain, on page 690
- radius timeout, on page 690
- radius trigger, on page 691
- realtime-trace-module, on page 692

- remote-server-list, on page 693
- route-access-list extended, on page 694
- route-access-list named, on page 695
- route-access-list standard, on page 697
- route-map, on page 698
- router, on page 699

nw-reachability server

Adds or deletes a reachability-detect server and configures parameters for retrying the failure-detection process. When network reachability is enabled, an ICMP ping request is sent to this device. If there is no response after a specified number of retries, the network is deemed failed. Execute this command multiple times to configure multiple network reachability servers.

Product

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

nw-reachability server *server_name* **[interval** *seconds* **] [local-addr** *ip_addr* **] [num-retry** *num* **] [remote-addr** *ip_addr* **] [timeout** *seconds***] [vfr** *name***]**
no nw-reachability server *server_name*

no

Delete the reference to the specified network reachability server.

server_name

Specifies the name for the network device that is sent ping packets to test for network reachability.

interval ***seconds***

Specifies the frequency in seconds for sending ping requests as an integer from 1 through 3600. Default: 60

local-addr ***ip_addr***

Specifies the IP address to be used as the source address of the ping packets; If this is unspecified, an arbitrary IP address that is configured in the context is used. *ip_addr* must be entered using IPv4 dotted-decimal notation.

num-retry ***num***

Specifies the number of retries before deciding that there is a network-failure as an integer from 0 through 100. Default: 5

remote-addr *ip_addr*

Specifies the IP address of a network element to use as the destination to send the ping packets for detecting network failure or reachability. *ip_addr* must be entered using IPv4 dotted-decimal notation.

timeout *seconds*

Specifies how long to wait (in seconds) before retransmitting a ping request to the remote address as an integer from 1 through 1. Default: 3

vrf *name*

Specifies an existing VRF name as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to set up a network device on a destination network that is used ensure that Mobile IP sessions can reach the required network from the P-GW.

Important Refer to the P-GW Configuration Mode command **policy nw-reachability-fail** to configure the action that should be taken when network reachability fails.

Important Refer to the Subscriber Config Mode command **nw-reachability-server** to bind the network reachability to a specific subscriber.

Important Refer to the **nw-reachability server server_name** keyword of the **ip pool** command in this chapter to bind the network reachability server to an IP pool.

Example

To set a network device called Internet Device with the IP address of *192.51.100.10* as the remote address that is pinged to determine network reachability and use the address *192.51.100.10* as the origination address of the ping packets sent, enter the following command:

```
nw-reachability server InternetDevice local-addr 192.51.100.10 remote-addr
 192.51.100.10
```

network-requested-pdp-context activate

Configures the mobile station(s) (MSs) for which network initiated PDP contexts are supported.

Product GGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

network-requested-pdp-context activate address *ip_address* **dst-context** *context_name* **imsi** *imsi* **apn** *apn_name*
no network-requested-pdp-context activate address *ip_address* **dst-context** *context_name*

no

Disables the system's ability to accept network-requested PDP contexts on the specified interface.

ip_address

Specifies the static IP address of the MS n IPv4 dotted-decimal notation.

dst-context *context_name*

Specifies the name of the destination context configured on the system containing the static IP address pool in which the MS's IP address is configured. *context_name* is an alphanumeric string of 1 through 79 characters that is case sensitive.

imsi *imsi*

Specifies the International Mobile Subscriber Identity (IMSI) of the MS as a string of 1 through 15 numeric characters

apn *apn_name*

Specifies the Access Point Name (APN) that is passed to the SGSN by the system. *apn_name* is an alphanumeric string of 1 through 63 characters that is case sensitive.

Usage Guidelines

Use this command to specify the MS(s) for which network initiated PDP contexts are supported.

When a packet is received for an MS that does not currently have a PDP context established, the system checks the configuration of this parameter to determine if the destination IP address specified in the packet is specified by this parameter. If the address is not specified, then the system discards the packet. If the address is specified, the system uses the configured IMSI and APN to determine the appropriate SGSN from the Home Location Register (HLR). The system communicates with the HLR through the interworking node configured using the network-requested-pdp-context gsn-map command.

Once the session is established, the destination context specified by this command is used in place of the one either configured within the specified APN template or returned by a RADIUS server during authentication.

This command can be issued multiple times supporting network initiated PDP contexts for up to 1,000 configured addresses per system context.

Example

The following command enables support for network initiated PDP contexts for an MS with a static IP address of *20.13.5.40* from a pool configured in the destination context pdn1 with an IMSI of *3319784450* that uses an APN template called *isp1*:

```
network-requested-pdp-context activate address 20.13.5.40 dst-context
pdn1 imsi 3319784450 apn isp1
```

network-requested-pdp-context gsn-map

Configures the IP address of the interworking node that is used by the system to communicate with the Home Location Register (HLR), and optionally sets the GTP version to use.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

network-requested-pdp-context gsn-map *ip_address* **[gtp-version { 0 | 1 }]**
no network-requested-pdp-context gsn-map

no

Deletes a previously configured gsn-map node.

ip_address

Specifies the IP address of the gsn-map node in Pv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

gtp-version { 0 | 1 }

Specifies the gtp version used. Default: 1

Usage Guidelines

Communications from the system to the HLR must go through a GSN-map interworking node that performs the protocol conversion from GTPC to SS7.

The UDP port for this communication is 2123.

Support for network requested PDP contexts must be configured within source contexts on the system. Only one gsn-map node can be configured per source context.

The source context also contains the GGSN service configuration that specifies the IP address of the Gn interface. If multiple GGSN services are configured in the source context, one is selected at random for initiating the Network Requested PDP Context Activation procedure.

Communication with the gsn-map node is done over the Gn interface configured for the GGSN service. The IP address of that interface is used as the system's source address.

Example

The following command configures the system to communicate with a gsn-map node having an IP address of *192.51.100.2*:

```
network-requested-pdp-context gsn-map 192.51.100.2
```

network-requested-pdp-context hold-down-time

Configures the time duration to that the system will wait after the SGSN rejects an attempt for a network-requested PDP context creation for the subscriber.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
network-requested-pdp-context hold-down-time time
default network-requested-pdp-context hold-down-time
```

default

Configures the default setting.

Default:60 seconds

time

Specifies the time interval (in seconds) as an integer from 0 through 86400.

Usage Guidelines

Packets received during this time period would be discarded, rather than being used to cause another network-requested PDP context creation attempt for the same subscriber. After the time period has expired, any subsequent packets received would cause another network-requested PDP context creation procedure to begin.

Example

The following command configures a hold-down-time of *120* seconds:

```
network-requested-pdp-context hold-down-time 120
```

network-requested-pdp-context interval

Configures the minimum amount of time that must elapse between the deletion of a network initiated PDP context and the creation of a new one for the same MS.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

network-requested-pdp-context interval *time*
default network-requested-pdp-context interval

default

Returns the command to its default setting of 60.

time

Specifies the minimum amount of time (in seconds) that must pass before the system allows another network-requested PDP context for a specific MS after the previous context was deleted. *time* is an integer from 0 through 86400. Default: 60

Usage Guidelines

Once an MS deletes a PDP context that initiated from the network, the system automatically waits the amount of time configured by this parameter before allowing another network initiated PDP context for the same MS.

Example

The following command specifies that the system waits *120* seconds before allowing another network requested PDP context for an MS:

network-requested-pdp-context interval 120

network-requested-pdp-context sgsn-cache-time

Configures the time duration that the GGSN keeps the SGSN/subscriber pair cached in its local memory.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

network-requested-pdp-context sgsn-cache-time *time*
default network-requested-pdp-context sgsn-cache-time

default

Configures the default setting.

Default: 300 seconds

time

Specifies the time interval (in seconds) as an integer from 0 through 86400.

Usage Guidelines

For an initial network-requested PDP context creation, the system contacts the HLR (via the GSN-MAP interworking node) to learn which SGSN is currently servicing the subscriber. The system keeps that information in cache memory for the configured time, so that future network-requested PDP context creations for that subscriber can be initiated without having to contact the HLR again.

Example

The following command configures an sgsn-cache-time of *500* seconds:

```
network-requested-pdp-context sgsn-cache-time 500
```

operator

Configures a context-level operator account within the current context.

Product

All

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

operator *user_name* **[encrypted] [nopassword] password** *password* **[ecs] [expiry-date** *date_time* **] [li-administration] [noconsole] [noecs] [timeout-absolute** *abs_seconds* **] [timeout-min-absolute** *abs_minutes* **] [timeout-idle** *timeout_duration* **] [timeout-min-idle** *idle_minutes* **][exp-grace-interval** *days***][exp-warn-interval** *days***][no-exp-grace-interval][no-exp-warn-interval]**
no operator *user_name*

no

Removes a previously configured context-level operator account.

user_name

Specifies a name for the account as an alphanumeric string of 1 through 32 characters.

[encrypted] password *password*

Specifies the password to use for the user which is being given context-level operator privileges within the current context. The **encrypted** keyword indicates the password specified uses encryption.

password is an alphanumeric string of 1 through 63 characters without encryption, or 1 through 127 with encryption.

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

[nopassword]

This option allows you to create an operator without an associated password. Enable this option when using ssh public keys (**authorized key** command in SSH Configuration mode) as a sole means of authentication. When enabled this option prevents someone from using an operator password to gain access to the user account.

ecs

Permits the specific user to access ACS-specific configuration commands from Exec Mode only. Default: ACS-specific configuration commands are not allowed.

expiry-date *date_time*

Specifies the date and time that this account expires. Enter the date and time in the format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss.

Where YYYY is the year, MM is the month, DD is the day of the month, HH is the hour, mm is minutes, and ss is seconds.

li-administration

Refer to the *Lawful Intercept Configuration Guide* for a description of this parameter.

noconsole

Disables user access to a Console line.



Note The Global Configuration mode **local-user allow-aaa-authentication noconsole** command takes precedence in a normal (non-Trusted) StarOS build. In this case, all AAA-based users cannot access a Console line.

noecs

Prevents the user from accessing ACS-specific configuration commands. Default: Enabled

timeout-absolute *abs_seconds*

This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.

Specifies the maximum amount of time (in seconds) the context-level operator may have a session active before the session is forcibly terminated. *abs_seconds* must be a value in the range from 0 through 300000000. The value 0 disables the absolute timeout. Default: 0

timeout-min-absolute *abs_minutes*

Specifies the maximum amount of time (in minutes) the context-level operator may have a session active before the session is forcibly terminated. *abs_minutes* must be an integer from 0 through 300000000. The value 0 disables the absolute timeout. Default: 0

timeout-idle *timeout_duration*

This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.

Specifies the maximum amount of idle time (in seconds) the context-level operator may have a session active before the session is terminated. *timeout_duration* must be an integer from 0 through 300000000. The value 0 disables the idle timeout. Default: 0

timeout-min-idle *idle_minutes*

Specifies the maximum amount of idle time (in minutes) the context-level operator may have a session active before the session is terminated. *idle_minutes* must be an integer from 0 through 300000000. The value 0 disables the idle timeout. Default: 0

Usage Guidelines

Use this command to create new context-level operator or modify existing operator's options, in particular, the timeout values.

Operators have read-only privileges. They can maneuver across multiple contexts, but cannot perform configuration operations. Refer to the *Command Line Interface Overview* chapter for more information.



Important A maximum of 128 administrative users and/or subscribers may be locally configured per context.

[max-age *days*]

Defines the maximum age of a user password before it has to be changed. **max-age** is the replacement for **expiry-date**.

[no-max-age]

This parameter ensures that password never expires (these are non expiring passwords).

exp-warn-interval *days*

Impends password expiry warning interval in days. There is no default value at per user level. If any of the value is specified, Context global values are considered.

For example:

```
operator trexpac111 password pass@1234
```

In the previous example, there are no values for expiry, grace, and warn are provided. In this case, Global values for both of them will be considered.

[no-exp-warn-interval]

Disables impending password expiry warnings .

exp-grace-interval *days*

Specifies password expiry grace interval in days. Default = 3 days after expiry.

[no-exp-grace-interval]

Disables grace period of expired password.

Example

The following command creates a context-level operator account named *user1* with ACS control:

operator user1 password secretPassword ecs

The following command removes a previously configured context-level operator account named *user1*:

no operator user1

Example

The following command shows the notifications you will receive if the password is not reset before the expiration date:

operator *user_name* **password** *password* **[max-age** *days***][password-exp-grace-interval** *days***][password-exp-grace-interval** *days***]**

```
login: xxx
password: xxx
1. <Normal>
# <you are logged in>

2. <When in warning period>
Warning: Your password is about to expire in 0 days.
We recommend you to change password after login.
Logins are not allowed without acknowleding this.
Do you wish to continue [y/n] (times out in 30 seconds) :

3.<when in grace period>
Your password has expired
Current password:
New password:
Repeat new password:
```

```
4. <after the grace period>
Password Expired (even beyond grace period, if configured). Contact Security Administrator
 to reset password
```

optimize pdsn inter-service-handoff

Controls the optimization of the system's handling of inter-PDSN handoffs.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ default | no ] optimize pdsn inter-service-handoff`

default

Resets the command to its default setting of enabled.

no

Disables the feature.

Usage Guidelines

When more than one PDSN service is defined in a context, each PDSN-Service acts as an independent PDSN. When a Mobile Node (MN) moves from one PDSN service to another PDSN service, by rule, it is an inter-PDSN handoff. This command optimizes PDSN handoffs between PDSN Services that are defined in the same context in the system.

The default for this parameter is enabled. The no keyword disables this functionality.

When enabled, the system treats handoffs happening between two PDSN services in the same context as an inter-PDSN handoff. Existing PPP session states and connection information is reused. If the inter-PDSN handoff requires a PPP restart, then PPP is restarted. The optimized inter-service-handoff may not restart the PPP during handoffs allowing the MN to keep the same IP address for the Simple IP session.

Example

`optimize pdsn inter-service-handoff`

password

Configures password rules (exp-grace-interval, exp-warn-interval, max-age, complexity, and minimum length) to be enforced for all users in this context.

Product All

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[default] password { [{ [complexity { ansi-t1.276-2003 | none }] } [auto-generate]
[none | password min-length *min_size* **][lockout-password-aging** *days* **][password exp-grace-interval** *days***][password exp-warn-interval** *days* **][password max-age** *days***]**

[default] password {exp-grace-interval | exp-warn-interval | max-age}

[default] no password {exp-grace-interval | exp-warn-interval | max-age}

default

The default password complexity is **ansi-t1.276-2003**.

The default minimum length is **8**.

The default password expiry warning interval is **30** days before expiry.

The default password expiry grace interval is **3** days after expiry.

The default value of max-age parameter is **90** days.

Note For non-default commands, the 3 variables needs *days* as an input

complexity { ansi-t1.276-2003 | none }

Specifies the complexity to be enforced for all context user passwords.

ansi-t1.276-2003 requires that all context user passwords comply with the following rules:

- Passwords may not contain the username or the reverse of the username

  .
- Passwords may contain no more than three of the same characters used consecutively.
- Passwords must contain at least three of the following:
  - uppercase alpha character (A, B,C, D...Z)
  - lowercase alpha character (a, b, c, d ...z)
  - numeric character (0, 1, 2, 3...)
  - special character (see the *Alphanumeric Stirngs* section of the *Command Line Interface Overview* chapter)

none results in only the password length being checked.

[auto-generate [none | length *password-length*]

Presents an automatically generated password to the user at login when password is found weak.

The auto-generate option is enabled by default with the password length of 8.

none : Specifies that the user must not be presented with the option to automatically generate a password.

length *password-length* : Specifies the length of the automatically-generated password for the user. The length of the automatically-generated password is an integer between 6 to 127.

exp-warn-interval *days*

Impends password expiry warning interval in days. Default = 30 days before expiry.

exp-grace-interval *days*

Specifies password expiry grace interval in days. Default = 3 days after expiry.

[lockout-password-aging *days*]

Specifies that the user account gets locked after passoword expiration

[no-lockout-password-aging *days*]

Specifies that the user account doest not get locked out after password expiration

max-age *days*

Defines the max-age of a user password before it has to be changed. Default = 90 days.

Description:

The password expiration notification to Context/AAA/Radius users is enhanced. With the enhancement after password expiry and within the grace period, you can log in and change the password on your own. Beyond the grace period, the security administrator will reset the password for you. The following password change prompt is displayed:

```
WARNING: Your password has expired.
You must change your password now and login again!
(current)  password:
Enter new  password:
Retype new password:
```

For example:

```
login: xxx
password: xxx

Case 1: [Normal]
# {you are logged in}

Case 2: [When in warning period]
Warning: Your password is about to expire in 0 days.
We recommend you to change password after login.
Logins are not allowed without acknowleding this.
Do you wish to continue [y/n] (times out in 30 seconds) :
```

```
Case 3: [when in grace period]
Your password has expired
Current password:
New password:
Repeat new password:

Case 4: [after the grace period]
Password Expired (even beyond grace period, if configured). Contact Security Administrator
to reset password
```

Usage Guidelines Use this command to specify the complexity and minimum length of all passwords assigned within this context.

Example

The following commands set the password complexity to ANSI-T1.276 requirements and minimum length to 12.

```
password complexity ansi-t1.276-2003
password min-length 12
```

The following command configures the auto-generated password with the specified length.

```
password auto-generate length 10
```

pcc-af-service

Creates or removes an IPCF Policy and Charging Control (PCC) Application Function (AF) service or configures an existing PCC-AF service. It enters the PCC-AF Service Configuration Mode to link, configure, and manage the Application Function endpoints and associated PCC services over the Rx interface for the IPCF services.

Product IPCF

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
pcc-af-service service_name [ -noconfirm ]
no pcc-af-service service_name
```

no

Removes the specified PCC-AF service from the context.

service_name

Specifies the name of the PCC-AF service. If *service_name* does not refer to an existing service, the new service is created if resources allow. *service_name* is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to enter the PCC-AF Service Configuration Mode for an existing service or for a newly defined PCC-AF service. This command is also used to remove an existing service.

The PCC-AF-Service consolidates the provisioning and management required for the PCC-AF services being supported by the network that fall under the PCC regime. The application service handles the **Rx** interface over which the IPCF may receive media information for the application usage from AF.

Important In the absence of an Rx interface, the media information is available in the PCC-AF Service statically.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-imsapp-service)#
```

The commands available in this mode are defined in the *PCC -AF Service Configuration Mode Commands* chapter.

Caution This is a critical configuration. The PCC-AF service cannot be configured without this configuration. Any change to this configuration would lead to restarting the PCC-AF service and removing or disabling this configuration will stop the PCC-AF service.

Example

The following command enters the existing PCC-AF Service Configuration Mode (or creates it if it does not already exist) for the service named *af-service1*:

```
pcc-af-service af-service1
```

The following command will remove *af-service1* from the system:

```
no pcc-af-service af-service1
```

pcc-policy-service

Creates or removes an IPCF PCC-Policy service or configures an existing PCC-Policy service. It enters the PCC-Policy Service Configuration Mode to link, configure, and manage the Gx interface endpoints for policy authorization where IPCF acts as a policy server.

Product

IPCF

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

pcc-policy-service *service_name* **[-noconfirm]**
no pcc-policy-service *service_name*

no

Removes the specified PCC-Policy service from the context.

service_name

Specifies the name of the PCC-Policy service. If *service_name* does not refer to an existing service, the new service is created if resources allow. *service_name* is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to enter the PCC-Policy Service Configuration Mode for an existing service or for a newly defined PCC-Policy service. This command is also used to remove an existing service.

The PCC-Policy-Service is mainly used to provide a mechanism to manage the external Gx or similar interfaces required for policy authorization purpose. It manages Gx and Gx-like interfaces such as Gxc/Gxa/S9 between IPCF/PCRF and PCEF or BBERF, which is based on the dictionary used for PCC.

Multiple instances of PCC-Policy-Service may exist in a system which could link with the same PCC-Service that controls the business logic. This service allows for management of configuration for peers as well self related to Gx like functions.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-pccpolicy-service)#
```

The commands available in this mode are defined in the *PCC-Policy Service Configuration Mode Commands* chapter.

Caution This is a critical configuration. The PCC-Policy service cannot be configured without this configuration. Any change to this configuration would lead to restarting the PCC-Policy service and removing or disabling this configuration will stop the PCC-Policy service.

Example

The following command enters the existing PCC-Policy Service Configuration Mode (or creates it if it does not already exist) for the service named *gx-service1*:

```
pcc-policy-service gx-service1
```

The following command will remove *gx-service1* from the system:

```
no pcc-policy-service gx-service1
```

pcc-service

Creates or removes an IPCF Policy and Charging Control (PCC) service or configures an existing PCC service. It enters the PCC Service Configuration Mode for IPCF related configurations in the current context.

Product IPCF

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
pcc-service service_name [ -noconfirm ]
no pcc-service service_name
```

no

Removes the specified PCC service from the context.

service_name

Specifies the name of the PCC service. If *service_name* does not refer to an existing service, the new service is created if resources allow. *service_name* is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to enter the PCC Service Configuration Mode for an existing service or for a newly defined PCC service. This command is also used to remove an existing service.

The IPCF PCC Service Configuration Mode is used to link, consolidate and manage the policy logic for the networks. The authorization of resources for a subscriber's data usage under various conditions and policies are defined in the IPCF PCC service.

Only one PCC service can be configured on a system which is further limited to a maximum of 256 services (regardless of type) configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-pcc-service)#
```

The commands available in this mode are defined in the *PCC Service Configuration Mode Commands* chapter.

Caution This is a critical configuration. The PCC service cannot be configured without this configuration. Any change to this configuration would lead to restarting the Policy and Charging Control service and removing or disabling this configuration will stop the PCC service.

Example

The following command enters the existing PCC Service Configuration Mode (or creates it if it does not already exist) for the service named *ipcf-service1*:

```
pcc-service ipcf-service1
```

The following command will remove *ipcf-service1* from the system:

```
no pcc-service ipcf-service1
```

pcc-sp-endpoint

Creates or removes a PCC Sp interface endpoint or configures an existing PCC Sp interface client endpoint. It enters the PCC Sp Endpoint Configuration Mode to link, configure, and manage the operational parameters related to its peer.

Product

IPCF

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
pcc-sp-endpoint sp_intfc1 [ -noconfirm ]
no pcc-sp-endpoint name sp_intfc1
```

no

Removes the specified PCC Sp interface endpoint from the context.

sp_intfc1

Specifies the name of the PCC Sp interface endpoint. If *sp_intfc_endpoint* does not refer to an existing endpoint, the new endpoint is created if resources allow.

sp_intfc_endpoint is an alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to enter the PCC-Sp-Endpoint Configuration Mode for an existing interface or for a newly defined PCC **Sp** interface endpoint. This command is also used to remove an existing endpoint.

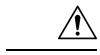
An instance of PCC Sp endpoint represents a client end for SSC/SPR interactions. It is possible to support multiple Sp endpoints each supporting the same or different protocol(s). The PCC Sp endpoint facilitates the configuration of the treatment required of the Sp interface as well as manages the connection and operational parameters related to its peer.

Only one PCC Sp endpoint across a chassis can be configured on a system.

Entering this command results in the following prompt:

```
[context_name]hostname(config-spendpoint)#
```

The commands available in this mode are defined in the *PCC-Sp-Endpoint Configuration Mode Commands* chapter.



Caution This is a critical configuration. The PCC Sp endpoint cannot be configured without this configuration. Any change to this configuration would lead to reset the PCC Sp interface and removing or disabling this configuration also disables the PCC Sp interface.

Example

The following command enters the existing PCC Sp Endpoint Configuration Mode (or creates it if it does not already exist) for the endpoint named *sp_intfc1*:

```
pcc-sp-endpoint sp_intfc1
```

The following command will remove *sp_intfc1* from the system:

```
pcc-sp-endpoint name sp_intfc1
```

pdg-service

Creates a new PDG service or specifies an existing PDG service and enters the PDG Service Configuration Mode. A maximum of 16 PDG services can be created. This limit applies per ASR 5000 chassis and per context.

Product PDG/TTG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **[no] pdg-service** *name*

no*name*

Deletes the specified PDG service.

name

Specifies the name of a new or existing PDG service as an alphanumeric string 1 through 63 characters that must be unique across all FNG services within the same context and across all contexts.



Important Service names must be unique across all contexts within a chassis.

Usage Guidelines Use this command in Context Configuration Mode to create a new PDG service or modify an existing one. Executing this command enters the PDG Service Configuration Mode.

Example

The following command configures an PDG service named *pdg_service_1* and enters the PDG Service Configuration Mode:

```
pdg-service pdg_service_1
```

pdif-service

Creates a new, or specifies an existing, Packet Data Interworking Function (PDIF) service and enters the PDIF Service Configuration Mode.

Product

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] pdif-service name [ -noconfirm ]
```

name

Specifies the name of a new or existing PDIF service as an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines

Use this command to create a new or enter an existing PDIF service.

Entering this command results in the following prompt:

[*context_name*]*hostname*(config-pdif-service)#

PDIF Service Configuration Mode commands are defined in the *PDIF Service Configuration Mode Commands* chapter.

Example

The following command configures a PDIF service called *pdif2* and enters the PDIF Service Configuration Mode:

```
pdif-service pdif2
```

pdsn-service

Creates or deletes a packet data service or specifies an existing PDSN service for which to enter the Packet Data Service Configuration Mode for the current context.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] pdsn-service` *name*

no

Indicates the packet data service specified is to be removed.

name

Specifies the name of the PDSN service to configure. If *name* does not refer to an existing service, the new service is created if resources allow. *name* is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines

Enter the PDSN Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your Cisco service representative for more information.

Example

The following command will enter the PDSN Service Configuration Mode creating the service *sampleService*, if necessary.

```
pdsn-service sampleService
```

The following command will remove *sampleService* as being a defined PDSN service.

```
no pdsn-service sampleService
```

pdsnclosedrp-service

Creates or deletes a Closed R-P packet data service or specifies an existing PDSN Closed R-P service for which to enter the Closed R-P Service Configuration Mode for the current context.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] pdsnclosedrp-service` *`name`*

no

Removes the specified PDSN Closed R-P service.

name

Specifies the name of the Closed R-P PDSN service to configure. If *name* does not refer to an existing service, the new service is created if resources allow. *name* is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines

Enter the Closed R-P Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Example

The following command enters the Closed R-P Service Configuration Mode creating the service *sampleService*, if necessary:

```
pdsnclosedrp-service sampleService
```

The following command removes *sampleService* as being a defined Closed R-P PDSN service:

no pdsnclosedrp-service sampleService

pgw-service

Creates a PDN-Gateway (P-GW) service or specifies an existing P-GW service and enters the P-GW Service Configuration Mode for the current context.

Product

P-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

pgw-service *service_name* **[-noconfirm]**
no pgw-service *service_name*

service_name

Specifies the name of the P-GW service. If *service_name* does not refer to an existing service, the new service is created if resources allow. *service_name* is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

no pgw-service *service_name*

Removes the specified P-GW service from the context.

Usage Guidelines

Enter the P-GW Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.



Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-pgw-service)#
```

P-GW Service Configuration Mode commands are defined in the *P-GW Service Configuration Mode Commands* chapter.

Use this command when configuring the following eHRPD and SAE components: P-GW.

Example

The following command enters the existing P-GW Service Configuration Mode (or creates it if it does not already exist) for the service named *pgw-service1*:

pgw-service pgw-service1

The following command will remove *pgw-service1* from the system:

no pgw-service pgw-service1

policy

Enters an existing accounting policy or creates a new one where accounting parameters are configured.

Product

HSGW

P-GW

S-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] policy accounting *name*

no

Removes the specified accounting policy from the context.

name

Specifies the name of the existing or new accounting policy as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to enter the Accounting Policy Configuration mode to edit an existing accounting policy or configure an new policy.

Entering this command results in the following prompt:

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

Accounting Policy Configuration Mode commands are defined in the *Accounting Policy Configuration Mode Commands* chapter.

Example

The following command enters the Accounting Policy Configuration Mode for a policy named *acct5*:

```
policy accounting acct5
```

policy-group

Creates or deletes a policy group. It enters the Policy-Group Configuration Mode within the current destination context for flow-based traffic policing to a subscriber session flow.

Product

PDSN

HA

ASN-GW

HSGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] policy-group name *policy_group*

no

Deletes configured policy group within the context.

name *policy_group*

Specifies the name of Policy-Group as an alphanumeric string of 1 through 15 characters that is case sensitive.

Usage Guidelines Use this command to form a policy group from a set of configured Policy-Maps. A policy group supports up to 16 policies for a subscriber session flow.

Example

The following command configures a policy group *policy_group1* for a subscriber session flow:

```
policy-group name policy_group1
```

policy-map

Creates or deletes a policy map. It enters the Traffic Policy-Map Configuration Mode within the current destination context to configure the flow-based traffic policing for a subscriber session flow.

Product

PDSN

HA

ASN-GW

HSGW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] policy-map name policy_name
```

no

Deletes configured Policy-Map within the context.

name *policy_name*

Specifies the name of Policy-Map as an alphanumeric string of 1 through 15 characters that is case sensitive.

Usage Guidelines Use this command to enter Traffic Policy-Map Configuration Mode and to set the Class-Map and corresponding traffic flow treatment to traffic policy for a subscriber session flow.

Example

Following command configures a policy map *policy1* where other flow treatments is configured.

```
policy-map name policy1
```

ppp

Configures point-to-point protocol parameters for the current context.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

ppp { acfc { receive { allow | deny } | transmit { apply | ignore | reject} } | auth-retry suppress-aaa-auth | chap fixed-challenge-length *length* **| dormant send-lcp-terminate | echo-max-retransmissions** *num_retries* **| echo-retransmit-timeout** *msec* **| first-lcp-retransmit-timeout** *milliseconds* **| lcp-authentication-discard retry-alternate** *num_discard* **| lcp-authentication-reject retry-alternate | lcp-start-delay** *delay* **| lcp-terminate connect-state | lcp-terminate mip-lifetime-expiry | lcp-terminate mip-revocation | max-authentication-attempts** *num* **| max-configuration-nak** *num* **| max-retransmissions** *number* **| max-terminate** *number* **| mru** *packet_size* **| negotiate default-value-options | peer-authentication** *user_name* **[encrypted] password** *password* **] | pfc { receive { allow | deny } | transmit { apply | ignore | reject} } | reject-peer-authentication | renegotiation retain-ip-address | retransmit-timeout** *milliseconds* **}**
no ppp { auth-retry suppress-aaa-auth | chap fixed-challenge-length | dormant send-lcp-terminate | lcp-authentication-descard retry-alternate *num_discard* **| lcp-authentication-reject retry-alternate | lcp-start-delay | lcp-terminate connect-state | reject-peer-authentication | renegotiation retain-ip-address }**
default lcp-authentication-descard retry-alternate *num_discard*

default

Restores the system defaults for the specific command/keyword.

no

Disables, deletes, or resets the specified option.

For **no ppp renegotiation retain-ip-address** the initially allocated IP address will be released and a new IP address will be allocated during PPP renegotiation.

acfc { receive { allow | deny } | transmit { apply | ignore | reject} }

Configures PPP Address and Control Field Compression (ACFC) parameters.

receive { allow | deny }

This keyword specifies whether to allow Address and Control Field Compressed PPP packets received from the Peer. During LCP negotiation, the local PPP side indicates whether it can handle ACFC compressed PPP packets. Default: **allow**

When allow is specified, the local PPP side indicates that it can process ACFC compressed PPP packets and compressed packets are allowed. When deny is specified, the local PPP side indicates that it cannot handle ACFC compressed packets and compressed packets are not allowed.

transmit { apply | ignore | reject }

Specifies how Address and Control Field Compression should be applied for PPP packets transmitted to the Peer. During LCP negotiation, the Peer indicates whether it can handle ACFC compressed PPP packets. Default: **ignore**

When apply is specified, if the peer requests ACFC, the request is accepted and ACFC is applied for transmitted PPP packets. When ignore is specified, if the peer requests ACFC, the request is accepted, but ACFC is not applied for transmitted PPP packets. When reject is specified, if the peer requests ACFC, the request is rejected and ACFC is not applied to transmitted packets.

auth-retry suppress-aaa-auth

This option does not allow PPP authentication retries to the AAA server after the AAA server has already authenticated a session. PPP locally stores the username and password, or challenge response, after a successful PPP authentication. If the Mobile Node retries the PAP request or CHAP-Response packet to the PDSN, PPP locally compares the incoming username, password or Challenge Response with the information stored from the previous successful authentication. If it matches, PAP ACK or CHAP Success is sent back to the Mobile Node, without performing AAA authentication. If the incoming information does not match with what is stored locally, then AAA authentication is attempted. The locally stored PPP authentication information is cleared once the session reaches a connected state.

Default: **no auth-retry suppress-aaa-auth**



Important This option is not supported in conjunction with the GGSN product.

chap fixed-challenge-length *length*

Normally PPP CHAP use sa random challenge length from 17 to 32 bytes. This command allows you to configure a specific fixed challenge length of from 4 through 32 bytes. *length* must be an integer from 4 through 32.

Default: Disabled. PAPCHAP uses a random challenge length.

dormant send-lcp-terminate

Indicates a link control protocol (LCP) terminate message is enabled for dormant sessions.



Important This option is not supported in conjunction with the GGSN product.

echo-max-retransmissions *num_retries*

Configures the maximum number of retransmissions of LCP ECHO_REQ before a session is terminated in an always-on session. *num_retries* must be an integer from 1 through 16. Default: 3

echo-retransmit-timeout *msec*

Configures the timeout (in milliseconds) before trying LCP ECHO_REQ for an always-on session. *msec* must be an integer from 100 through 5000. Default: 3000

first-lcp-retransmit-timeout *milliseconds*

Specifies the number of milliseconds to wait before attempting to retransmit control packets. This value configures the first retry. All subsequent retries are controlled by the value configured for the ppp **retransmit-timeout** keyword.

milliseconds must be an integer from 100 through 5000. Default: 3000

lcp-authentication-discard retry-alternate *num_discard*

Sets the number of discards up to which authentication option is discarded during LCP negotiation and retries starts to allow alternate authentication option. *num_discard* must be an integer from 0 through 5. Recommended value is 2. Default: Disabled.

lcp-authentication-reject retry-alternate

Specifies the action to be taken if the authentication option is rejected during LCP negotiation and retries the allowed alternate authentication option.

Default: Disabled. No alternate authentication option will be retried.

lcp-start-delay *delay*

Specifies the delay (in milliseconds) before link control protocol (LCP) is started. *delay* must be an integer from 0 through 5000. Default: 0

lcp-terminate connect-state

Enables sending an LCP terminate message to the Mobile Node when a PPP session is disconnected if the PPP session was already in a connected state.

Note that if the no keyword is used with this option, the PDSN must still send LCP Terminate in the event of an LCP/PCP negotiation failure or PPP authentication failure, which happens during connecting state.



Important This option is not supported in conjunction with the GGSN product.

lcp-terminate mip-lifetime-expiry

Configures the PDSN to send an LCP Terminate Request when a MIP Session is terminated due to MIP Lifetime expiry (default).

Note that if the no keyword is used with this option, the PDSN does not send a LCP Terminate Request when a MIP session is terminated due to MIP Lifetime expiry.

lcp-terminate mip-revocation

Configures the PDSN to send a LCP Terminate Request when a MIP Session is terminated due to a Revocation being received from the HA (default).

Note that if the no keyword is used with this option, the PDSN does not send a LCP Terminate Request when a MIP session is terminated due to a Revocation being received from the HA.

max-authentication-attempts *num*

Configures the maximum number of time the PPP authentication attempt is allowed. *num* must be an integer from 1 through 10. Default: 1

max-configuration-nak *num*

This command configures the maximum number of consecutive configuration REJ/NAKs that can be sent during CP negotiations, before the CP is terminated. *num* must be an integer from 1 through 20. Default: 10

max-retransmission *number*

Specifies the maximum number of times control packets will be retransmitted. *number* must be an integer from 1 through 16. Default: 5

max-terminate *number*

Sets the maximum number of PPP LCP Terminate Requests transmitted to the Mobile Node. *number* must be an integer from 0 through 16. Default: 2



Important This option is not supported in conjunction with the GGSN product.

mru *packet_size*

Specifies the maximum packet size that can be received in bytes. *packet_size* must be an integer from 128 through 1500. Default: 1500

negotiate default-value-options

Enables the inclusion of configuration options with default values in PPP configuration requests. Default: Disabled

The PPP standard states that configuration options with default values should not be included in Configuration Request (LCP, IPCP, etc.) packets. If the option is missing in the Configuration Request, the peer PPP assumes the default value for that configuration option.

When **negotiate default-value-options** is enabled, configuration options with default values are included in the PPP configuration Requests.

peer-authenticate *user_name* [[encrypted] password *password*]

Specifies the username and an optional password required for point-to-point protocol peer connection authentications. *user_name* is an alphanumeric string of 1 through 63 characters. The keyword **password** is optional and if specified *password* is an alphanumeric string of 1 through 63 characters. The password specified must be in an encrypted format if the optional keyword **encrypted** was specified.

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

pfc { receive { allow | deny } | transmit { apply | ignore | reject} }

Configures Protocol Field Compression (PFC) parameters.

receive { allow | deny } Default: **allow**

This keyword specifies whether to allow Protocol Field Compression (PFC) for PPP packets received from the peer. During LCP negotiation, the local PPP side indicates whether it can handle Protocol Field Compressed PPP packets.

When allow is specified, the peer is allowed to request PFC during LCP negotiation. When deny is specified, the Peer is not allowed to request PFC during LCP negotiation.

transmit { apply | ignore | reject } Default: **ignore**

This keyword specifies how Protocol field Compression should be applied for PPP packets transmitted to the Peer. During LCP negotiation, the Peer indicates whether it can handle PFC compressed PPP packets.

When **apply** is specified, if the peer requests PFC, it is accepted and PFC is applied for transmitted PPP packets. When **ignore** is specified, If the peer requests PFC, it is accepted but PFC is not applied for transmitted packets. When **reject** is specified, all requests for PCF from the peer are rejected.

reject-peer-authentication

If disabled, re-enables the system to reject peer requests for authentication. Default: Enabled

renegotiation retain-ip-address

If enabled, retain the currently allocated IP address for the session during PPP renegotiation (SimpleIP) between FA and Mobile node. Default: Enabled

If disabled, the initially allocated IP address will be released and a new IP address will be allocated during PPP renegotiation.

retransmit-timeout *milliseconds*

Specifies the number of milliseconds to wait before attempting to retransmit control packets. *milliseconds* must be an integer from 100 through 5000. Default: 3000

Usage Guidelines

Modify the context PPP options to ensure authentication and communication for PPP sessions have fewer dropped sessions.

Example

The following commands set various PPP options:

```
ppp dormant send-lcp-terminate
ppp max-retransmission 3
ppp peer-authenticate user1 password secretPwd
ppp peer-authenticate user1
ppp retransmit-timeout 1000
```

The following command disables the sending of LCP terminate messages for dormant sessions.

```
no ppp dormant send-lcp-terminate
```

ppp magic-number

Manages magic number checking during LCP Echo message handling. The magic number is a random number chosen to distinguish a peer and detect looped back lines.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no | default ] ppp magic-number receive ignore
```

no

Disables the specified behavior.

default

Restores the system defaults for the specific command/keyword.

receive ignore

Ignores the checking of magic number at the PDSN during LCP Echo message handling. Default: Disabled.

If a valid magic numbers were negotiated for the PPP endpoints during LCP negotiation and LCP Echo Request/Response have invalid magic numbers, enabling this command will cause the system to ignore the checking of magic number during LCP Echo message handling.

Usage Guidelines

Use this command to allow the system to ignore invalid magic number during LCP Echo Request/Response handling.

Example

The following command allows the invalid magic number during LCP Echo Request/Response negotiation:

```
ppp magic-number receive ignore
```

ppp statistics

Changes the manor in which some PPP statistics are calculated.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] ppp statistics success-sessions { lcp-max-retry | misc-reasons | remote-terminated }`

no

Disable the specified behavior.

ppp statistics success-sessions lcp-max-retry

Alters statistical calculations so that: ppp successful session = successful sessions + lcp-max-retry.

success-sessions misc-reasons

Alters statistical calculations so that: ppp successful session = successful sessions + misc-reasons.

success-sessions remote-terminated

Alters statistical calculations so that: ppp successful session = successful sessions + remote-terminated.

Usage Guidelines

Use this command to alter how certain PPP statistics are calculated.



Caution This command alters the way that some PPP statistics are calculated. Please consult your designated service representative before using this command

Example

The following command alters the statistic "ppp successful session" so that it displays the sum of successful sessions and lcp-max-retry:

`ppp statistics success-sessions lcp-max-retry`

The following command disables the alteration of the statistic ppp successful session:

`no ppp statistics success-sessions lcp-max-retry`

proxy-dns intercept-list

Enters the HA Proxy DNS Configuration Mode and defines a name of a redirect rules list for the domain name servers associated with a particular FA (Foreign Agent) or group of FAs.



Important HA Proxy DNS Intercept is a license-enabled feature.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] proxy-dns intercept-list *name*

no

Removes the intercept list from the system.

name

Defines the rules list and enters the Proxy DNS Configuration Mode. *name* must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to define a name for a list of rules pertaining to the IP addresses associated with the foreign network's DNS. Up to 128 rules of any type can be configured per rules list.

Upon entering the command, the system switches to the HA Proxy DNS Configuration Mode where the lists can be defines. Up to 64 separate rules lists can be configured in a single AAA context.

This command and the commands in the HA Proxy DNS Configuration Mode provide a solution to the Mobile IP problem that occurs when a MIP subscriber, with a legacy MN or MN that does not support IS-835D, receives a DNS server address from a foreign network that is unreachable from the home network. The following flow shows the steps that occur when this feature is enabled:

By configuring the Proxy DNS feature on the Home Agent, the foreign DNS address is intercepted and replaced with a home DNS address while the call is being handled by the home network.

Example

The following command creates a proxy DNS rules list named *list1* and places the CLI in the HA Proxy DNS Configuration Mode:

```
proxy-dns intercept-list list1
```

rac-profile

Configures Routing Area Code (RAC) profile for the current context. This command is used to enter the RAC Profile Configuration Mode.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

rac-profile *profile_name*

rac-profile *profile_name*

Specifies the name of RAC profile. *profile_name* is an alphanumeric string of 1 through 31 characters. If *profile_name* does not refer to an existing profile, the new profile is created if resources allow.

Usage Guidelines

Enter the Configuration Mode to set the RAC profile options.

Entering this command results in the following prompt:

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

Example

The following command creates a RAC profile named *rp1* in the current context (or enters the existing RAC Profile Configuration Mode if it already exists):

```
rac-profile rp1
```

radius accounting

This command configures RADIUS accounting parameters for the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
radius accounting { archive [ stop-only ] | deadtime dead_minutes |
detect-dead-server { consecutive-failures consecutive_failures | keepalive |
 response-timeout timeout_duration } | interim interval seconds |
max-outstanding max_messages | max-pdu-size octets | max-retries max_retries |
 max-transmissions max_transmissions | timeout timeout_duration |
unestablished-sessions }
default radius accounting { deadtime | detect-dead-server | interim
interval seconds | max-outstanding | max-pdu-size | max-retries |
max-transmissions | timeout }
no radius accounting { archive | detect-dead-server | interim interval |
 max-transmissions | unestablished-sessions }
```

default

Configures the default settings.

no

Removes earlier configuration for the specified keyword.

archive [stop-only]

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

stop-only specifies archiving of STOP accounting messages only.

Default: Enabled

deadtime *dead_minutes*

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

dead_minutes must be an integer from 0 through 65535.

Default: 10

detect-dead-server { consecutive-failures *consecutive_failures* | keepalive | response-timeout *timeout_duration* }

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

  consecutive_failures must be an integer from 0 through 1000.

  Default: 4

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

  Default: Disabled

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

  timeout_duration must be an integer from 1 through 65535.



Important If both **consecutive-failures** and **response-timeout** are configured, then both parameters have to be met before a server is considered unreachable, or dead.

interim interval *seconds*

Specifies the time interval (in seconds) for sending accounting INTERIM-UPDATE records. *seconds* must be an integer from 50 through 40000000.



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

Default: Disabled

max-outstanding *max_messages*

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

max-pdu-size *octets*

Specifies the maximum sized packet data unit which can be accepted/generated in bytes (octets). *octets* must be an integer from 512 through 4096. Default: 4096

max-retries *max_retries*

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

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

max-transmissions *max_transmissions*

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

timeout *seconds*

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

unestablished-sessions

Indicates RADIUS STOP events are to be generated for sessions that were initiated but never fully established.

Usage Guidelines

Manage the RADIUS accounting options according to the RADIUS server used for the context.

Example

The following commands configure accounting options.

```
radius accounting detect-dead-server consecutive-failures 5
radius accounting max-pdu-size 1024
radius accounting timeout 16
```

radius accounting algorithm

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

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
radius accounting algorithm { first-n n | first-server [ fallback ] |
round-robin }
default radius accounting algorithm
```

default

Configures the default setting.

Default: **first-server**

first-n *n*

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

n is the number of AAA accounting servers to which accounting data will be sent, and must be an integer from 2 through 128. Default: 1 (Disabled)

first-server[fallback]

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

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

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

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

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

- When **radius max-outstanding** command or **max-rate** is configured, there are chances that the generated requests might be queued and waiting to be sent when bandwidth is available. If a higher priority server recovers, the queued requests will not be switched to the newly available higher priority server.
- When a higher priority server becomes reachable, all existing requests, which are being retried to a lower priority server, will not be switched to the newly available higher priority RADIUS server.

round-robin

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

Usage Guidelines

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

Example

The following command specifies to use the round-robin algorithm to select the RADIUS accounting server:

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

radius accounting apn-to-be-included

This command configures the Access Point Name (APN) to be included for RADIUS accounting.

Product GGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

default

Configures the default setting.

gi

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

gn

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

Usage Guidelines Use this command to configure the APN name for RADIUS Accounting. This can be set to either gi or gn.

Example

The following command specifies the usage of Gn APN name in the RADIUS accounting request:

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

radius accounting billing-version

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

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

radius accounting billing-version *version*
default radius accounting billing-version

default

Configures the default setting. Default: 0

version

Specifies the billing-system version of RADIUS accounting servers as an integer from 0 through 4294967295. Default: 0

Usage Guidelines

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

Example

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

radius accounting billing-version 10

radius accounting gtp trigger-policy

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

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

default

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

standard

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

ggsn-preservation-mode

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



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

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

Example

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

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

radius accounting ha policy

This command configures the RADIUS accounting policy for HA sessions.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

session-start-stop

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

custom1-aaa-res-mgmt

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

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

Usage Guidelines Use this command to set the behavior of the AAA accounting for an HA session.

Example

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

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

radius accounting interim volume

This command configures the volume of uplink and downlink volume octet counts that triggers RADIUS interim accounting.

Product GGSN

PDSN

HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
radius accounting interim volume { downlink bytes uplink bytes | total bytes
 | uplink bytes downlink bytes }
no radius accounting interim volume
```

no

Disables volume based RADIUS accounting.

downlink *bytes* uplink *bytes*

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

total *bytes*

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

uplink *bytes*

Specifies the uplink volume limit for RADIUS interim accounting in bytes. *bytes* must be an integer from 100000 through 4000000000.

downlink *bytes*

Specifies the downlink volume limit for RADIUS interim accounting in bytes. *bytes* must be an integer from 100000 through 4000000000.

Usage Guidelines

Use this command to trigger RADIUS interim accounting based on the volume of uplink and downlink bytes.

Example

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

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

radius accounting ip remote-address

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

Product

PDSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

no

Removes earlier configuration for the specified keyword.

collection

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

list *list_id*

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

Usage Guidelines

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

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

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

Example

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

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

radius accounting keepalive

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

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
radius accounting keepalive { calling-station-id id | consecutive-response
 responses_no_of | framed-ip-address ip_address | interval interval_duration |
retries retries_no_of | timeout timeout_duration | username user_name }
no radius accounting keepalive framed-ip-address
default radius accounting keepalive { calling-station-id |
consecutive-response | interval | retries | timeout | username }
```

no

Removes configuration for the specified keyword.

default

Configures the default settings.

calling-station-id *id*

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

consecutive-response *responses_no_of*

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

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

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

framed-ip-address *ip_address*

Specifies the framed ip-address to be used for the keepalive accounting in IPv4 dotted-decimal notation.

interval *interval_duration*

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

retries *retries_no_of*

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

timeout *timeout_duration*

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

username *user_name*

Configures the username to be used for the authentication as an alphanumeric string of 1 through 127 characters. Default: Test-Username

Usage Guidelines

Configures the keepalive authentication parameters for the RADIUS accounting server.

Example

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

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

The following command sets the number of retries to *4*:

```
radius accounting keepalive retries 4
```

radius accounting rp

This command configures the current context's RADIUS accounting R-P originated call options.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
radius accounting rp { handoff-stop { immediate | wait-active-stop } |
tod minute hour | trigger-event { active-handoff | active-start-param-change
 | active-stop } | trigger-policy { airlink-usage [ counter-rollover ] |
 custom [ active-handoff | active-start-param-change | active-stop ] |
standard } | trigger-stop-start }
no radius accounting rp { tod minute hour | trigger-event { active-handoff
 | active-start-param-change | active-stop } | trigger-stop-start }
default radius accounting rp { handoff-stop | trigger-policy }
```

no

Removes earlier configuration for the specified keyword.

default

Configures this command with the default settings.

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

Specifies the behavior of generating accounting STOP when handoff occurs.

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

Default: **wait-active-stop**

tod *minute hour*

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

minute must be an integer from 0 through 59.

hour must be an integer from 0 through 23.

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

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

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

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



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

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

Default:**airlink-usage**: Disabled

custom:

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

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

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

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

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



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

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



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

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

trigger-stop-start

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

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

Example

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

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

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

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

radius accounting server

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

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

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

no

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

mediation-device

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



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

ip_address

Specifies the IP address of the accounting server.

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

[encrypted] key *value*

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

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

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

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

acct-on { enable | disable }

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

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

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

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

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

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

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

acct-off { enable | disable }

Default: **enable**

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

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

max *max_messages*

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

oldports

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

port *port_number*

Specifies the port number to use for communications as an integer from 1 through 65535. Default:1813

priority *priority*

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

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

Default: 1000

type { mediation-device | standard }

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

- **standard**:Use standard AAA transactions.
- **mediation-device**: This keyword is obsolete.

Default: **standard**

type standard

Specifies the use of standard AAA transactions to use to communicate with this RADIUS server. Default: **standard**

admin-status { enable | disable }

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

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

This command is used to configure the RADIUS accounting servers with which the system is to communicate for accounting.

Up to 128 RADIUS servers can be configured per context. The servers can be configured as Accounting, Authentication, charging servers, or any combination thereof.

Example

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

```
radius accounting server 10.2.3.4 key sharedKey port 1024 max 127
radius accounting server 10.2.3.4 encrypted key scrambledKey oldports
priority 10
no radius accounting server 10.2.5.6
```

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

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

radius algorithm

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

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

default

Configures this command with the default setting. Default: **first-server**

first-server

Sends authentication data to the first available RADIUS authentication server based upon the relative priority of each configured server.

round-robin

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

Usage Guidelines

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

Example

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

```
radius algorithm round-robin
```

radius allow

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

Product

PDSN

HA

FA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

no

Removes earlier configuration for the specified keyword.

accounting-down

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

authentication-down

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

Usage Guidelines

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



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

Example

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

`radius allow accounting-down`

radius attribute

This command configures the system's RADIUS identification parameters.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
radius attribute { nas-identifier id | nas-ip-address address primary_address
 [ backup secondary_address ] [ nexthop-forwarding-address nexthop_ip_address ]
[ vlan vlan_id ] [ mpls-label input in_label_value output out_label_value1
out_label_value1 ] }
no radius attribute { nas-identifier | nas-ip-address }
default radius attribute nas-identifier
```

no

Removes earlier configuration for the specified keyword.

default

Configures the default setting.

nas-identifier *id*

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

nas-ip-address address *primary_address*

Specifies the AAA interface IP address(es) used to identify the system. Up to two addresses can be configured. *primary_address* is the IP address of the primary interface to use in the current context in IPV4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

backup *secondary_address*

Specifies the IP address of the secondary interface to use in the current context in IPV4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

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

This command configures the traffic from the specified AAA client NAS IP address to use the specified MPLS labels.

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

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



Important This option is available only when nexthop-forwarding gateway is also configured with the **nexthop-forwarding-address** keyword.

nexthop-forwarding-address *nexthop_ip_address*

Configures the next hop IP address for this NAS IP address in IPV4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

vlan *vlan_id*

Specifies the VLANID to be associated with the next-hop IP address as an integer from 1 through 4094.

Usage Guidelines

This is necessary for NetWare Access Server usage such as the system must be identified to the NAS.

The system supports the concept of the active nas-ip-address. The active nas-ip-address is defined as the current source ip address for RADIUS messages being used by the system. This is the content of the nas-ip-address attribute in each RADIUS message.

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

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

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

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

Example

The following command configures the RADIUS attribute nas-ip-address as *10.2.3.4*:

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

radius authenticate null-username

This command enables (allows) or disables (prevents) the authentication of user names that are blank or empty. This is enabled by default.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no | default ] radius authenticate null-username
```

default

Configures the default setting.

Default: Authenticate, send Access-Request messages to the AAA server, all user names, including NULL user names.

no

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

null-username

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

Usage Guidelines

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

Example

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

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

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

```
radius authenticate null-username
```

radius authenticate apn-to-be-included

This command configures the Access Point Name (APN) to be included for RADIUS authentication.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ default ] radius authenticate apn-to-be-included { gi | gn }
```

default

Configures the default setting.

gi

Specifies the use of the Gi APN name in the RADIUS authentication request. The Gi APN represents the APN received in the Create PDP Context Request message from the SGSN.

gn

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

Usage Guidelines

Use this command to configure the APN name for RADIUS authentication. This can be set to either gi or gn.

Example

The following command specifies the usage of Gn APN name in the RADIUS authentication request.

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

radius authenticator-validation

This command enables (allows) or disables (prevents) the MD5 authentication of RADIUS users. By default this feature is enabled.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ default | no ] radius authenticator-validation`

default

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

no

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

Usage Guidelines

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

Example

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

`no radius authenticator-validation`

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

`radius radius authenticator-validation`

radius change-authorize-nas-ip

This command configures the NAS IP address and UDP port on which the current context will listen for Change of Authorization (COA) messages and Disconnect Messages (DM). If the NAS IP address is not defined with this command, any COA or DM messages from the RADIUS server are returned with a Destination Unreachable error.

Product

FA

GGSN

HA

LNS

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

radius change-authorize-nas-ip *ip_address* **[encrypted] key** *value* **[port** *port* **] [event-timestamp-window** *window* **] [no-nas-identification-check] [no-reverse-path-forward-check] [mpls-label input** *in_label_value* **| output** *out_label_value1* **[** *out_label_value2* **]**
no radius change-authorize-nas-ip

no

Deletes the NAS IP address information which disables the system from receiving and responding to COA and DM messages from the RADIUS server.

ip_address

Specifies the NAS IP address of the current context's AAA interface that was defined with the **radius attribute** command.

ip_address can be expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

[encrypted] key *value*

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

The key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 256 characters with encryption.

The key *value* must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 236 characters with encryption enabled.

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

port *port*

The UDP port on which to listen for CoA and DM messages. Default: 3799

event-timestamp-window *window*

When a COA or DM request is received with an event-time-stamp, if the current-time is greater than the received-pkt-event-time-stamp plus the event-time-stamp-window, the packet is silently discarded

When a COA or DM request is received without the event-time stamp attribute, the packet is silently discarded.

window must be an integer from 0 through 4294967295. If *window* is specified as 0 (zero), this feature is disabled; the event-time-stamp attribute in COA or DM messages is ignored and the event-time-stamp attribute is not included in NAK or ACK messages. Default: 300

no-nas-identification-check

Disables the context from checking the NAS Identifier/NAS IP Address while receiving the CoA/DM requests. By default this check is enabled.

no-reverse-path-forward-check

Disables the context from checking whether received CoA or DM packets are from one of the AAA servers configured under the default AAA group in the current context. Only the src-ip address in the received CoA or DM request is validated and the port and key are ignored. The reverse-path-forward-check is enabled by default.

If **reverse-path-forward-check** is disabled, the CoA and DM messages will be accepted from AAA servers from any groups. If the check is enabled, then the CoA and DM messages will be accepted only from servers under default AAA group.

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

This command configures COA traffic to use the specified MPLS labels.

- *in_label_value* is the MPLS label that identifies inbound COA traffic.
- *out_label_value1* and *out_label_value2* identify the MPLS labels to be added to COA response.
  - *out_label_value1* is the inner output label.
  - *out_label_value2* is the outer output label.

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

Usage Guidelines

Use this command to enable the current context to listen for COA and DM messages.

Any one of the following RADIUS attributes may be used to identify the subscriber:

- **3GPP-IMSI**: The subscriber's IMSI. It may include the 3GPP-NSAPI attribute to delete a single PDP context rather than all of the PDP contexts of the subscriber when used with the GGSN product.
- **Framed-IP-address**: The subscriber's IP address.
- **Acct-Session-Id**:Identifies a subscriber session or PDP context.



Important For the GGSN product, the value for Acct-Session-Id that is mandated by 3GPP is used instead of the special value for Acct-Session-Id that we use in the RADIUS messages we exchange with a RADIUS accounting server.



Important When this command is used in conjunction with the GGSN, CoA functionality is not supported.

Example

The following command specifies the IP address *192.51.100.10* as the NAS IP address, a key value of *123456* and uses the default port of *3799*:

radius change-authorize-nas-ip 192.51.100.10 key 123456

The following command disables the nas-identification-check for the above parameters:

radius change-authorize-nas-ip 192.51.100.10 key 123456 no-nas-identification-check

radius charging

This command configures basic RADIUS options for Active Charging Services.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax Description

radius charging { deadtime *dead_minutes* **| detect-dead-server { consecutive-failures** *consecutive_failures* **| response-timeout** *timeout_duration* **} | max-outstanding** *max_messages* **| max-retries** *max_retries* **| max-transmissions** *transmissions* **| timeout** *timeout_duration* **}**
default radius charging { deadtime | detect-dead-server | max-outstanding | max-retries | max-transmissions | timeout }
no radius charging { detect-dead-server | max-transmissions | timeout }

no

Removes configuration for the specified keyword.

default

Configures the default settings.

deadtime *dead_minutes*

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

dead_minutes must be an integer from 0 through 65535.

Default: 10

detect-dead-server { consecutive-failures *consecutive_failures* | response-timeout *timeout_duration* }

consecutive-failures *consecutive_failures*: Default: 4. Specifies the number of consecutive failures, for each AAA manager, before a server is marked as unreachable. *consecutive_failures* must be an integer from 0 through 1000.

response-timeout *timeout_duration*: Specifies the number of seconds for each AAA manager to wait for a response to any message before a server is detected as failed, or in a down state. *timeout_duration* must be an integer from 1 through 65535.

max-outstanding ***max_messages***

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

max-retries ***max_retries***

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

max-transmissions ***transmissions***

Sets the maximum number of re-transmissions for RADIUS authentication requests. This limit is used in conjunction with the **max-retries** for each server. *transmissions* must be an integer from 1 through 65535. Default: Disabled

When failing to communicate with a RADIUS sever, the subscriber is failed once all of the configured RADIUS servers have been exhausted or once the configured number of maximum transmissions is reached.

For example, if 3 servers are configured and if the configured max-retries is 3 and max-transmissions is 12, then the primary server is tried 4 times (once plus 3 retries), the secondary server is tried 4 times, and then a third server is tried 4 times. If there is a fourth server, it is not tried because the maximum number of transmissions (12) has been reached.

timeout ***timeout_duration***

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

Usage Guidelines

Manage the basic Charging Service RADIUS options according to the RADIUS server used for the context.

Example

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

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

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

```
radius charging timeout 300
```

radius charging accounting algorithm

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

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

first-n *n*

Specifies that the AGW must send accounting data to *n* (more than one) AAA servers based on their priority. Response from any one of the *n* AAA servers would suffice to proceed with the call. The full set of accounting data is sent to each of the *n* AAA servers.

n is the number of AAA servers to which accounting data will be sent, and must be an integer from 2 through 128. Default: 1 (Disabled)

first-server

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

round-robin

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

Usage Guidelines

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

Example

The following command specifies to use the round-robin algorithm to select the RADIUS server:

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

radius charging accounting server

This command configures RADIUS charging accounting servers in the current context for Active Charging Services prepaid accounting.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

radius charging accounting server *ip_address* **[encrypted] key** *key* **[max** *max_messages* **] [max-rate** *max_rate* **] [oldports] [port** *port_number* **] [priority** *priority* **] [admin-status { enable | disable }] [-noconfirm]**
no radius charging accounting server *ip_address* **[oldports | port** *port_number* **]**

no

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

ip_address

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

[encrypted] key *key*

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

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

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

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

max *max_messages*

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

max-rate *max_rate*

Specifies the rate (number of messages per second) at which the authentication messages should be sent to the RADIUS server. *max_rate* must be an integer from 0 through 1000. Default: 0 (Disabled)

oldports

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

port *port_number*

Specifies the port number to use for communications as an integer from 1 through 65535. Default: 1813

priority *priority*

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

admin-status { enable | disable }

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

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

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

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

Example

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

```
radius charging accounting server 10.2.3.4 key sharedKey port 1024 max
127
radius charging accounting server 10.2.3.4 encrypted key scrambledKey
oldports priority 10
```

radius charging algorithm

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

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

default

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

first-server

Sends accounting data to the first available server based upon the relative priority of each configured server.

round-robin

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

Usage Guidelines

Set the context's RADIUS server selection algorithm for Active Charging Services to ensure proper load distribution through the servers available.

Example

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

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

radius charging server

This command configures the RADIUS charging server(s) in the current context for Active Charging Services prepaid authentication.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
radius charging server ip_address [ encrypted ] key key [ max max_messages ] [
 max-rate max_rate ] [ oldports ] [ port port_number ] [ priority priority ] [
 admin-status { enable | disable } ] [ -noconfirm ]
no radius charging server ip_address [ oldports | port port_number ]
```

no

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

ip_address

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

[encrypted] key *key*

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

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

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

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

max *max_messages*

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

max-rate *max_rate*

Specifies the rate (number of messages per second), at which the authentication messages should be sent to the RADIUS server. *max_rate* must be an integer from 0 through 1000. Default: 0 (Disabled)

oldports

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

port *port_number*

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

priority *priority*

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

admin-status { enable | disable }

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

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

This command is used to configure the RADIUS charging server(s) with which the system is to communicate for Active Charging Services prepaid authentication requests.

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

Example

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

```
radius charging server 10.2.3.4 key sharedKey port 1024 max 127
radius charging server 10.2.3.4 encrypted key scrambledKey oldports
priority 10
```

radius deadtime

This command configures the maximum period of time (in minutes) that must elapse between when a context marks a RADIUS server as unreachable and when it can re-attempt to communicate with the server.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

radius deadtime *minutes*
default radius deadtime

default

Configures the default setting.

Default: 10 minutes

minutes

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



Important Configuring deadtime as 0 disables the feature and the server is never marked as DOWN.

Usage Guidelines

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

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

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

Important For a complete explanation of RADIUS server states, if you are using StarOS 12.3 or an earlier release, refer to the *RADIUS Server State Behavior* appendix in the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

Example

The following command configures the RADIUS deadtime to 100 minutes:

```
radius deadtime 100
```

radius detect-dead-server

This command configures how the system detects a dead RADIUS server.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
radius detect-dead-server { consecutive-failures consecutive_failures_count |
 keepalive | response-timeout timeout_duration }
{ default | no } radius detect-dead-server
```

no

Removes the configuration.

default

Configures the default setting.

- **consecutive-failures**:Enabled; 4 consecutive failures
- **keepalive**: Disabled
- **response-timeout**: Disabled

consecutive-failures *consecutive_failures_count*

Specifies the consecutive number of times that the system must find the AAA server unreachable for the server to be marked unreachable, that is the server's state is changed from "Active" to "Down".

consecutive_failures_count must be an integer from 1 through 1000. Default: Enabled; 4 consecutive failures

keepalive

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

response-timeout *timeout_duration*

Specifies the time duration, in seconds, that the system must wait for a response from the AAA server to any message before the server is marked unreachable, that is the server's state is changed from "Active" to "Down".

timeout_duration must be an integer from 1 through 65535. Default: Disabled

Usage Guidelines

Use this command to configure how the system detects a dead RADIUS server.

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

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

Example

The following command enables the detect-dead-server consecutive-failures mechanism and configures the consecutive number of failures to *10*:

```
radius detect-dead-server consecutive-failures 10
```

radius dictionary

Configures the RADIUS dictionary.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

radius dictionary *dictionary*
default radius dictionary

default

Configures the default setting.

dictionary

Specifies which dictionary to use.

dictionary must be one of the following values:

Table 2: RADIUS Dictionary Types

Dictionary	Description
3gpp	This dictionary consists of all the attributes in the standard dictionary, and all of the attributes specified in 3GPP 32.015.
3gpp2	This dictionary consists of all the attributes in the standard dictionary, and all of the attributes specified in IS-835-A.
3gpp2-835	This dictionary consists of all the attributes in the standard dictionary, and all of the attributes specified in IS-835.
custom*XX*	These are customized dictionaries. For information on custom dictionaries, contact your local service representative. *XX* is the integer of the custom dictionary. NOTE: RADIUS dictionary *custom23* should be used in conjunction with Active Charging Service (ACS).
standard	This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC2869.

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

Usage Guidelines

Use this command to configure the RADIUS dictionary.

Example

The following command configures the RADIUS dictionary standard.

```
radius dictionary standard
```

radius group

This command has been deprecated and is replaced by AAA Server Group configurations. Seethe *AAA Server Group Configuration Mode Commands* chapter.

radius ip vrf

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

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

radius ip vrf *vrf_name*
no radius ip vrf

no

Disables the configured IP Virtual Routing and Forwarding (VRF) context instance and removes the association between the VRF context instance and the AAA group instance (NAS-IP).

By default this command is disabled, which means the NAS-IP being used is assumed a non-VRF IP and specific AAA group does not have any VRF association.

vrf_name

Specifies the name of a pre-configured VRF context instance. *vrf_name* is the alphanumeric string of a pre-configured VRF context configured in Context Configuration Mode via the **ip vrf** command.

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

Usage Guidelines

Use this command to associate/disassociate a pre-configured VRF context for a feature such as BGP/MPLS VPN or GRE, and IPSec tunneling which needs VRF support for RADIUS communication.

By default the VRF is NULL, which means that AAA group (NAS-IP) is associated with global routing table and NAS-IP being used is assumed a non-VRF IP.

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

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

Example

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

```
radius ip vrf ip_vrf1
```

radius keepalive

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

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

radius keepalive [calling-station-id *id* **| consecutive-response** *responses_no_of* **| encrypted | interval** *interval_duration* **| password | retries** *retries_no_of* **| timeout** *timeout_duration* **| username** *user_name* **| valid-response access-accept [access-reject]]**
default radius keepalive { calling-station-id | consecutive-response | interval | password | retries | timeout | username | valid-response }

default

Configures the default setting for the specified parameter.

calling-station-id *id*

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

consecutive-response *responses_no_of*

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

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

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

encrypted password

Designates use of encryption for the password.

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

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

Default: Test-Password

interval *interval_duration*

Configures the time interval (in seconds) between two keepalive access requests. *interval_duration* must be an integer from 30 through 65535. Default: 30

password

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

retries *retries_no_of*

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

timeout *timeout_duration*

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

username *user_name*

Configures the username to be used for authentication as an alphanumeric string of 1 through 127 characters. Default: Test-Username

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

Configures the valid response for the authentication request.

If *access-reject* is configured, then both access-accept and access-reject are considered as success for the keepalive authentication request.

If *access-reject* is not configured, then only access-accept is considered as success for the keepalive access request.

Default: **keepalive valid-response access-accept**

Usage Guidelines

Use this command to configure the Keepalive Authentication parameters for the RADIUS server.

Example

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

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

The following command sets the number of retries to *4*:

```
radius keepalive retries 4
```

radius max-outstanding

This command configures the maximum number of outstanding messages a single AAA Manager instance will queue.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

radius max-outstanding *max_messages*
default radius max-outstanding

default

Configures the default setting.

Default: 256

max_messages

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

Usage Guidelines

Use this command to configure the maximum number of outstanding messages a single AAA Manager instance will queue.

Example

The following command configures the maximum number of outstanding messages a single AAA Manager instance will queue to *100*:

```
radius max-outstanding 100
```

radius max-retries

This command configures the maximum number of times communication with a AAA server will be attempted before it is marked as "Not Responding".

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

radius max-retries *max_retries*
default radius max-retries

default

Configures the default setting.

max_retries

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

Usage Guidelines

Use this command to configure the maximum number of times communication with a AAA server will be attempted before it is marked as "Not Responding".

Example

The following command configures the maximum number of times communication with a AAA server will be attempted before it is marked as "Not Responding" to *10*:

```
radius max-retries 10
```

radius max-transmissions

This command configures the maximum number of re-transmissions for RADIUS authentication requests.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

radius max-transmissions *max_transmissions*
{ default | no } radius max-transmissions

no

Deletes the RADIUS max-transmissions configuration.

default

Configures the default setting.

Default: Disabled

max_transmissions

Specifies the maximum number of re-transmissions for RADIUS authentication requests. This limit is used in conjunction with **radius max-retries** configuration for each server. *max_transmissions* must be an integer from 1 through 65535. Default: Disabled

When failing to communicate with a RADIUS sever, the subscriber is failed once all of the configured RADIUS servers have been exhausted, or once the configured number of maximum transmissions is reached.

For example, if three servers are configured and if the configured max-retries is 3 and max-transmissions is 12, then the primary server is tried four times (once plus three retries), the secondary server is tried four times, and then a third server is tried four times. If there is a fourth server, it is not tried because the maximum number of transmissions (12)has been reached.

Usage Guidelines Use this command to configure the maximum number of re-transmissions for RADIUS authentication requests.

Example

The following command configures the maximum number of re-transmissions for RADIUS authentication requests to *10*:

```
radius max-transmissions 10
```

radius mediation-device

See the **radius accounting server** command.

radius probe-interval

This command configures the interval between two RADIUS authentication probes.

Product All products supporting Interchassis Session Recovery (ICSR)

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
radius probe-interval seconds
default radius probe-interval
```

default

Configures the default setting of 3.

seconds

Specifies the time duration (in seconds) to wait before sending another probe authentication request to a RADIUS server. The value must be an integer from 1 through 65535. Default: 3

Usage Guidelines

Use this command for ICSR support to set the duration between two authentication probes to the RADIUS server.

Example

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

```
radius probe-interval 30
```

radius probe-max-retries

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

Product

All products supporting Inter chassis Session Recovery (ICSR)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

default

Configures the default setting.

Default: 5

retries

Specifies the number of retries for RADIUS authentication probe response before the authentication is declared as failed. *retries* must be an integer from 1 through 65535. Default: 5

Usage Guidelines

Use this command for ICSR support to set the number of attempts to send RADIUS authentication probe without a response before the authentication is declared as failed.

Example

The following command sets the maximum number of retries to *6*:

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

radius probe-message

This command configures the service ip-address to be sent as an AVP in RADIUS authentication probe messages.

Product

All products supporting Inter chassis Session Recovery (ICSR)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
radius probe-message local-service-address ipv4/ipv6_address
no radius probe-message local-service-address
```

no

Disables sending of AVPs configured under probe-message cli in RADIUS authentication probe messages.

radius probe-message local-service-address

radius probe-message

Configures AVPs to be sent in RADIUS authentication probe messages.

local-service-address

Configures the service ip-address to be sent as an AVP in RADIUS authentication probe messages.

ipv4/ipv6_address

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

Example

The following command configures the service ip-address *21.32.36.25* to be sent as an AVP in RADIUS authentication probe messages:

```
radius probe-message local-service-address 21.32.36.25
```

radius probe-timeout

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

Product

All products supporting Interchassis Session Recovery (ICSR)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

radius probe-timeout *timeout_duration*
default radius probe-timeout

default

Configures the default setting.

Default: 3

timeout_duration

Specifies the time duration (in seconds) to wait for a response from the RADIUS server before resending the authentication probe. *timeout_duration* must bean integer from 1 through 65535. Default: 3

Usage Guidelines

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

Example

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

```
radius probe-timeout 120
```

radius server

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

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

```
 { enable | disable } ] [ -noconfirm ]
no radius server ip_address [ oldports | port port_number ]
```

no

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

ip_address

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

[encrypted] key *value*

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

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

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

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

max *max_messages*

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

max-rate *max_rate*

Specifies the rate (number of messages per second), at which the authentication messages should be sent to the RADIUS server. *max_rate* must be an integer from 0 through 1000. Default: 0 (Disabled)

oldports

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

port *port_number*

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

priority *priority*

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

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

Default: 1000

probe

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

no-probe

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

probe-username *username*

Specifies the username sent to the RADIUS server to authenticate probe messages. *username* must be an alphanumeric string of 1 through 127 characters.

probe-password [encrypted] password *password*

The password sent to the RADIUS server to authenticate probe messages.

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

password *password*: Specifies the probe-user password for authentication. *password* must be an alphanumeric string of 1 through 63 characters.

type { mediation-device | standard }

Specifies the type of transactions the RADIUS server accepts.

mediation-device: Specifies mediation-device specific AAA transactions. This device is available if you purchased a transaction control services license. Contact your local sales representative for licensing information.

standard: Specifies standard AAA transactions. (Default)

admin-status { enable | disable }

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

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

This command is used to configure the RADIUS authentication server(s) with which the system is to communicate for authentication.

Up to 128 RADIUS servers can be configured per context. The servers can be configured as Accounting, Authentication, charging servers, or any combination thereof.

Example

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

```
radius server 10.2.3.4 key sharedKey port 1024 max 127
radius server 10.2.3.4 encrypted key scrambledKey oldports priority 10
```

radius strip-domain

This command configures the stripping of the domain from the user name prior to authentication or accounting.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
radius strip-domain { authentication-only | accounting-only }
no radius strip-domain
```

no

Removes the RADIUS strip-domain configuration.

authentication-only

Specifies that the domain must be stripped from the user name prior to authentication.

accounting-only

Specifies that the domain must be stripped from the user name prior to accounting.

Usage Guidelines

Use this command to configure the stripping of domain from the user name prior to authentication or accounting.

By default, strip-domain configuration will be applied to both authentication and accounting messages, if configured. When the argument **authentication-only** or **accounting-only** is present, **strip-domain** is applied only to the specified RADIUS message types.

Example

The following command configures the stripping of domain from the user name prior to authentication:

```
radius strip-domain authentication-only
```

radius timeout

This command configures the time duration to wait for a response from the RADIUS server before resending the messages.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
radius timeout timeout_duration
default radius timeout
```

default

Configures the default setting.

timeout_duration

Specifies the time duration (in seconds) to wait for a response from the RADIUS server before resending the messages. *timeout_duration* must be an integer from 1 through 65535. Default: 3

Usage Guidelines Use this command to configure the time duration to wait for a response from the RADIUS server before resending the messages.

Example

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

```
radius timeout 300
```

radius trigger

This command enables specific RADIUS triggers. The RADIUS Trigger configuration in the Context Configuration Mode is to enable backward compatibility. To configure RADIUS triggers for the default AAA group, you must configure them in the Context Configuration Mode.

Product GGSN

P-GW

SAEGW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

no

Disables the specified RADIUS trigger.

default

Configures the default setting.

Default: All RADIUS triggers are enabled.

ms-timezone-change

Specifies to enable RADIUS trigger for MS time zone change.

qos-change

Specifies to enable RADIUS trigger for Quality of Service change.

rai-change

Specifies to enable RADIUS trigger for Routing Area Information change.

rat-change

Specifies to enable RADIUS trigger for Radio Access Technology change.

serving-node-change

Specifies to enable RADIUS trigger for Serving Node change.

uli-change

Specifies to enable RADIUS trigger for User Location Information change.

Usage Guidelines

Use this command to enable RADIUS triggers.

Example

The following command enables RADIUS trigger for RAT change:

```
radius trigger rat-change
```

realtime-trace-module

This command is used to create, configure, or delete the module for Real Time Cell Traffic Tracing in a context.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] realtime-trace-module

no

Removes the real time trace module configuration for the current context.

realtime-trace-module

Creates the module for real time cell traffic tracing.

Once the realtime trace module is configured, the real time trace file transfer parameters can be configured.

Usage Guidelines

Use this command to configure the module for Real Time Cell Traffic Tracing in a context. The user must be in a non-local context when specifying the **realtime-trace-module** command.

On entering this command, the CLI prompt changes to:

[*context_name*]*host_name*(config-realtime-trace)#

remote-server-list

Creates or specifies the name of an existing remote server list for this context and enters the Remote Access List Configuration Mode.

Product

All

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

remote-server-list name *list_name*
no remote-server-list name *list_name*

no

Removes the specified remote server list from the context.

list_name

Specifies the name of the remote server list. If *list_name* does not refer to an existing list, the new list is created if resources allow. *list_name* is an alphanumeric string of 1 through 31 characters.

Usage Guidelines

Enter the Remote Server List Configuration Mode for an existing list or for a newly defined list. This command is also used to remove an existing remote access list.

A maximum of 256 services (regardless of type) can be configured per system.

Entering this command results in the following prompt:

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

Remote Server List Configuration Mode commands are defined in the *remote Server List Configuration Mode Commands* chapter.

Example

The following command enters the Remote Server List Configuration Mode for the list named *remote_list_1*:

```
remote-server-list remote_list_1
```

The following command will remove *remote_list_1* from the system:

```
no remote-server-list remote_list_1
```

route-access-list extended

Configures an access list for filtering routes based on a specified range of IP addresses.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] route-access-list extended *identifier* **{ deny | permit } ip {** *network_parameter* **} {** *mask_parameter*

no

Deletes the specified route access list.

identifier

Specifies a value to identify the route access list as an integer from 100 through 999.

deny

Deny routes that match the specified criteria.

permit

Permit routes that match the specified criteria.

ip *network_parameter ip_address wildcard_mask*

Specifies the network portion of the route to match. The network portion of the route is mandatory and must be expressed in one of the following ways:

- *ip_address wildcard_mask*: Matches a network address and wildcard mask expressed in IPv4 dotted-decimal notation.
- **any**: Matches any network address.
- **host** *network_address*: Match the specified network address exactly. *network_address* must be an IPv4 address specified in dotted-decimal notation.

mask_parameter

This specifies the mask portion of the route to match. The mask portion of the route is mandatory and must be expressed in one of the following ways:

- *mask_address wildcard_mask*: A mask address and wildcard mask expressed in IPv4 dotted-decimal notation.
- **any**: Match any network mask.
- **host** *mask_address*: Match the specified mask address exactly. *mask_address* must be an IPv4 address specified in dotted-decimal notation.

Usage Guidelines

Use this command to create an extended route-access-list that matches routes based on network addresses and masks.

Example

Use the following command to create an extended route-access-list:

```
route-access-list extended 100 permit ip 198.51.100.0 0.0.0.255
```

route-access-list named

Configures an access list for filtering routes based on a network address and net mask.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] route-access-list named *list_name* **{ deny | permit } {** *ip_address/mask* **| any } [exact-match]**

no

Deletes the specified route access list.

list_name

Specifies name that identifies the route access list as an alphanumeric string of 1 through 79 characters.

deny

Denies routes that match the specified criteria.

permit

Permits routes that match the specified criteria.

ip_address/mask

Specifies the IP address (in IPv4 dotted-decimal notation) and the number of subnet bits, representing the subnet mask in CIDR notation (for example 209.165.200.225/24).

any

Matches any route.

exact-match

Matches the IP address prefix exactly.

Usage Guidelines

Use this command to create route-access lists that specify routes that are accepted.

Up to 16 routes can be added to each route-access-list.

Example

Use the following command to create a route access list named *list27* that permits routes that match *192.168.1.0/24* exactly:

```
route-access-list named list 27 permit 198.51.100.1/24 exact-match
```

To delete the list, use the following command:

no route-access-list named list 27 permit 198.51.100.1/24 exact-match

route-access-list standard

Configures an access-list for filtering routes based on network addresses.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] route-access-list standard *identifier* **{ permit | deny } {** *ip_address wildcard_mask* **| any | host** *network_address* **}**

no

Deletes the specified route access list.

identifier

Specifies a value that identifies the route-access-list as an integer from 1 through 99.

deny

Denies routes that match the specified criteria.

permit

Permits routes that match the specified criteria.

ip_address wildcard_mask

Specifies the IP address and subnet mask to match for routes. Both *ip_address* and *wildcard_mask* must be entered in IPv4 dotted-decimal notation. (For example, 192.168.100.0 255.255.255.0)

any

Matches any route.

host *network_address*

Matches only route shaving the specified network address as if it had a 32-bit network mask. *network_address* must be an IPv4 address specified in dotted-decimal notation.

Usage Guidelines

Use this command to create route-access-lists that specify routes that are accepted.

Example

Use the following command to create a route access list with an identifier of *10* that permits routes:

```
route-access-list standard 10 permit 192.51.100.1 255.255.255.0
```

To delete the list, use the following command:

```
no route-access-list standard 10 permit 192.51.100.1 255.255.255.0
```

route-map

Creates a route-map that is used by the routing features and enters Route-map Configuration mode. A route-map allows redistribution of routes and includes a list of match and set commands associated with it. The match commands specify the conditions under which redistribution is allowed; the set commands specify the particular redistribution actions to be performed if the criteria specified by match commands are met. Route-maps are used for detailed control over route distribution between routing processes. Up to eight route-maps can be created in each context. Refer to the *Route-map Configuration Mode Commands* chapter for more information.

Product

PDSN

HA

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
route-map map_name { deny | permit } seq_number
no route-map map_name
```

no

Deletes the specified route map.

map_name

Specifies the name of the route map to create or edit as an alphanumeric string of 1 through 69 characters.

deny

If the deny parameter is specified and the match command criteria are met, the route is not redistributed and any other route maps with the same map name are not examined. Set commands have no affect on deny route-maps.

permit

If the permit parameter is specified, and the match criteria are met, the route is redistributed as specified by set actions. If the match criteria are not met, the next route map with the same name is tested.

seq_number

Specifies the sequence number that indicates the position a new route map is to have in the list of route maps already configured with the same name. Route maps with the same name are tested in ascending order of their sequence numbers. This must be an integer from 1 through 65535.

Usage Guidelines

Use this command to create route maps that allow redistribution of routes based on specified criteria and set parameters for the routes that get redistributed. The chassis supports a maximum of 64 route maps per context.

Example

To create a route map named map1 that permits routes that match the specified criteria, use the following command:

```
route-map map1 permit 10
```

To delete the route-map, enter the following command:

```
no route-map map1 permit 10
```

router

Enables BGP, Open Shortest Path First (OSPF) or OSPF version 3 (OSPFv3) routing functionality and enters the corresponding Configuration Mode. Refer to the *BGP Configuration Mode Commands*, *OSPF Configuration Mode Commands* or *OSPFv3 Configuration Mode Commands* chapter for details on associated Configuration mode commands.

Product

PDSN

HA

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] router { bgp *as_number* **| ospf | ospfv3 | rip }**

no

Disables the specified routing support in the current context.

bgp *as_number*

Enables a BGP routing service for this context and assigns it the specified Autonomous System (AS) number before entering the BGP Configuration mode. *as_number* must be an integer from 1 through 4294967295.

Important BGP routing is supported only for use with the HA.

ospf

Enables OSPF routing in this context and enters OSPF Configuration mode.

ospfv3

Enables OSPFv3 routing in this context and enter OSPFv3 Configuration mode.

rip

Enters RIP (Routing Information Protocol) Configuration mode.

Usage Guidelines

Use this command to enable and configure OSPF and BGP routing in the current context.

Important You must obtain and install a valid license key to use these features. Refer to the *System Administration Guide* for details on obtaining and installing feature use license keys.

Example

The following command enables the OSPF routing functionality and enters the OSPF Configuration Mode:

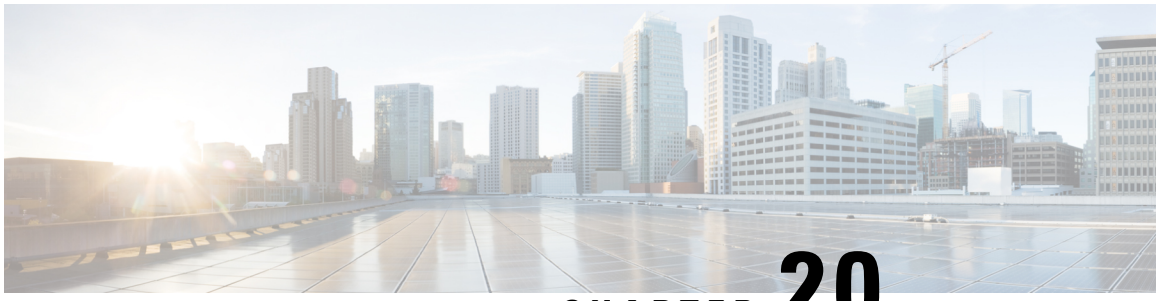
router ospf

The following command enables the OSPFv3 routing functionality and enters the OSPFv3 Configuration Mode:

router ospfv3

The following command enables a BGP routing service with an AS number of *100*, and enters the BGP Configuration Mode:

router bgp 100



CHAPTER 20

Context Configuration Mode Commands S-Z

Command Modes

This section includes the commands **s102-service** through **wsg-service** service.

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

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

- s102-service, on page 702
- saegw-service, on page 703
- sbc-service, on page 704
- server, on page 705
- service-redundancy-protocol, on page 707
- session-event-module, on page 707
- sgsn-service, on page 708
- sgs-service, on page 709
- sgtp-service, on page 710
- sgw-service, on page 711
- sls-service, on page 712
- smsc-service, on page 713
- ssh, on page 715
- ssl, on page 716
- subscriber, on page 717
- sx-service, on page 718
- tac-profile, on page 719
- threshold available-ip-pool-group, on page 719
- threshold ha-service init-rrq-rcvd-rate, on page 721
- threshold ip-pool-free, on page 722
- threshold ip-pool-hold, on page 723
- threshold ip-pool-release, on page 724

- threshold ip-pool-used, on page 726
- threshold ip-pool-usable, on page 727
- threshold ip-pool-usable-final, on page 728
- threshold monitoring, on page 729
- threshold pdsn-service init-rrq-rcvd-rate, on page 730
- twan-profile, on page 731
- udr-module active-charging-service, on page 732
- udr-module charging-service, on page 733
- uidh-server, on page 733
- user-plane-service, on page 734
- uut-profile name, on page 734
- wsg-service, on page 735

s102-service

Creates and configures an S102 service instance to manage an S102 interface. The S102 interface is used in support of the CSFB for CDMA 1xRTT feature and the SRVCC for CDMA 1xRTT feature.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] s102-service` *`service_name`*

no

Remove the configuration for the specified S102 service from the configuration of the current context.

service_name

Specifies the name of the S102 service as a unique alphanumeric string from 1 through 63 characters in length.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines

Use this command to create, edit, or remove an S102 service. The S102 service configuration is used to configure and manage the S102 interface.

An unlimited number of S102 service configurations can be created. However, for the S102 interface associated with the S102 service configuration to function, the S102 service/interface must be associated with an MME service, using the **associate** command in the MME service configuration mode. This requirement effectively limits the MME to supporting a maximum of 8 'associated' S102 service configurations at one time.

For details on the configuration and use of an S102 service/interface, refer to either the CSFB for 1xRTT or SRVCC for 1xRTT feature chapter in the *MME Administration Guide.*

Example

The following command creates an S102 service named *S102intf-1* in the current context:

```
s102-service s102intf-1
```

saegw-service

Creates a System Architecture Evolution Gateway (SAEGW) service or specifies an existing SAEGW service and enters the SAEGW Service Configuration Mode for the current context.

Product

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

saegw-service *service_name* **[-noconfirm]**
no saegw-service *service_name*

no

Removes the specified SAEGW service from the context.

service_name

Specifies the name of the SAEGW service. If *service_name* does not refer to an existing service, the new service is created if resources allow. *service_name* is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Enter the SAEGW Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

Important An S-GW and/or P-GW created in the same context must be associated with this SAEGW service.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-saegw-service)#
```

SAEGW Service Configuration Mode commands are defined in the *SAEGW Service Configuration Mode Commands* chapter.

Use this command when configuring the following SAE components: SAEGW.

Example

The following command enters the existing SAEGW Service Configuration Mode (or creates it if it does not already exist) for the service named *saegw-service1*:

```
saegw-service saegw-service1
```

The following command will remove *pgw-service1* from the system:

```
no saegw-service saegw-service1
```

sbc-service

Creates or removes an SBc service and enters the SBc Service Configuration mode. This mode configures or edits the configuration for an SBc service which controls the interface between the MME and E-SMLC.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **[no] sbc-service** *sbc_svc_name*

no

Remove the configuration for the specified SBc service from the configuration of the current context.

sbc_svc_name

Specifies the name of the SBc service as a unique alphanumeric string from 1 to 63 characters.

The SBc service name must be unique across all contexts.



Important Service names must be unique across all contexts within a chassis.

Usage Guidelines

Use this command to create, edit, or remove an SBc service.

Up to 8 SGs + MME + SBc + SLs Services can be configured on the system.

Example

The following command creates an SBc service named *sbc1* in the current context:

```
sbc-service sbc1
```

server

Configures remote server access protocols for the current context. This command is used to enter the specified protocols configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
server { confd | ftpd | named | sshd | telnetd | tftpd }
no server { confd | ftpd | named | sshd | telnetd | tftpd } [ kill ]
```

no

Disables the specified service.

confd

Enables ConfD-NETCONF protocol that supports a YANG model for transferring configuration and operations data with the Cisco Network Service Orchestrator (NSO). This command is restricted to the local context only. Enabling this command moves you to the NETCONF Protocol Configuration mode.



Important ConfD-NETCONF support requires that a V2-RSA SSH key be configured on the local context. If an SSH key is not available, StarOS generates an error message.

ftpd

Enters the FTP Server Configuration Mode.

Important The FTPD server can only be configured in the local context. FTP is not available in Trusted builds.

Caution For maximum system security, you should not enable FTP functionality. SFTP is the recommended file transfer protocol.

named

Starts the named server.

sshd

Enters the SSH Server Configuration Mode. SSH is the recommended remote access protocol. SSH must be configured to support SFTP.

Important The SSHD server allows only three unsuccessful login attempts before closing a login session attempt.

telnetd

Enters the Telnet Server Configuration Mode. Telnet is not available in Trusted builds.

Important The TELNET server allows only three unsuccessful login attempts before closing a login session attempt.

Caution For maximum system security, you should not enable telnet functionality. SSH is the recommended remote access protocol.

tftpd

Enters the TFTP Server Configuration Mode.

Important The TFTPD server can only be configured in the local context.

kill

Indicates all instances of the server are to be stopped.

This option only works with the **ftpd**, **sshd**, **telnetd**, and **tftpd** commands.

Usage Guidelines Enter the Context Configuration Mode for the appropriate, previously defined context, to set the server option(s). Repeat the command as needed to enable/disable more than one option server daemon.

Example

The following command sequence enables SSH login:

```
server sshd
```

service-redundancy-protocol

Configures Interchassis Session Recovery (ICSR) services for the current context. This command is used to enter the Service Redundancy Protocol Configuration Mode.

Product All products supporting ICSR

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **service-redundancy-protocol**

Usage Guidelines Enter the Configuration Mode to set the service redundancy protocol options.

Example

The following command enters Service Redundancy Protocol Configuration Mode.

```
service-redundancy-protocol
```

session-event-module

Enables the event module, enters the Session Event Module Configuration Mode where the sending of P-GW or S-GW subscriber-specific event files to an external server can be configured. From release 15.0 onwards, the session-event module is used by SGSN for event logging. By default, EDR files are generated at the location: /hd-raid/records/edr. After upgrading to release R15.0, if this CLI is configured, the path for EDR files changes to: /hd-raid/records/event.

Product P-GW

SAEGW (Pure-S calls)

S-GW

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] session-event-module

no

Disables the event module configuration.

Usage Guidelines

Enter the Session Event Module Configuration Mode where the sending of P-GW or S-GW subscriber-specific event files to an external server can be configured.

Entering this command results in the following prompt:

```
[context_name]hostname(config-event)#
```

Session Event Module Configuration Mode commands are defined in the *Session Event Module Configuration Mode Commands* chapter.

sgsn-service

Creates an SGSN service instance and enters the SGSN Service Configuration mode. This mode configures or edits the configuration for an SGSN service which controls the SGSN functionality.

An SGSN mediates access to GPRS/UMTS network resources on behalf of user equipment (UE) and implements the packet scheduling policy between different QoS classes. It is responsible for establishing the packet data protocol (PDP) context with the GGSN.

Important For details about the commands and parameters, check the *SGSN Service Configuration Mode* chapter.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] sgsn-service *srvc_name*

no

Remove the configuration for the specified SGSN service from the configuration of the current context.

srvc_name

Specifies the name of the SGSN service as a unique alphanumeric string of 1 through 63 characters.



Important Service names must be unique across all contexts within a chassis.

Usage Guidelines Use this command to create, edit, or remove an SGSN service.

Example

The following command creates an SGSN service named *sgsn1* in the current context:

```
sgsn-service sgsn1
```

The following command removes the sgsn service named *sgsn1* from the configuration for the current context:

```
no sgsn-service sgsn1
```

sgs-service

Creates an SGs service instance and enters the SGS Service Configuration mode.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **[no] sgs-service** *name*

no

Remove the configuration for the specified SGs service from the configuration of the current context.

name

Specifies a name for an SGs service as a unique alphanumeric string of 1 through 63 characters.



Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Enter the SGS Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.



Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following CLI prompt:

```
[context_name]hostname(config-sgs-service)#
```

SGS Service Configuration Mode commands are defined in the *MME SGS Service Configuration Mode Commands* chapter.

Example

The following command creates an SGS service named *sgs1* in the current context:

```
sgs-service sgs1
```

The following command removes the SGS service named *sgs1* from the configuration for the current context:

```
no sgs-service sgs1
```

sgtp-service

Creates an SGTP service instance and enters the SGTP Service Configuration mode. This mode configures the GPRS Tunneling Protocol (GTP) related settings required by the SGSN and eWAG to support GTP-C (control plane) messaging and GTP-U (user data plane) messaging.

Product

eWAG

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] sgtp-service *sgtp_service_name*

no

If previously configured, removes the specified SGTP service configuration in the current context.

sgtp_service_name

Specifies name of the SGTP service.

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



Important Service names must be unique across all contexts within a chassis.

Usage Guidelines

Use this command to create, edit, or remove an SGTP service.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-sgtp-service)#

Example

The following command creates an SGTP service named *sgtp1* in the current context:

```
sgtp-service sgtp1
```

The following command removes, if previously configured, the SGTP service named *sgtp1* from the current context:

```
no sgtp-service sgtp1
```

sgw-service

Creates an S-GW service or specifies an existing S-GW service and enters the S-GW Service Configuration Mode for the current context.

Product

S-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
sgw-service service_name [ -noconfirm ]
no sgw-service service_name
```

service_name

Specifies the name of the S-GW service. If *service_name* does not refer to an existing service, the new service is created if resources allow. *service_name* is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

no sgw-service *service_name*

Removes the specified S-GW service from the context.

Usage Guidelines

Enter the S-GW Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-sgw-service)#
```

S-GW Service Configuration Mode commands are defined in the *S-GW Service Configuration Mode Commands* chapter.

Use this command when configuring the following SAE components: S-GW.

Example

The following command enters the existing S-GW Service Configuration Mode (or creates it if it does not already exist) for the service named *sgw-service1*:

```
sgw-service sgw-service1
```

The following command will remove *spgw-service1* from the system:

```
no sgw-service sgw-service1
```

sls-service

Creates an SLs service or configures an existing SLs service and enters the SLs Service Configuration Mode in the current context.

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

sls-service *service_name* **[-noconfirm]**
[no] sls-service *service_name*

no

Removes the specified SLs service from the context.

service_name

Specifies the name of the SLs service. If *service_name* does not refer to an existing service, the new service is created if resources allow.

service_name is an alphanumeric string of 1 through 64 characters.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines

Enter the SLs Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

Up to 4 SLs services can be configured on the system.

The SLs service name must be unique across all contexts.

Entering this command results in the following prompt:

```
[context_name]hostname(config-sls-service)#
```

SLs Service Configuration Mode commands are defined in the SLs Service Configuration Mode Commands chapter.

Example

The following command enters the existing SLs Service Configuration Mode (or creates it if it does not already exist) for the service named *sls1*.

```
sls-service sls1
```

smsc-service

Creates and configures an SMSC peer service to allow communication with SMSC peer.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] smsc-service *smsc_svc_name* **[-noconfirm]**

no

Removes the specified SMSC service from the current context.

smsc_svc_name

Specifies the name of the SMSC service. *smsc_svc_name* is an alphanumeric string of 1 through 63 characters. If *smsc_svc_name* does not refer to an existing service, the new service is created if resources allow.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to create and configure an SMSC peer service to allow communication with SMSC peer.

Entering this command results in the following prompt:

```
[context_name]hostname(config-smsc-service)#
```

SMSC Service Configuration Mode commands are defined in the *MME SMSC Service Configuration Mode Commands* chapter.

Example

The following command creates an SMSC service named *sm1* in the current context (or enters the existing SMSC Service Configuration Mode if it already exists):

```
smsc-service sm1
```

The following command will remove the configured SMSC service named *sm1* from the current context:

```
no smsc-service sm1
```

ssh

Generates public/private key pairs for use with the configured Secure Shell (SSH) server and sets the public/private key pair to specified values.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
ssh { generate key | key data length octets } [ type { v1-rsa | v2-rsa |
v2-dsa } ]
no ssh key [ type { v1-rsa | v2-rsa | v2-dsa } ]
```

no ssh key [type { v1-rsa | v2-rsa | v2-dsa }]

This command clears configured SSH keys. If type is not specified, all SSH keys are cleared.

generate key

Generates a public/private key pair which is to be used by the SSH server. The generated key pair is in use until the command is issued again.

Important In Release 19.2 and higher, the **v2-dsa** keyword is removed in tthe **ssh generate key type** syntax.

key *data* length *octets*

Sets the public/private key pair to be used by the system where *data* is the encrypted key and *length* is the length of the encrypted key in octets. *data* must be an alphanumeric string of 1 through 1023 characters and *octets* must be a value in the range of 0 through 65535.

Important In Release 19.2 and higher, the **v2-dsa** keyword is cconcealed in the **ssh key** *name* **length** *key_length* **type v2-rsa** syntax.

[type { v1-rsa | v2-rsa | v2-dsa }]

Specifies the type of SSH key to generate. If type is not specified, all three key types are generated.

- **v1-rsa**: SSHv1 RSA host key only (obsolete)
- **v2-dsa**: SSHv2 DSA host key only (deprecated)

- **v2-rsa**: SSHv2 RSA host key only

Important For maximum security, it is recommended that only SSH v2 be used. **v2-rsa** is the recommended key type.

Usage Guidelines Generate secure shell keys for use in public key authentication.

Example

The following command generates SSH key pairs for all supported types:

```
ssh generate key
```

The following command generates an SSH key pair of a specified length using an encrypted key:

```
ssh key g6j93fw59cx length 128
```

ssl

Creates a new Secure Sockets Layer (SSL) template or specifies an existing one and enters the SSL Template Configuration Mode.

Product SCM

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **[no] ssl template** *name* **{ ssl-subscriber }**

no

Removes the specified SSL template from the context.

template *name*

Specifies the name of a new or existing SSL template as an alphanumeric string of 1 through 127 alphanumeric characters.

ssl-subscriber

Specifies that the SSL template is an SSL subscriber template.

Usage Guidelines Use this command to create a new SSL template or modify an existing one.

Entering this command results in the following prompt:

```
[context_name]hostname(cfg-ctx-ssl-subscriber-template)#
```

SSL Template Configuration Mode commands are defined in the *SSL Template Configuration Mode Commands* chapter.

Example

The following command specifies the SSL template *ssl_template_1* and enters the SSL Template Configuration Mode:

```
ssl template ssl_template_1 ssl-subscriber
```

subscriber

Configures the specified subscriber for the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
subscriber { default | name user_name } asn-service-info mobility [ ipv4 |
 ipv6 | ipv6-ipv4 ]
no subscriber { default | name user_name }
```

no

Indicates the subscriber specified is to be removed from the list of allowed users for the current context.

default | name *user_name*

default: Enters the Subscriber Configuration Mode for the context's default subscriber settings.

name *user_name*: Specifies the user which is to be allowed to use the services of the current context. *user_name* must be an alphanumeric string of 1 through 127 characters.

asn-service-info mobility:Indicates the type of mobility supported and enabled in the Autonomous System Number (ASN).

Usage Guidelines

Enter the Subscriber Configuration Mode for actual users as well as for a default subscriber for the current context.

Entering this command results in the following prompt:

```
[context_name]hostname(config-subscriber)#
```

Subscriber Configuration Mode commands are defined in the *Subscriber Configuration Mode Commands* chapter.

NAS uses the specified parameter for asn-service-info mobility to indicate and pack the mobility support field for IPv4, IPv6, or both, in the Service-Info attribute in the Access-request. RADIUS sends back this attribute in the Access-accept message by indicating respective bits to authorize the service indicated by NAS.



Important A maximum of 128 subscribers and/or administrative users may be locally configured per context.

Example

Following command configures the default subscriber in a context:

```
subscriber default
```

Following command removes the default subscriber from a context:

```
no subscriber default
```

Following command configures a subscriber named *user1* in a context:

```
subscriber name user1
```

Following command removes a subscriber named *user1* from a context:

```
no subscriber name user1
```

sx-service

Configures Sx service for the current context. This command is used to enter the Sx Service Configuration Mode.

Product CUPS

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
sx-service
```

Usage Guidelines Enter the Configuration Mode to set the Sx service options.

Example

The following command enters Sx Service Configuration Mode.

```
sx-service
```

tac-profile

Configures Tracking Area Code (TAC) profile for the current context. This command is used to enter the TAC Profile Configuration Mode.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

tac-profile *profile_name*

tac-profile *profile_name*

Specifies the name of TAC profile. *profile_name* is an alphanumeric string of 1 through 31 characters. If *profile_name* does not refer to an existing profile, the new profile is created if resources allow.

Usage Guidelines

Enter the Configuration Mode to set the TAC profile options.

Entering this command results in the following prompt:

```
[context_name]hostname(config-tac-profile)#
```

Example

The following command creates a TAC profile named *tp1* in the current context (or enters the existing TAC Profile Configuration Mode if it already exists):

```
tac-profile tp1
```

threshold available-ip-pool-group

Configures context-level thresholds for IP pool utilization for the system.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

threshold available-ip-pool-group *low_thresh* **[clear** *high_thresh* **]**
default threshold available-ip-pool-group

default

Configures the default setting.

low_thresh

The low threshold IP pool utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. *low_thresh* can be configured as an integer from 0 through 100. Default: 10

clear *high_thresh*

Specifies the high threshold IP pool utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm will be generated. *high_thresh* can be configured as an integer from 0 through 100. Default: 10

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage Guidelines

When IP address pools are configured on the system, they can be assigned to a group. IP address pool utilization thresholds generate alerts or alarms based on the utilization percentage of all IP address contained in the pool group during the specified polling interval.

All configured public IP address pools that were not assigned to a group are treated as belonging to the same group. Individual configured static or private pools are each treated as their own group.

Alerts or alarms are triggered for IP address pool utilization based on the following rules:

- **Enter Condition**: Actual IP address utilization percentage per pool group ≤ Low Threshold
- **Clear Condition**: Actual IP address utilization percentage per pool group > High Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

The following table describes the possible methods for configuring IP pool utilization thresholds:

Table 3: IP Pool Utilization Thresholds - Configuration Methods

Method	Description
Context-level	A single IP pool utilization threshold can be configured for all IP pool groups with given system context. If a single threshold is configured for all pool groups, separa alerts or alarms can be generated for each group. This command configures that threshold.

Method	Description
IP address pool-level	Each individual IP address pool can be configured with its own threshold. Thre configured for individual pools take precedence over the context-level threshol would otherwise be applied (if configured). In the event that two IP address pools belonging to the same pool group are co with different thresholds, the system uses the pool configuration that has the gr low threshold for that group.

Example

The following command configures a context-level IP pool utilization low threshold percentage of *10* and a high threshold of *35* for an system using the Alarm thresholding model:

```
threshold available-ip-pool-group 10 clear 35
```

threshold ha-service init-rrq-rcvd-rate

Sets an alarm or alert based on the average number of calls setup per second for an HA service.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
threshold ha-service init-rrq-rcvd-rate high_thresh [ clear low_thresh ]
no threshold ha-service init-rrq-rcvd-rate
```

no

Deletes the alert or alarm.

high_thresh

Sets the high threshold average number of calls setup per second that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer from 0 through 1000000. Default: 0

clear *low_thresh*

Sets the low threshold average number of calls setup per second that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured as an integer from 0 through 1000000. Default: 0

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines Use this command to set an alert or an alarm when the average number of calls set upper second is equal to or less than a specified number of calls per second.

Alerts or alarms are triggered for the number of calls setup per second based on the following rules:

- **Enter Condition**: Actual number of calls setup per second > High Threshold
- **Clear Condition**: Actual number of calls setup per second ≤ Low Threshold

Example

The following command configures a number of calls setup per second threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold ha-service init-rrq-rcvd-rate 1000 clear 500
```

threshold ip-pool-free

Sets an alarm or alert based on the percentage of IP addresses that are unassigned in an IP pool. This command affects all IP pools in the current context.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
threshold ip-pool-free low_thresh [ clear high_thresh ]
default threshold ip-pool-free
```

default

Configures the default setting.

low_thresh

Sets the low threshold percentage of addresses available in an IP pool that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer between 0 and 100. Default:0

clear *high_thresh*

Sets the high threshold percentage of addresses available in an IP pool that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm will be generated. It may be configured as an integer between 0 and 100. Default: 0

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage Guidelines Use this command to set an alert or an alarm when the number of unassigned IP addresses in any pool is equal to or less than a specified percentage of the total number of addresses in the pool.

Alerts or alarms are triggered for percentage of IP address pool free based on the following rules:

- **Enter Condition**: Actual percentage of IP addresses free per pool ≤ Low Threshold
- **Clear Condition**: Actual percentage of IP addresses free per pool > High Threshold

Important This command is overridden by the settings of the **alert-threshold** keyword of the **ip pool** command.

Example

The following command configures a context-level IP pool percentage of IP addresses that are unused low threshold percentage of *10* and a high threshold of *35* for an system using the Alarm thresholding model:

```
threshold ip-pool-free 10 clear 35
```

threshold ip-pool-hold

Sets an alert based on the percentage of IP addresses from an IP pool that are on hold. This command affects all IP pools in the current context.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
threshold ip-pool-hold high_thresh [ clear low_thresh ]
default threshold ip-pool-hold
```

default

Configures the default setting.

high_thresh

Sets the high threshold percentage of addresses on hold in an IP pool that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer from 0 through 100. Default: 0

clear *low_thresh*

Sets the low threshold percentage of addresses on hold in an IP pool that maintains a previously generated alarm condition. If the utilization percentage rises below the low threshold within the polling interval, a clear alarm will be generated. It may be configured as an integer from 0 through 100. Default: 0



Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Use this command to set an alert or an alarm when the percentage of IP addresses on hold in any pool is equal to or greater than a specified percentage of the total number of addresses in the pool.

Alerts or alarms are triggered for percentage of IP address pool addresses on hold based on the following rules:

- **Enter Condition**: Actual percentage of IP addresses on hold per pool > High Threshold
- **Clear Condition**: Actual percentage of IP addresses on hold per pool ≤ Low Threshold



Important This command is overridden by the settings of the **alert-threshold** keyword of the **ip pool** command.

Example

The following command configures a context-level IP pool percentage of IP addresses that are on high threshold percentage of *35* and a low threshold of *10* for an system using the Alarm thresholding model:

```
threshold ip-pool-hold 35 clear 10
```

threshold ip-pool-release

Sets an alert based on the percentage of IP addresses from an IP pool that are in the release state. This command affects all IP pools in the current context.

Product All

Privilege Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

threshold ip-pool-release *high_thresh* **[clear** *low_thresh* **]**
default threshold ip-pool-release

default

Configures the default setting.

high_thresh

Sets the high threshold percentage of addresses in the release state in an IP pool that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer from 0 through 100. Default: 0

clear *low_thresh*

Sets the low threshold percentage of addresses in the release state in an IP pool that maintains a previously generated alarm condition. If the utilization percentage rises below the low threshold within the polling interval, a clear alarm will be generated. It may be configured as an integer from 0 through 100. Default:0

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage Guidelines

Use this command to set an alert or an alarm when the number of IP addresses the release state in any pool is equal to or greater than a specified percentage of the total number of addresses in the pool.

Alerts or alarms are triggered for percentage of IP address pool addresses in the release state based on the following rules:

- **Enter Condition**: Actual percentage of IP addresses in the release state per pool> High Threshold
- **Clear Condition**: Actual percentage of IP addresses in the release state per pool ≤ Low Threshold

Important This command is overridden by the settings of the **alert-threshold** keyword of the **ip pool** command.

Example

The following command configures a context-level IP pool percentage of IP addresses that are in the release state high threshold percentage of *35* and a low threshold of *10* for an system using the Alarm thresholding model:

```
threshold ip-pool-release 35 clear 10
```

threshold ip-pool-used

Sets an alert based on the percentage of IP addresses that have been assigned from an IP pool. This command affects all IP pools in the current context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

threshold ip-pool-used *high_thresh* **[clear** *low_thresh* **]**
default threshold ip-pool-used

default

Configures the default setting.

high_thresh

Sets the high threshold percentage of addresses assigned from an IP pool that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer from 0 through 100. Default:0

clear *low_thresh*

Sets the low threshold percentage of addresses assigned from an IP pool that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm will be generated. It may be configured to any integer between0 and 100. Default: 0

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage Guidelines

Use this command to set an alert or an alarm when the number of IP addresses assigned from any pool is equal to or greater than a specified percentage of the total number of addresses in the pool.

Alerts or alarms are triggered for percentage of IP address pool addresses used based on the following rules:

- **Enter Condition**: Actual percentage of IP addresses used per pool > High Threshold
- **Clear Condition**: Actual percentage of IP addresses used per pool ≤ Low Threshold

Important This command is overridden by the settings of the **alert-threshold** keyword of the **ip pool** command.

Example

The following command configures a context-level IP pool percentage of IP addresses that are used high threshold percentage of *35* and a low threshold of *10* for an system using the Alarm thresholding model:

```
threshold ip-pool-used 35 clear 10
```

threshold ip-pool-usable

Enable the **ip-pool-usable** threshold for ip pool usable of IPs, which are in either FREE or RELEASE states.

Product

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

threshold ip-pool-usable *low_thresh* **[clear** *high_thresh* **]interval** *time*

ip-pool-usable*low_thresh*clear *high_thresh*

Configures the IP pool usable pre threshold state as either free or release. The trap is raised if the ip pool usable is less than or equal to the configured ip-pool-usable low threshold value.

The **PreThreshClearIPPoolUsable** trap gets triggered if the pool usable value is greater than a clear high threshold value.

Usage Guidelines

Use this command to set an alert or an alarm when the number of IP addresses assigned from any pool is equal to or greater than a specified percentage of the total number of addresses in the pool.

These are the types of Pre and final threshold SNMP alarms generated based on the configured thresholds:

- PreThreshIPPoolUsable alarm for entering condition
- PreThreshClearIPPoolUsable alarm for clearing condition
- FinalThreshIPPoolUsable alarm for entering condition
- FinalThreshClearIPPoolUsable alarm for clearing condition

Example

The following command configures a context-level IP pool percentage of IP addresses that are used high threshold percentage of *50* and a low threshold of *40* for an system using the Alarm thresholding model:

```
threshold ip-pool-usable 40 clear 50
```

threshold ip-pool-usable-final

Enable the **ip-pool-usable-final** threshold for ip pool usable of IPs, which are in either FREE or RELEASE states.

Product

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

threshold ip-pool-usable-final *low_thresh* **[clear** *high_thresh* **]interval** *time*

ip-pool-usable-final*low_thresh*clear *high_thresh*

Configures Configure the IP pool usable final threshold state in either free or release state.

The **FinalThreshIPPoolUsable** alarm is raised when the measured pool usable value is less than or equal to the **ip-pool-usable-final** value.

The FinalThreshClearIPPoolUsable trap clears when the ip-pool-usable-final clear value is greater than a clear threshold.

Usage Guidelines

Use this command to Configure the IP pool usable final threshold state in either free or release state.

These are the types of Pre and final threshold SNMP alarms generated based on the configured thresholds:

- PreThreshIPPoolUsable alarm for entering condition
- PreThreshClearIPPoolUsable alarm for clearing condition
- FinalThreshIPPoolUsable alarm for entering condition
- FinalThreshClearIPPoolUsable alarm for clearing condition

Example

The following command configures a context-level IP pool percentage of IP addresses that are used high threshold percentage of *36* and a low threshold of *35* for an system using the Alarm thresholding model:

```
threshold ip-pool-usable-final 35 clear 36
```

threshold monitoring

Enables or disables thresholds alerting for a group of thresholds.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[default | no] threshold monitoring available-ip-pool-group

default

Configures the default setting.

no

Disables threshold monitoring for the specified value.

available-ip-pool-group

Enables threshold monitoring for IP pool thresholds at the context level and the IP address pool-level.

Refer to the **threshold available-ip-pool-group** command, the **threshold ip-pool-x** commands and the **alert-threshold** keyword of the **ip pool** command for additional information on these values.

Usage Guidelines

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e high CPU utilization, or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps:** SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Complete descriptions and other information pertaining to these traps is located in the starentMIB(8164).starentTraps(2)section of the *SNMPMIB Reference*.

The generation of specific traps can be enabled or disabled on the system allowing you to view only those traps that are most important to you.

- **Logs:** The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.

- **Alarm System:** High threshold alarms generated within the specified polling interval are considered "outstanding" until a the condition no longer exists and/or a condition clear alarm is generated.

"Outstanding" alarms are reported to through the system's alarm subsystem and are viewable through the CLI.

The following table indicates the reporting mechanisms supported by each of the above models.

Table 4: Thresholding Reporting Mechanisms by Model

Model	SNMP Traps	Logs	Alarm System
Alert	X	X	
Alarm	X	X	X

Refer to the **threshold poll** command in Global Configuration Mode Commands for information on configuring the polling interval over which IP address pool utilization is monitored.

Example

the following command enables threshold monitoring for IP pool thresholds at the context level and the IP address pool-level:

```
threshold monitoring available-ip-pool-group
```

threshold pdsn-service init-rrq-rcvd-rate

Sets an alarm or alert based on the average number of calls setup per second for a PDSN service.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
threshold pdsn-service init-rrq-rcvd-rate high_thresh [ clear low_thresh ]
no threshold pdsn-service init-rrq-rcvd-rate
```

no

Deletes the alert or alarm.

high_thresh

Sets the high threshold average number of calls setup per second that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer between 0 and 1000000. Default: 0

clear *low_thresh*

Sets the low threshold average number of calls setup per second that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured as an integer between 0 and 1000000. Default: 0

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines Use this command to set an alert or an alarm when the average number of calls set upper second is equal to or less than a specified number of calls per second.

Alerts or alarms are triggered for the number of calls setup per second based on the following rules:

- **Enter Condition**: Actual number of calls setup per second > High Threshold
- **Clear Condition**: Actual number of calls setup per second ≤ Low Threshold

Example

The following command configures a number of calls setup per second threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold pdsn-service init-rrq-rcvd-rate 1000 clear 500
```

twan-profile

Creates a Trusted Wireless Access Network (TWAN) profile and enters the TWAN Profile Configuration Mode for the current context. The TWAN profile contains information on the RADIUS client addresses (WLC) and access-type corresponding to the RADIUS clients.

Product SaMOG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **[no] twan-profile** *twan_profile_name*

no

Deletes the TWAN profile configuration for the current context.

twan_profile_name

Specifies the name of the TWAN profile. If a *twan_profile_name* does not already exist, a new profile is created.

In Release 17 and earlier, *twan_profile_name* must be an alphanumeric string of 1 through 64 characters.

In Release 18 and later, *twan_profile_name* must be an alphanumeric string of 1 through 48 characters.

Usage Guidelines

Use this command to create a Trusted Wireless Access Network (TWAN) profile and enter the TWAN Profile Configuration Mode for the current context.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-twan-profile)#

TWAN Profile Configuration Mode commands are defined in the *TWAN Profile Configuration Mode Commands* chapter.

udr-module active-charging-service

Enables creation, configuration and deletion of the User Data Record (UDR) module for the context.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] udr-module active-charging-service`

no

Deletes the UDR module configuration for the current context.

Usage Guidelines

Use this command to create the UDR module for the context, and configure the UDR module for active charging service records. You must be in a non-local context when specifying this command, and you must use the same context when specifying the EDR module command.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-udr)#

Example

The following command creates the UDR module for the context, and enters the UDR Module Configuration Mode:

`udr-module active-charging-service`

udr-module charging-service

Enters the UDR Charging Service Configuration Mode.

Product

PDSN

HA

LNS

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

udr-module charging-service

Usage Guidelines

Use this command to enter the UDR Charging Service Configuration Mode.

Example

The following command enters the UDR Charging Service Configuration Mode:

udr-module charging-service

uidh-server

Use this command to enter the UIDH Server Configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

uidh-server *uidh_server_name*

uidh_server_name

Is a string of size ranging from 1 to 63 characters.

user-plane-service

Creates User Plane Service. Minimum or critical parameters to start a user-plane service is to have one Sx interface and thre GTPU services of the interface type PGW-ingress, SGW-ingress, and SGW-egress. The associated services must also be in the running mode. Stopping of associated services result in stopping of user-plane service. If any of the critical parameters are removed or changed from the user-plane service, it results in user-plane service being stopped. By default, this CLI command is disabled.

Product

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] user-plane-service` *<userplane_service_name>*

no

Removes the user-plane service from the particular context.

user-plane-service

Creates specified User Plane service name to allow configuration of User Plane service.

userplane_service_name

Assigns a service name to the user-plane service.

Usage Guidelines

Use this command to create the user plane service for the context and configure it.

On entering this command, the CLI prompt changes to:

[*context_name*]*hostname*(config-user-plane-service)#

Example

The following command creates the user plane service "UPLte" for the context, and enters the User Plane Service Configuration Mode:

```
user-plane-service UPLte
```

uut-profile name

Configures UE Usage Type (UUT) profile name for the current context. This command is used to enter the UUT Profile Name Configuration Mode.

Product CUPS

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **[no] uut-profile name** *profile_name*

uut-profile name *profile_name*

Specifies the name of UUT profile. *profile_name* is an alphanumeric string of 1 to 63 characters.

Usage Guidelines Enter the Configuration Mode to set the UUT profile options.

Entering this command results in the following prompt:

```
[context_name]hostname(config-uut-profile)#
```

Example

The following command disables the UUT profile with the name *prof1*.

no uut-profile name prof1

wsg-service

Enables or disables Wireless Security Gateway (WSG) service. When enabled you are in WSG Service Configuration mode. (VPC only)

Product SecGW (WSG)

Privilege Security Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **wsg-service** *service_name*
no wsg-service *service_name*

no

Disables the specified WSG service.

service_name

Specifies the name of the WSG service as an alphanumeric string of 1 through 63 characters.



Important Service names must be unique across all contexts within a chassis.

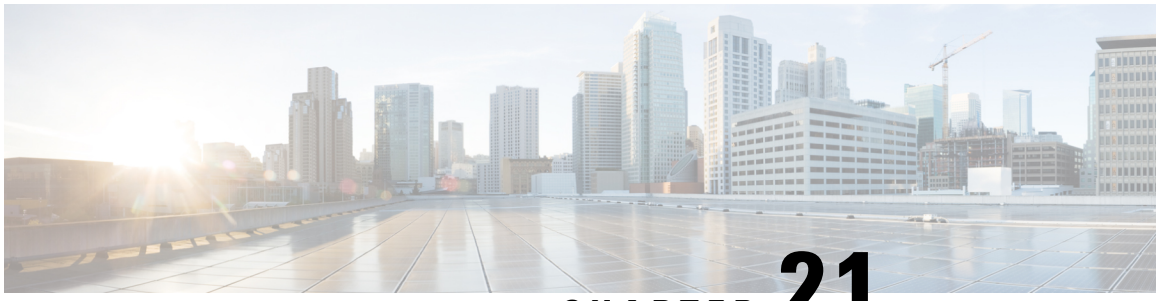
Usage Guidelines

Use this command to enter the WSG Service Configuration Mode. For additional information, see the *WSG Service Configuration Mode Commands* chapter.

Example

The following command enters the WSG Service Configuration Mode:

```
wsg-service wsg01
```



CHAPTER 21

Credit Control Configuration Mode Commands

The Credit Control configuration Mode is used to configure prepaid services for Diameter/RADIUS applications.

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

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

- apn-name-to-be-included, on page 738
- app-level-retransmission, on page 739
- associate, on page 740
- charging-rulebase-name, on page 741
- debit-failure-handling, on page 742
- diameter dictionary, on page 743
- diameter disable-final-reporting-in-ccru, on page 744
- diameter dynamic-rules request-quota, on page 745
- diameter enable-quota-retry, on page 746
- diameter exclude-mscc-in-ccr-terminate, on page 747
- diameter fui-redirected-flow, on page 747
- diameter gsu-with-only-infinite-quota, on page 748
- diameter hdd, on page 749
- diameter ignore-returned-rulebase-id, on page 750
- diameter ignore-service-id, on page 751
- diameter mscc-final-unit-action terminate, on page 752
- diameter mscc-per-ccr-update, on page 753
- diameter msg-type, on page 754
- diameter origin host, on page 756
- diameter origin endpoint, on page 756
- diameter peer-select, on page 757
- diameter pending-timeout, on page 760

- diameter reauth-blockedlisted-content, on page 761
- diameter redirect-url-token, on page 763
- diameter redirect-validity-timer, on page 765
- diameter result-code, on page 766
- diameter send-ccri, on page 767
- diameter service-context-id, on page 768
- diameter session failover, on page 769
- diameter suppress-avp, on page 770
- diameter suppress-ccru zero-gsu-with-validity-timer, on page 771
- diameter update-dictionary-avps, on page 772
- end, on page 773
- event-based-session, on page 773
- exit, on page 774
- failure-handling, on page 775
- gy-rf-trigger-type, on page 778
- imsi-imeisv-encode-format, on page 779
- mode, on page 780
- offline-session re-enable, on page 781
- pending-traffic-treatment, on page 782
- quota, on page 784
- quota request-trigger, on page 785
- quota time-threshold, on page 786
- quota units-threshold, on page 786
- quota volume-threshold, on page 787
- radius usage-reporting-algorithm, on page 788
- redirect-indicator-received, on page 789
- redirect-require-user-agent, on page 790
- servers-unreachable, on page 791
- subscription-id service-type, on page 797
- timestamp-rounding, on page 798
- trigger type, on page 799
- usage-reporting, on page 800

apn-name-to-be-included

This command configures whether the virtual or real Access Point Name (APN) is sent in Credit Control Application (CCA) messaging.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

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

default

Configures this command with the default setting.

Default: **gn**

gn

Sends the Gn APN name in the CCA messages.

virtual

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

Usage Guidelines

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

Example

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

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

app-level-retransmission

This command enables/disables application-level retransmissions with the "T" bit set.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
app-level-retransmission { set-retransmission-bit |
unset-retransmission-bit }
default app-level-retransmission
```

default

Configures this command with the default setting.

Default: **unset-retransmission-bit**

set-retransmission-bit

Sets the retransmission bit.

unset-retransmission-bit

Unsets the retransmission bit.

Usage Guidelines

Use this command to enable application-level transmission with "T" bit set.

'T' bit setting is done only for DIABASE protocol-based rerouting and not for application-based retransmissions. In order to identify such retransmissions, the server expects the T bit to be set at all levels (both DIABASE and application) of retransmission, which can be achieved with this CLI command.

Example

The following command specifies to set retransmission bit:

```
app-level-retransmission set-retransmission-bit
```

associate

This command associates/disassociates a failure handling template with the Diameter Credit Control Application (DCCA) service.

Product

GGSN

HA

HSGW

IPSG

PDSN

P-GW

S-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

associate failure-handling-template *template_name*
no associate failure-handling-template

no

Disassociates a failure handling template with the DCCA service.

failure-handling-template *template_name*

Associates a previously created failure handling template with the DCCA service. *template_name* specifies the name for a pre-configured failure handling template. *template_name* must be an alphanumeric string of 1 through 63 characters.

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

Usage Guidelines

Use this command to associate a configured failure handling template with the DCCA service.

The failure handling template defines the action to be taken when the Diameter application encounters a failure supposing a result-code failure, Tx-expiry or response-timeout. The application will take the action given by the template. For more information on failure handling template configurations, refer to the *Diameter Failure Handling Template Configuration Mode Commands* chapter.



Important Only one failure handling template can be associated with the DCCA service. The failure handling template should be configured prior to issuing this command.

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

Example

The following command associates a pre-configured failure handling template called *fht1* to the DCCA service:

```
associate failure-handling-template fht1
```

charging-rulebase-name

This command allows static configuration of charging rulebase name to be sent to OCS through the CCR message.

Product

eHRPD

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

charging-rulebase-name *rulebase_name*
no charging-rulebase-name

no

The **no** variant, when configured, sends the rulebase that was configured in APN/subscriber template to the OCS.

rulebase_name

Specifies the name for a charging rulebase to be sent to OCS via CCR message. *rulebase_name* must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to override/change the charging rulebase name in the Gy CCRs for eHRPD, GGSN and P-GW service types.

With this feature in 18.0 release, an APN/subscriber can have a single rulebase applied to it, but allowing a static configuration to always pass a different or same rulebase to the OCS through CCR messages.

The rulebase value configured in Credit Control (CC) group will be sent to OCS via CCR. If this CLI command is not configured, then the rulebase obtained from APN/subscriber template will be sent to OCS.

The configured value of rulebase under CC group is sent in all CCR (I/U/T) messages. This implies that any change in rulebase value in CC group during mid-session gets reflected in the next CCR message.

Example

The following command defines a charging rulebase name called *rb1* in the credit control group:

charging-rulebase-name rb1

debit-failure-handling

This command specifies the Diameter Credit Control Debit Failure Handling behavior.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

debit-failure-handling { continue | terminate-or-buffer }
default debit-failure-handling

default

Configures this command with the default setting.

Default: **continue**

continue

Continues processing in the event of a Diameter communication failure.

terminate-or-buffer

Terminates or buffers in the event of a Diameter communication failure.

Usage Guidelines

Use this command to configure the Diameter Credit Control Debit Failure Handling behavior.

Example

The following command sets the Diameter Credit Control Debit Failure Handling behavior to **continue**:

```
debit-failure-handling continue
```

diameter dictionary

This command configures the Diameter Credit Control dictionary for the Active Charging Service (ACS).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
diameter dictionary { dcca-custom1 | dcca-custom10 | dcca-custom11 |
dcca-custom12 | dcca-custom13 | dcca-custom14 | dcca-custom15 |
dcca-custom16 | dcca-custom17 | dcca-custom18 | dcca-custom19 |
dcca-custom2 | dcca-custom20 | dcca-custom21 | dcca-custom22 |
dcca-custom23 | dcca-custom24 | dcca-custom25 | dcca-custom26 |
dcca-custom27 | dcca-custom28 | dcca-custom29 | dcca-custom3 |
dcca-custom30 | dcca-custom4 | dcca-custom5 | dcca-custom6 | dcca-custom7
 | dcca-custom8 | dcca-custom9 | dynamic-load | standard }
default diameter dictionary
```

default

Configures this command with the default setting.

Default: standard dictionary

dcca-custom1 ... dcca-custom30

Configures a custom Diameter dictionary.

dynamic-load

Configures the dynamically loaded Diameter dictionary. The dictionary name must be an alphanumeric string of 1 through 15 characters.

For more information on dynamic loading of Diameter dictionaries, see the **diameter dynamic-dictionary** in the *Global Configuration Mode Commands* chapter of this guide.

standard

Configures the standard Diameter dictionary.

Default: Enabled

Usage Guidelines

Use this command to select the Diameter dictionary for ACS.

Example

The following command selects the standard Diameter dictionary:

```
diameter dictionary standard
```

diameter disable-final-reporting-in-ccru

This command controls sending of CCR-U with reporting reason as FINAL immediately on receiving a 4012 or 4010 result-code at MSCC level.

Product



Important In StarOS release 16.0 and later, this command is obsolete and is only supported for backward compatibility reasons. Release 16.0 and beyond, use the diameter msg-type { ccru| ccrt } suppress-final-reporting command for this functionality.

GGSN

HA

IPSG

PDSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
diameter disable-final-reporting-in-ccru
{ default | no } diameter disable-final-reporting-in-ccru
```

default | no

Configures this command with the default setting. Default behavior is to send CCR-U with reporting reason as FINAL immediately on receiving 4010/4012 result-code.

Usage Guidelines

As per the current implementation, CCR-U is sent immediately on receiving 4010 or 4012 Result-Code at MSCC level. This new CLI command controls sending of immediate CCR-U with FINAL as Reporting-Reason. All other behaviors remain almost same like a Rating-group being blacklisted.

If this CLI command is configured, on receiving the result-code 4010/4012 at MSCC-level, immediate CCR-U with FINAL as Reporting-Reason will not be sent. All USU corresponding to that rating group is reported in CCR-T message.

Example

The following command specifies not to send immediate CCR-U with FINAL as Reporting-Reason:

```
diameter disable-final-reporting-in-ccru
```

diameter dynamic-rules request-quota

This command specifies to request quota immediately in the CCR sent to the Gy interface when the traffic matches the dynamic rules with Online AVP enabled and received over Gx interface.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
diameter dynamic-rules request-quota { on-traffic-match | on-receiving-rule
 }
default diameter dynamic-rules request-quota
```

default

Configures this command with the default setting.

Default: **on-receiving-rule**

on-traffic-match

Requests quota only when there is traffic matching the dynamic rules with Online AVP enabled.

on-receiving-rule

Requests quota on receiving a dynamic rule with Online AVP enabled.

Usage Guidelines Use this command to request quota when the traffic matches the dynamic rules with Online AVP enabled.

Example

The following command specifies to request quota on receiving a dynamic rule with Online AVP enabled:

```
diameter dynamic-rules request-quota on-receiving-rule
```

diameter enable-quota-retry

This command enables/disables Quota Retry Timer for blockedlisted content.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
[ no ] diameter enable-quota-retry end-user-service-denied
```

no

Configures this command with the default setting.

Usage Guidelines Quota-Retry-Time is currently not applicable to a Rating-Group which is blockedlisted with 4010 (END_USER_SERVICE_DENIED).

If this CLI command is configured, after the quota-retry timeout, CCR-U including the RSU is sent for blockedlisted content also. That is, quota will be requested for 4010 blacklisted content also.

Without the configuration of this CLI command, the old behavior persists that is, after quota retry-timer expiry, CCR-U is not sent for 4010 blacklisted category.

Example

In releases prior to StarOS 21.26:

The following command allows sending CCR-U requesting quota for blacklisted content:

diameter enable-quota-retry end-user-service-denied

diameter exclude-mscc-in-ccr-terminate

This command enables to exclude Multiple-Services-Credit-Control (MSCC) AVP in CCR-T message.

Product

GGSN

IPSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-dcca)#`

Syntax Description

[default | no] diameter exclude-mscc-in-ccr-terminate

default

Includes MSCC AVP in CCR-T.

no

Includes MSCC AVP in CCR-T.

Usage Guidelines

Use this command to exclude MSCC AVP in CCR-T, which is included by default.

Also, see the **diameter mscc-per-ccr-update** command.

Example

The following command specifies to exclude MSCC AVP in CCR-T:

diameter exclude-mscc-in-ccr-terminate

diameter fui-redirected-flow

This command enables to control the behavior of marking redirected HTTP flow as free-of-charge.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
[ no ] diameter fui-redirected-flow allow
```

no

Disables the behavior of marking redirected HTTP flow as free-of-charge.

Default: **diameter fui-redirected-flow allow**

Usage Guidelines

Use this command to control the behavior of marking redirected HTTP flow as free-of-charge when the Final-Unit-Indication (FUI) Diameter AVP comes without Filter IDs.

Important Note that the default value, when configured, does not appear in the output of the **show configuration** command output; instead appear only in the output of the **show configuration verbose** command. When the HTTP redirection feature is disabled using the **no diameter fui-redirected-flow allow** command, it will be appear in the output of the **show configuration** command.

Example

The following command specifies to allow the packets free of charge, when matching the redirected-flow:

```
diameter fui-redirected-flow allow
```

diameter gsu-with-only-infinite-quota

This command configures whether to accept/reject CCA messages that contain Granted-Service-Unit AVP with only infinite quota grants from the server.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
diameter gsu-with-only-infinite-quota { accept-credit-control-answer |
reject-credit-control-answer }
default diameter gsu-with-only-infinite-quota
```

default

Configures this command with the default setting.

Default: **reject-credit-control-answer**

accept-credit-control-answer

Accepts the Credit-Control-Answer message.

reject-credit-control-answer

Rejects the Credit-Control-Answer message.

Usage Guidelines

Use this command to accept/reject CCA messages that contain the Granted-Service-Unit AVP with only infinite quota grants from the server.

Example

The following command specifies to accept CCA with the Granted-Service-Unit AVP containing only Infinite quota:

```
diameter gsu-with-only-infinite-quota accept-credit-control-answer
```

diameter hdd

This command enables/disables the Hard Disk Drive (HDD) to store the failed CCR-T messages for the corresponding credit control group.



Important This command is license dependent. For more information, contact your Cisco account representative.

Product

HA

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
[ no ] diameter hdd
```

no

Disables the HDD from storing the failed CCR-T messages for the corresponding credit control group.

Usage Guidelines

Use this command to enable the HDD to store the failed CCR-T messages. The Gy application sends the failed CCR-T messages to the CDR module for storing in the HDD. By default, this feature is disabled.

In the existing implementation with Assume Positive feature, there are high chances of losing the usage data reported through the CCR-T when the session is being terminated while in Assume Positive mode. This problem is addressed by allowing the DCCA module to write the CCR-T messages in the HDD of the chassis.

In cases where the Assume-Positive interim-quota is allocated, and CCR-T is not reported/answered, the CCR-T message is written to a local file, and saved in the HDD. This local file and directory information can be fetched and parsed to account for the lost bytes/usage. The retrieval of the file can be done with the PULL mechanism.



Important This feature requires a valid license to be installed prior to configuring this feature. Contact your Cisco account representative for more information on the licensing requirements.



Important This feature is applicable only when Assume Positive feature is enabled.

For more information on this feature, see the *AAA Interface Administration and Reference* document.

Limitations:

- When an ICSR event occurs unexpectedly before the CCR-T is written, the CCR-T will not written to the HDD and hence the usage will be lost.
- It is expected that the customers requiring this feature should monitor the HDD and periodically pull and delete the files so that the subsequent records can be buffered.

The **diameter-hdd-module** CLI command is used to configure the file characteristics for storing the Diameter records (CCR-Ts) in the HDD. For more information on this command, see the *Diameter HDD Module Configuration Mode Commands* chapter in this guide.

Example

The following command enables the HDD to store the failed CCR-T messages:

```
diameter hdd
```

diameter ignore-returned-rulebase-id

This command configures to accept/ignore the rulebase ID in the Rulebase-Id AVP returned by the Diameter server in CCA messages.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

[default | no] diameter ignore-returned-rulebase-id

default

Configures this command with the default setting.

Default: Accept

no

Accepts the rulebase ID received from Diameter server in CCA.

Usage Guidelines

Use this command to ignore/accept rulebase ID returned from the Diameter server in CCA.

Example

The following command ignores the rulebase ID returned from the Diameter server in CCA:

diameter ignore-returned-rulebase-id

diameter ignore-service-id

This command enables to accept/ignore service ID in the Service-Identifier AVP defined in the Diameter dictionaries. This command is applicable to all products that use the Gy interface.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

[default | no] diameter ignore-service-id

default

Configures this command with the default setting.

Default: Accept

no

Specifies to accepts the service ID.

Usage Guidelines

Use this command to ignore/accept service ID value in the Service-Identifier AVP in the Diameter dictionaries for Gy interface implementations.

This command can be used to disable the usage of the Service-Identifier AVP for Gy interface implementations even if any of the Diameter dictionaries support the Service-Identifier AVP, and if this AVP should not be used for Gy interactions but must be present in GCDRs/eGCDRs.

Example

The following command specifies to ignore service ID in the Diameter dictionaries:

```
diameter ignore-service-id
```

diameter mscc-final-unit-action terminate

This command enables either to terminate a PDP session immediately when the Final-Unit-Action (FUA) in a particular Multiple Service Credit Control (MSCC) is set as TERMINATE and the quota is exhausted for that service, or to terminate the session after all other MSCCs (categories) have used up their available quota.



Important This command is available only in StarOS 10.2 and later releases.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
diameter mscc-final-unit-action terminate { category | session {
on-per-mscc-exhaustion | on-all-mscc-exhaustion } }
default diameter mscc-final-unit-action terminate
```

default

Configures this command with the default setting.

Default: Same as **diameter mscc-final-unit-action terminate category**

category

This is the standard behavior wherein the category is terminated if the Final-Unit-Indication AVP comes with TERMINATE for a given MSCC.

session { on-per-mscc-exhaustion | on-all-mscc-exhaustion }

Terminates the session depending on the quota usage of one MSCC or all the MSCCs.

on-per-mscc-exhaustion: When the FUA in a particular MSCC is set as TERMINATE and the quota is exhausted for that service, the session will be terminated immediately regardless of the state of the other MSCCs.

on-all-mscc-exhaustion: When the FUA in a particular MSCC is set as TERMINATE and the quota is exhausted for that service, the session termination will be initiated after all the other MSCCs (categories) have used up their available quota. There will no more CCR(U) messages sent requesting quota after receiving the FUA as TERMINATE in the MSCC level.

Usage Guidelines

Use this command to terminate a PDP session immediately when the FUA in a particular MSCC is set as TERMINATE and the quota is exhausted for that service, or to terminate the session after all other MSCCs (categories) have used up their available quota.

Example

The following command terminates the PDP session after quota exhausts for all MSCCs when MSCC FUA is set to TERMINATE:

```
diameter mscc-final-unit-action terminate session on-all-mscc-exhaustion
```

diameter mscc-per-ccr-update

This command configures sending single/multiple Multiple-Services-Credit-Control (MSCC) AVP in CCR-U messages.



Important This command is available only in StarOS 8.3 and later releases.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
diameter mscc-per-ccr-update { multiple | single }
default diameter mscc-per-ccr-update
```

default

Configures this command with the default setting.

Default: **multiple**

multiple

Sends multiple Multiple-Services-Credit-Control AVP in a single CCR-U message.

single

Sends only one Multiple-Services-Credit-Control AVP in a CCR-U message.

Usage Guidelines

Use this command to configure sending single/multiple Multiple-Services-Credit-Control AVP in CCR-U messages.

Example

The following command configures sending a single Multiple-Services-Credit-Control AVP in CCR-U messages:

```
diameter mscc-per-ccr-update single
```

diameter msg-type

This command controls sending of CCR-U/CCR-T with reporting reason as FINAL immediately on receiving a 4012 or 4010 result-code at MSCC level or when the MSCC is in FUI Redirect/Restrict-access state.

Product

GGSN

HA

IPSG

PDSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

In 18 and later releases:

```
[ no ] diameter msg-type { ccru { suppress-final-reporting } | ccrt {
suppress-final-reporting | suppress-blacklist-reporting } }
```

In 17 and earlier releases:

```
diameter msg-type { ccru | ccrt } suppress-final-reporting
[ no ] diameter msg-type ccru suppress-final-reporting
```

no

Depending on the configuration, this keyword will selectively send FINAL either in CCR-U or CCR-T even if MSCC is in FUI Redirect/Restrict-access state and USU is zero.

The default behavior is to not send CCR-T with reporting reason as FINAL even when MSCC is in FUI Redirect/Restrict-access state and USU is zero.



Important This default behavior is applicable to all dictionaries except for dcca-custom12 and dcca-custom13 dictionaries. In the case of dcca-custom12 and dcaa-custom13, the FINAL reporting will always be sent in CCR-T even if MSCC is in FUI Redirect/Restrict-access and USU is zero.

ccru

This keyword disables Immediate FINAL reporting for result code 4010/4012 in CCR-U message.

ccrt

This keyword disables FINAL reporting for MSCC which are in no-quota and FUI Redirect/Restrict-access state.

suppress-final-reporting



Important This keyword is available only in 18.3, 19.2 and later releases.

When used with the **diameter msg-type ccru** command, this keyword disables immediate FINAL reporting for result code 4010/4012. When used with the **diameter msg-type ccrt** command, this keyword disables FINAL reporting for no-quota FUA Redirect/Restrict-access.

suppress-blacklist-reporting



Important This keyword is available only in 18.3, 19.2 and later releases.

Disables FINAL reporting for blacklisted (4010/4012) content in CCR-T.

Usage Guidelines

With this CLI command "diameter msg-type ccrt suppress-final-reporting" configured:

Before MSCC enters into FUI Redirect or Restrict-Access state, all the used quota is reported using the Reporting-Reason as "OTHER_QUOTA_TYPE". Since all the quota is reported, there is no need to send any other FINAL reporting to OCS.

Releases prior to 16.0, even if there is no quota utilization, the gateway sends FINAL with USU as '0' octets in CCR-T. In this release, the FINAL reporting in CCR message is controlled when there is no quota usage to report to the OCS server during the FUI Redirect/Restrict-access scenario.

With this CLI command "diameter msg-type ccru suppress-final-reporting" configured:

In releases prior to 15.0, CCR-U is sent immediately on receiving 4010 or 4012 Result-Code at MSCC level. This new CLI command controls sending of immediate CCR-U with FINAL as Reporting-Reason. All other behaviors remain almost same like a Rating-group being blacklisted.

If this CLI command is configured, on receiving the result-code 4010/4012 at MSCC-level, immediate CCR-U with FINAL as Reporting-Reason will not be sent. All USU corresponding to that rating group is reported in CCR-T message.

In releases prior to 18, configuration control was available for filtering FINAL USU reporting in CCR-U for blacklisted content and in CCR-T for Final-Unit-Indication (REDIRECT/RESTRICT-ACCESS) activated content. In the case of CCR-T message, there is no way to ignore the FINAL reporting for blacklisted (4010/4012) content if the FINAL was previously disabled in CCR-U.

In 18 and later releases, the current CLI configuration is enhanced to disable FINAL reporting in CCR-T message for blacklisted (4010/4012) content. The **diameter msg-type ccrt** CLI command includes an additional keyword **suppress-blacklist-reporting** to support this enhancement. The default behavior of CCR-T is to send the FINAL reporting to be sent for blacklisted (4010/4012) content, if not reported already in CCR-U.



Important This feature is available only in 18.3, 19.2 and later releases.

This feature is used to selectively control the reporting of FINAL Used-Service-Unit (USU) in CCR-T for a Rating-Group (RG) which is blacklisted using 4010 and 4012 transient result-codes. This customization is required for a seamless integration with the operator network.

Example

The following command specifies not to send FINAL reporting for FUA Redirect/Restrict-access:

```
diameter msg-type ccrt suppress-final-reporting
```

diameter origin host

This command is obsolete. See the diameter origin endpoint, on page 756 command.

diameter origin endpoint

This command configures the Diameter Credit Control Origin Endpoint.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

diameter origin endpoint *endpoint_name* **[realm** *realm_name* **]**
no diameter origin endpoint

no

Removes the Diameter Credit Control Origin Endpoint configuration.

endpoint *endpoint_name*

Specifies the Diameter Credit Control Origin Endpoint name as an alphanumeric string of 1 through 63 characters.

realm *realm_name*

Specifies the Diameter Credit Control Realm ID as an alphanumeric string of 1 through 127 characters.

Usage Guidelines

Use this command to configure the Diameter Credit Control Origin Endpoint.

The endpoint to configure should be pre-configured. For information on creating and configuring a Diameter endpoint, see the **diameter endpoint** command in the Context Configuration mode.

Example

The following command configures a Diameter Credit Control Origin Endpoint named *test*:

```
diameter origin endpoint test
```

diameter peer-select

This command configures the Diameter credit control primary and secondary hosts for DCCA.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

In 8.x and earlier releases:

diameter peer-select peer *peer_name* **[realm** *realm_name* **] [secondary-peer** *secondary_peer_name* **[realm** *realm_name* **]] [imsi-based start-value** *imsi_start_value* **end-value** *imsi_end_value* **]**
no diameter peer-select [imsi-based start-value *imsi_start_value* **end-value** *imsi_end_value* **]**

In 9.0 and later releases, for UMTS deployments:

diameter peer-select peer *peer_name* **[realm** *realm_name* **] [secondary-peer** *secondary_peer_name* **[realm** *realm_name* **]] [imsi-based { { prefix | suffix }** *imsi/prefix/suffix_start_value* **} [to** *imsi/prefix/suffix_end_value* **]] [msisdn-based { { prefix | suffix }** *msisdn-based/prefix/suffix_start_value* **} [to** *msisdn-based/prefix/suffix_end_value* **]]**
no diameter peer-select [imsi-based { { prefix | suffix } *imsi/prefix/suffix_start_value* **} [to** *imsi/prefix/suffix_end_value* **]] | [msisdn-based { { prefix | suffix }** *msisdn-based/prefix/suffix_start_value* **} [to** *msisdn-based/prefix/suffix_end_value* **]]**

no

Removes previously configured Diameter credit control peer selection setting.

peer ***peer_name***

Specifies the primary host name. as an alphanumeric string of 1 through 63 characters that can contain punctuation characters.

imsi-based start-value ***imsi_start_value*** **end-value** ***imsi_end_value***

Important This section applies only to 8.3 and earlier releases.

Specifies peer selection based on International Mobile Subscriber Identification (IMSI) range.

start-value *imsi_start_value* specifies the start of range in integer value of IMSI, and **end-value** *imsi_end_value* specifies the end of range in integer value of IMSI.

imsi-based { { prefix | suffix } ***imsi/prefix/suffix_start_value*** **} [to** ***imsi/prefix/suffix_end_value*** **]**

Important This section applies only to 9.0 and later releases for UMTS deployments.

Selects peer based on IMSI prefix or suffix or IMSI range.

prefix: Specifies the prefix range

suffix: Specifies the suffix range

imsi/prefix/suffix_start_value: Specifies the IMSI/prefix/suffix start value. *prefix/suffix* must be an IMSI prefix/suffix, and must be an integer from 1 through 15 characters.

imsi/prefix/suffix_end_value: Specifies the IMSI/prefix/suffix end value. *prefix/suffix* must be an IMSI prefix/suffix, and must be an integer from 1 through 15 characters that must be greater than the start value.

Important If prefix/suffix is used, the lengths of both start and end prefix/suffix must be equal. If the **prefix** or **suffix** keyword is not specified, it will be considered as suffix.

msisdn-based { { prefix | suffix } *msisdn/prefix/suffix_start_value* } [to *msisdn/prefix/suffix_end_value*]

Specifies peer selection based on MSISDN prefix or suffix or MSISDN range.

prefix: Specifies the prefix range

suffix: Specifies the suffix range

msisdn/prefix/suffix_start_value: Specifies the MSISDN/prefix/suffix start value. *prefix/suffix* must be an MSISDN prefix/suffix, and must be an integer from 1 through 15 characters.

msisdn/prefix/suffix_end_value: Specifies the MSISDN/prefix/suffix end value. *prefix/suffix* must be an MSISDN prefix/suffix, and must be an integer from 1 through 15 characters that must be greater than the start value.

realm *realm_name*

The *realm_name* must be an alphanumeric string of 1 through 127 characters, and can contain punctuation characters. The realm may typically be a company or service name.

secondary-peer *secondary_peer_name*

Specifies a name for the secondary host to be used for failover processing. When the route-table does not find an AVAILABLE route, the secondary host performs a failover processing if the diameter session failover, on page 769 command is set.

secondary_peer_name must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters.

Usage Guidelines

Use this command to configure Diameter credit control host selection.

If the **diameter peer-select** command is not configured, and if multiple peers are configured in the endpoint, the available peers configured in the endpoint are automatically chosen in a load-balanced round-robin manner.

9.0 and later releases support peer selection using prefix or suffix of IMSI or IMSI range. Subscribers are now assigned to a primary OCS instance based on the value of the IMSI prefix or suffix of a length of 1 to 15 digits. If the prefix or suffix keyword is not specified, it will be considered as suffix. Up to 64 peer selects can be configured. At a time either prefix or suffix mode can be used in one DCCA config. If prefix or suffix mode is used, the lengths of all prefix/suffix must be equal.

In 12.2 and later releases, Diameter peer selection can also be performed based on the configurable prefix or suffix of MSISDN or MSISDN range.

Each primary OCS may have a designated secondary OCS in case of failure of the primary. It will be the responsibility of the GGSN to use the appropriate secondary OCS in case of primary failure. The secondary OCS for each primary OCS will be one of the existing set of OCSs.



Note Load-balancing is not supported if the **diameter peer-select** command is configured under the credit control group.

If the directly connected hosts/peers are configured under the credit control application, thenround-robin selection is not available even if the equal weighted peers are configured under the diameter end-point. In this scenario, the primary host/peer configured under the credit control group have precedence and selected always.

Example

The following command configures a Diameter credit control peer named *test* and the realm *companyx*:

```
diameter peer-select peer test realm companyx
```

The following command configures IMSI-based Diameter credit control peer selection in the IMSI range of *1234567890* to *1234567899*:

```
diameter peer-select peer star imsi-based start-value 1234567890 end-value
 1234567899
```

The following command configures IMSI-based DCCA peer selection with IMSI suffix of *100* through *200*:

```
diameter peer-select peer test_peer realm test_realm secondary-peer
test_sec_realm realm test_realm2 imsi-based suffix 100 to 200
```

diameter pending-timeout

This command configures the maximum time period to wait for response from a Diameter peer.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
diameter pending-timeout duration deciseconds msg-type { any | ccr-event |
 ccr-initial | ccr-terminate | ccr-update }
default diameter pending-timeout
```

default

Disables DCCA resending message at pending-timeout.

duration

Specifies the timeout duration (in deciseconds). The value must be an integer from 1 through 3000.

deciseconds msg-type { any | ccr-event | ccr-initial | ccr-terminate | ccr-update }

Specifies independent timers (in deciseconds) for all message types like CCR-I, CCR-U, CCR-T and CCR-E. The default time will be 100 deciseconds (10 seconds).

This keyword option provides additional flexibility for operator to configure independent timers with reduced granularity.

This feature implementation ensures that the timer configuration is backward compatible. If the CLI command is configured without "**desiseconds**" and "**msg-type**", the configured time will be taken as seconds and while displaying the CLI it will be converted to deciseconds and msg-type will be "**any**".

after-expiry-try-secondary-host

This keyword is deprecated. This can now be managed using the **retry-after-tx-expiry** and **go-offline-after-tx-expiry** keywords in the **failure-handling** command.

Usage Guidelines

Use this command to set the maximum time for Diameter credit control to receive a response from its peer.

DCCA refers to this as the Tx Timer. Typically, this should be configured to a value smaller than the response-timeout value of Diameter Endpoint Configuration Mode. That value is typically too large for DCCA's purposes.

If DCCA gets a "no available routes" error before pending-timeout expires, then DCCA tries to send to the secondary host (if one has been configured). If DCCA gets no response and pending-timeout expires, then DCCA either tries the secondary host or gives up. This can now be managed using the **failure-handling** command.

If routing has failed, i.e., the attempt to the primary host, as well as, the attempt to the secondary host (if that has been configured), then the processing configured by the **failure-handling** command is performed.

The routing (i.e., returning a good response, no response or an error response such as "no available routes") is controlled by Diameter Endpoint Configuration Mode. That uses a watchdog timer (called Tw Timer) to attempt a different route to a host. Multiple routes could be attempted. If there's no response before the endpoint's configured response-timeout expires, then "no available routes" is the routing result. The routing logic remembers the status of routes, so it can return "no available routes" immediately, without using any timers.

The default case will disable DCCA resending message at Tx (pending-timeout). So messages are retried only at Tw (device watchdog timeout) by diabase or at response-timeout by DCCA.

Example

The following command configures a Diameter Credit Control Pending Timeout setting of *20* seconds:

```
diameter pending-timeout 20
```

diameter reauth-blockedlisted-content

This command allows reauthorization of blockedlisted content (blacklisted with Result-Code like 4012, 4010, etc) when a Rating Group (RG) based Re-Authorization Request (RAR) or generic RAR is received.

Product

GGSN

HA

IPSG

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

In releases prior to StarOS 21.26:

```
diameter reauth-blacklisted-content [ content-based-rar ]
no diameter reauth-blacklisted-content
```

From StarOS 21.26 and later releases:

```
diameter reauth-blockedisted-content [ content-based-rar ]
no diameter reauth-blockedlisted-content
```

no

Configures this command with the default setting. That means, the reauthorization of blockedlisted RG will not happen.

content-based-rar

Reauthorizes blockedlisted RG only when RG specific RAR is received.

Usage Guidelines

The current Gy implementation does not allow reauthorization of Blockedlisted content (blacklisted with Result-Code like 4012, 4010, etc) when Gy receives an RAR (either a RG based RAR or generic RAR).

With this CLI based enhancement, it is possible to perform one of the following actions:

- to reauthorize blockedlisted RG only when RG specific RAR is received.
- to reauthorize blockedlisted RG on any kind of RAR (both RG specific or generic).
- do not reauthorize blockedlisted RG (default implementation).

This feature determines if the RAR received from OCS is generic or to any specific rating-group.

If it is a generic RAR:



Note From StarOS 21.26 and later releases, the term “blacklist” is replaced with “blockedlist” in the help string.

- If this CLI command "**diameter reauth-blacklisted-content**" is configured, then reauthorize all the Rating-Groups (RGs) which are blacklisted. CCR-U forced-reauthorization will be triggered all the RGs.
- If this CLI command "**diameter reauth-blacklisted-content content-based-rar**" is configured, then RG which are blacklisted will not be reauthorized. CCR-U forced-reauthorization will be triggered only for active RGs alone.

If Rating-Group information is received in RAR:

Note From StarOS 21.26 and later releases, the term “blacklist” is replaced with “blockedlist” in the help string.

- If either "**diameter reauth-blacklisted-content**" or "**diameter reauth-blacklisted-content content-based-rar**" is configured, then RG gets re-authorized even it is blacklisted. CCR-U forced-reauthorization will be triggered for the received RG.

If this CLI command is not configured, then the default behavior which is not to reauthorize blacklisted RG persists.

Example

In releases prior to StarOS 21.26:

The following command enables reauthorization of blacklisted content on receiving RG specific RAR:

```
diameter reauth-blacklisted-content [ content-based-rar ]
```

From StarOS 21.26 and later releases:

The following command enables reauthorization of blockedisted content on receiving RG specific RAR:

```
diameter reauth-blockedlisted-content [ content-based-rar ]
```

diameter redirect-url-token

This command allows configuring a token to be used for appending original URL to the redirect address.

Important This command is customer specific. For more information contact your Cisco account representative.

Product

GGSN

HA

IPSG

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

diameter redirect-url-token *string*
default diameter redirect-url-token

default

Configures this command with the default setting.

string

The redirect url token name must be an alphanumeric string of size 1 through 63 characters.

Usage Guidelines

The chassis should perform dynamic Advice of Charge (AoC) redirections (URL provided by Online Charging System (OCS)) for a particular Service ID/Rating Group combination without affecting the flows mapped to other Service ID/Rating Group combinations. Redirections can be removed by OCS for a particular MSCC (Service ID/Rating Group combination) using a RAR message containing a specific Service ID/Rating Group combination.

As part of redirection to an AoC or Top-UP server (302 Moved HTTP message) the PCEF should be able to append the original HTTP URL to the redirected session. This way, once the subscriber has successfully been redirected (and potentially topped up their prepaid account) they can be presented with an option to be redirected back to their original URL. The OCS can indicate to the PCEF if the original URL is to be appended to the redirection by specifying a special character to the end of the AoC redirection — for example, a "?" character.

Upon final unit indication a redirect server address will be returned together with the FUI.

On redirection, the redirect URL will be appended with the original URL information using the token name configured with the **diameter redirect-url-token** command so that on completion of AoC, the AoC server may redirect the client back to the original location.

The rules for appending the original URL before redirection are as follows:

1. The "?" character at the end of the AoC page provided by the OCS in the redirect URL will be replaced with the "&" character.
2. A configurable parameter will be appended after the "&" character. The parameter whose name will be defined in a command line in the chassis configuration. The parameter name is case sensitive.
3. An "=" will be appended to the parameter.
4. The subscriber's original URL will be appended to the "=" character.

The following table shows an example of how the URL redirection is implemented.

If	Then
the original URL was ***http://homepage/*** and OCS provided URL is: *href="http://test.dev.mms.ag/test/aoc.htm?appName=Return&* *CODE=UPSELL&OCSCode=FWB&SessionID=4:0001-diamproxy.* *st40gy2;130020198;9243;1b02:12000:12000:H:AOC:1299597546:UPSELL:N* *&transID=AOCPurchasepage**?***	the dynamic AoC redirection is implemented as shown in the following example: *http://test.dev.mms.ag/test/aoc.htm?appName=Return&* *CODE=UPSELL&OCSCode=FWB&SessionID=4:0001-diamproxy.* *st40gy2;130020198;9243;1b02:12000:12000:H:AOC:1299597546:UPSELL:N* *&transID=AOCPurchasepage**&returnUrl*** ***=http%3A%2F%2Fhomepage%2F***

Example

The following command configures the redirect-url-token as *returnUrl*:

diameter redirect-url-token *returnUrl*

diameter redirect-validity-timer

This command allows you to control the starting of validity timer for the FUI-redirect scenario.

Product

GGSN

HA

IPSG

PDSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

`[local]host_name(config-dcca)#`

Syntax Description

diameter redirect-validity-timer { immediate | traffic-start }
default diameter redirect-validity-timer

default

Configures this command with the default setting. By default, the validity timer is started on receiving the first matching packet.

immediate

This keyword will make the redirect-validity-timer to get started immediately.

traffic-start

This keyword will make the redirect-validity-timer to get started only on receiving matchingtraffic. This is the default configuration.

Usage Guidelines

Use this CLI command to control the starting of validity timer on receipt of CCA in all cases. Based on the configuration value, DCCA decides when to start the redirect-validity-timer. By default, it is started on receiving the first matching packet.

Example

The following command configures the redirect-validity-timer to get started immediately on receiving CCA:

```
diameter redirect-validity-timer immediate
```

diameter result-code

This command enables sending a GTP Create-PDP-Context-Rsp message with cause code based on the DCCA result code.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
diameter result-code { authorization-rejected | credit-limit-reached |
end-user-service-denied | user-unknown } use-gtp-cause-code {
apn-access-denied-no-subscription | authentication-failure |
no-resource-available | system-failure }
default diameter result-code { authorization-rejected |
credit-limit-reached | end-user-service-denied | user-unknown }
use-gtp-cause-code
```

default

Configures this command with the default setting.

In 12.1 and earlier releases: **no-resource-available**

In 12.2 and later releases: **system-failure**

authorization-rejected

Result code received as DIAMETER_AUTHORIZATION_REJECTED(5003).

credit-limit-reached

Result code received as DIAMETER_CREDIT_LIMIT_REACHED(4012).

end-user-service-denied

Result code received as DIAMETER_END_USER_DENIED(4010).

user-unknown

Result code received as DIAMETER_USER_UNKNOWN(5030).

use-gtp-cause-code

Cause code to be sent in GTP response.

apn-access-denied-no-subscription

Sends the GTP cause code GTP_APN_ACCESS_DENIED_NO_SUBSCRIPTION in GTP response.

If this keyword is configured and if the CCR-U is received with auth-rejected(5003) or credit-limit-reached(4012) or user-unknown(5030) or end-user-service-denied(4010), then the GTP result-code is sent as "apn-access-denied-no-subscription".

authentication-failure

Sends the GTP cause code GTP_USER_AUTHENTICATION_FAILED in GTP response.

no-resource-available

Sends the GTP cause code GTP_NO_RESOURCES_AVAILABLE in GTP response.

system-failure

Sends the GTP cause code GTP_SYSTEM_FAILURE in GTP response.

Usage Guidelines

On receiving result-code as AUTHORIZATION-REJECTED, CREDIT_LIMIT_REACHED, END_USER_DENIED or USER_UNKNOWN from DCCA server, based on this CLI configuration, in GTP Create-PDP-Context Response message the cause code can either be sent as GTP_NO_RESOURCE_AVAILABLE or GTP_AUTHENTICATION_FAILED or GTP_SYSTEM_FAILURE or GTP_APN_ACCESS_DENIED_NO_SUBSCRIPTION.

Example

The following command sets the deny cause as user authentication failure when the CCA-Initial has the result code DIAMETER_AUTHORIZATION_REJECTED(5003):

```
diameter result-code authorization-rejected use-gtp-cause-code
authentication-failure
```

diameter send-ccri

This command configures when to send an initial Credit Control Request (CCR-I) for the subscriber session.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
diameter send-ccri { session-start | traffic-start }
default diameter send-ccri
```

default

Configures this command with the default setting.

Default: **session-start**

session-start

Sends CCR-I when the PDP context is being established (on receiving Create-PDP-Context-Request).

traffic-start

Delays sending CCR-I until the first data packet is received from the subscriber.



Important Please note that the CCR-I will be sent only with the default rulebase and not with Rulebase list even if the **rulebase-list** configuration is enabled. When the **rulebase-list** command is used in conjunction with **diameter send-ccri traffic-start** command, the former one's function is invalidated. The rulebase-list is used to allow the OCS to select one of the rulebases from the list configured during the session setup. But in case of **send-ccri traffic-start** the CLI causes the session setup to complete without OCS interaction. For more information on **rulebase-list** command, please see the *ACS Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Usage Guidelines Use this command to configure when to send CCR-Initial for the subscriber session.

Example

The following command configures to send CCR-I on traffic detection and not on context creation:

```
diameter send-ccri traffic-start
```

diameter service-context-id

This command configures the value to be sent in the Service-Context-Id AVP, which identifies the context in which DCCA is used.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

diameter service-context-id *service_context_id*
default diameter service-context-id

default

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

service_context_id

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

Usage Guidelines

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

Example

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

```
diameter service-context-id version@customer.com
```

diameter session failover

This command enables or disables Diameter Credit Control Session Failover. When enabled, the secondary peer is used in the event the main peer is unreachable.

Product

GGSN

HA

IPSG

PDSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

[default | no] diameter session failover

default

Configures this command with the default setting.

Default: Depends on the **failure-handling** configuration

no

If the primary server is not reachable, failover is not triggered and the session is torn down. No failover action is taken.

Usage Guidelines

Use this command to enable/disable Diameter Credit Control Session Failover.

The failure-handling, on page 775 configuration comes into effect only if **diameter session failover** is present in the configuration. The failover can be overridden by the server in the response message, and it takes precedence.

Example

The following command enables Diameter Credit Control Session Failover:

```
diameter session failover
```

diameter suppress-avp

This command specifies to suppress the AVPs like the MVNO-subclass-id and MVNO-Reseller-Id AVPs.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
diameter suppress-avp reseller-id subclass-id
[no | default] diameter suppress-avp reseller-id subclass-id
```

no

Disables AVP suppression. Whenever PCRF sends the MVNO-subclassid and MVNO-Reseller-id AVPs in the Gx interface, the same is sent in the Gy message.

default

Sets the default configuration. AVPs are not suppressed by default. Whenever PCRF sends the MVNO-subclassid and MVNO-Reseller-id AVPs in the Gx interface, the same is sent in the Gy message.

suppress-avp

Suppresses both MVNO-subclassid and MVNO-Reseller-id AVPs.

reseller-id

Supresses the MVNO-Reseller-Id AVP.

subclass-id

Supresses the MVNO-Sub-Class-Id AVP.

Usage Guidelines

Use this command to suppress the AVPs like the MVNO-subclass-id and MVNO-Reseller-Id AVPs.

Example

The following command specifies to request quota on receiving a dynamic rule with Online AVP enabled:

```
diameter suppress-avp reseller-id subclass-id
```

diameter suppress-ccru zero-gsu-with-validity-timer

This command is used to suppress CCR-U quota with validity timer running.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
diameter suppress-ccru zero-gsu-with-validity-timer
[ no ] diameter suppress-ccru
```

[no]

It specifies that if previously configured, it disables the CCR-U suppression **zero-gsu-with-validity-timer** configuration.

suppress-ccru

P-GW suppresses sending CCR-U message for Quota.

zero-gsu-with-validity-timer

P-GW suppresses sending CCR-U for Quota for No GSU when the validity timer is running.

Example

The following command suppresses CCR-U quota with the validity timer running:

```
diameter suppress-ccru zero-gsu-with-validity-timer
```

diameter update-dictionary-avps

This command enables dictionary control of the AVPs that need to be added based on the version of the specification with which the Online Charging System (OCS) is compliant. This command is applicable to all products that use the dcca-custom8 dictionary for Gy interface implementation.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
diameter update-dictionary-avps { 3gpp-rel8 | 3gpp-rel9 | 3gpp-rel10 |
3gpp-rel11| 3gpp-rel13 }
[ default | no ] diameter update-dictionary-avps
```

default | no

Configures this command with the default setting.

Default: Compliant with the oldest release (Rel. 7) and send only Rel. 7 AVPs

3gpp-rel8

Select the 3GPP Rel. 8 AVPs for encoding.

3gpp-rel9

Selects the 3GPP Rel. 9 AVPs for encoding.

3gpp-rel10

Select the 3GPP Rel. 10 AVPs for encoding.

3gpp-rel11

Select the 3GPP Rel. 11 AVPs for encoding.

3gpp-rel13

Select the 3GPP Rel. 13 AVPs for encoding.

Usage Guidelines



Important This command is applicable ONLY to the dcca-custom8 dictionary. If, for any dictionary other than dcca-custom8, this command is configured with a value other than the default, configuration errors will be indicated in the output of the **show configuration errors section active-charging** command.

Use this command to encode the AVPs in the dictionary based on the release version of the specification to which the OCS is compliant with.

Example

The following command enables encoding of AVPs in the dictionary based on 3GPP Rel. 9:

```
diameter update-dictionary-avps 3gpp-rel9
```

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-based-session

This command configures the parameters for event-based Gy session.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
[ no ] event-based-session trigger type { location-any | mcc | mnc |
timezone } +
default event-based-session trigger type
```

default

Configures this command with the default setting.

Default: No triggers.

no

Removes the previously configured trigger type.

location-any

Sets the trigger based on change in user location.

mcc

Sets the trigger based on change in Mobile Country Code (MCC) of the serving node (for e.g. SGSN, S-GW).

mnc

Sets the trigger based on change in Mobile Network Code (MNC) of the serving node (for e.g. SGSN, S-GW).

timezone

Sets the trigger based on change in the timezone of UE.

+

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

Usage Guidelines

Use this command to enable the credit control reauthorization triggers for event-based-session in the credit-control group.

Example

The following command selects a credit control trigger as **mcc**:

```
event-based-session trigger type mcc
```

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.

failure-handling

This command configures Diameter Credit Control Failure Handling (CCFH) behavior in the event of communication failure with the prepaid server or on reception of specific error codes from prepaid server.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
failure-handling { initial-request | terminate-request | update-request
} { continue [ go-offline-after-tx-expiry | retry-after-tx-expiry ] |
retry-and-terminate [ retry-after-tx-expiry ] | terminate }
default failure-handling [ initial-request | terminate-request |
update-request ]
```

default failure-handling [initial-request | terminate-request | update-request]

Configures the default CCFH setting.

initial-request: The default setting is **terminate**.

update-request: The default setting is **retry-and-terminate**.

terminate-request: The default setting is **retry-and-terminate**.

initial-request

Specifies the message type as CCR-Initial.

terminate-request

Specifies the message type as CCR-Terminate.

update-request

Specifies the message type as CCR-Update.

continue

Specifies the CCFH setting as continue. The online session is converted into an offline session. The associated PDP Context is established (new sessions) or not released (ongoing sessions).

retry-and-terminate

Specifies the CCFH setting as retry-and-terminate. The user session will continue for the duration of one retry attempt with the prepaid server. If there is no response from both primary and secondary servers, the session is torn down.

terminate

Specifies the CCFH setting as terminate. All type of sessions (initial or update) are terminated in case of failure.

go-offline-after-tx-expiry

Starts offline charging after Tx expiry.

retry-after-tx-expiry

Retries after Tx expiry. Enables secondary-host, if up, to take over after Tx expiry.

Usage Guidelines

Use this command to select the CCFH behavior. The specified behavior is used for sessions when no behavior is specified by the prepaid server. By default, the CCFH is taken care at response-timeout except for terminate setting.

If the Credit-Control-Failure-Handling AVP is received from the server, the received setting will be applied to all the message types.

The following table indicates the CCFH behavior for the combination of different CCFH settings, and the corresponding CLI commands.

CCFH Setting	CLI Command	Behavior at Tx	Behavior at RT	Secondary is Up	Secondary is Down
Initial-request Message Type					
Continue	**initial-request continue**	N/A	Continue	Secondary takes over after RT	Offline after another RT. No more quota requests are performed for any rating group within the session after DCCA failure (even if connectivity to DCCA is restored)
	initial-request continue go-offline-after-tx-expiry	Offline	N/A	Offline at Tx	Offline at Tx
	initial-request continue retry-after-tx-expiry	Continue	N/A	Secondary takes over after Tx	Offline after another Tx
Retry-and-terminate	**initial-request retry-and-terminate**	N/A	Retry	Secondary takes over after RT	Terminate after another RT

CCFH Setting	CLI Command	Behavior at Tx	Behavior at RT	Secondary is Up	Secondary is Down
	initial-request retry-and-terminate retry-after-tx-expiry	Retry	N/A	Secondary takes over after Tx	Terminate after another Tx
Terminate	**initial-request terminate**	Terminate	N/A	Terminate after Tx	Terminate after Tx
Update-request Message Type					
Continue	**update-request continue**	N/A	Continue	Secondary takes over after RT	Offline after another RT
	update-request continue go-offline-after-tx-expiry	Offline	N/A	Offline at Tx	Offline at Tx
	update-request continue retry-after-tx-expiry	Continue	N/A	Secondary takes over after Tx	Offline after another Tx
Retry-and-terminate	**update-request retry-and-terminate**	N/A	Retry	Secondary takes over after RT	Sends CCR-T after another RT
	update-request retry-and-terminate retry-after-tx-expiry	Retry	N/A	Secondary takes over after Tx	Sends CCR-T after another Tx
Terminate	**update-request terminate**	Terminate	N/A	Sends CCR-T after Tx	Sends CCR-T after Tx
Terminate-request Message Type					
Continue	**terminate-request continue**	N/A	Retry	CCR-T is sent to secondary after RT	Terminate after another RT
	terminate-request continue go-offline-after-tx-expiry	Retry	N/A	CCR-T is sent to secondary after Tx	Terminate after another Tx
	terminate-request continue retry-after-tx-expiry	Retry	N/A	CCR-T is sent to secondary after Tx	Terminate after another Tx
Retry-and-terminate	**terminate-request retry-and-terminate**	N/A	Retry	CCR-T is sent to secondary after RT	Terminate after another RT
	terminate-request retry-and-terminate retry-after-tx-expiry	Retry	N/A	CCR-T is sent to secondary after Tx	Terminate after another Tx
Terminate	**terminate-request terminate**	Terminate	N/A	Terminate after Tx	Terminate after Tx

Example

The following command sets the Credit Control Failure Handling behavior for initial request message type to **retry-and-terminate**:

```
failure-handling initial-request retry-and-terminate
```

gy-rf-trigger-type

This command enables the Gy event triggers for configuration of matching Rf ACR containers.

Product

GGSN

HA

IPSG

PDSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
gy-rf-trigger-type { final | forced-reauthorization | holding-time |
quota-exhausted | rating-condition-change | threshold | validity-time }
{ default | no } gy-rf-trigger-type
```

default | no

The "default/no" variant of this command will not enable any of the Gy event-triggers which means the containers would not be closed for any of the event-triggers.

final

Enables Gy trigger "final" for Rf

forced-reauthorization

Enables Gy trigger "forced-reauthorization" for Rf.

holding-time

Enables Gy trigger "qht" for Rf. The trigger "qht" indicates Quota Holding Time.

quota-exhausted

Enables Gy trigger "quota-exhausted" for Rf.

rating-condition-change

Enables Gy trigger "rating-condition-change" for Rf.

threshold

Enables Gy trigger "threshold" for Rf.

validity-time

Enables Gy trigger "validity-time" for Rf.

Usage Guidelines

Use this command to enable the Gy reporting reasons/event triggers.

For all the Gy event triggers a container will be cached at Rf and will be sent based on other events at Rf (for example, max-charging-change-condition, RAT-Change, etc).



Important The CLI command "gy-rf-trigger-type" is currently applicable only for CCR-U and not CCR-T.

For example, when the CLI for QUOTA_EXHAUSTED event trigger is configured under credit-control group configuration, if there is quota_exhausted event then the container should be cached with appropriate change-condition value and ACR-I would be sent out based on other Rf event triggers. Similar behavior is applicable to other event triggers when configured.

Example

The following command specifies the validity-time event trigger to be enabled.

```
gy-rf-trigger-type validity-time
```

imsi-imeisv-encode-format

This command configures the encoding format of IMSI/IMEISV in the User-Equipment-Info, 3GPP-IMSI and 3GPP-IMEISV AVPs.

Product

GGSN

HA

IPSG

PDSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

[default | no] imsi-imeisv-encode-format { ascii | tbcd }

ascii

Sends IMSI/IMEISV as an octet string in ASCII encoded format. By default, the IMSI/IMEISV will be encoded in ASCII format.

tbcd

Sends IMSI/IMEISV as an octet string in Telephony Binary Coded Decimal (TBCD) format, i.e. the nibbles in an octet are inter-changed.

Usage Guidelines

Use this command to configure the encoding format of IMSI/IMEISV in User-Equipment-Info, 3GPP-IMSI and 3GPP-IMEISV AVPs.

Example

The following command specifies the encoding format of IMSI/IMEISV as ASCII:

imsi-imeisv-encode-format ascii

mode

This command configures the Prepaid Credit Control mode to RADIUS or Diameter.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

mode { diameter | radius }
default mode

default

Configures the default prepaid credit control mode.

Default: **diameter**

diameter

Enables Diameter Credit Control Application (DCCA) for prepaid charging.

Important After you configure this keyword, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

radius

Enables RADIUS Credit Control for prepaid charging.

Important After you configure this keyword, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Usage Guidelines

Use this command to configure the prepaid charging application mode to Diameter or RADIUS credit control.

Important After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Example

The following command specifies to use RADIUS prepaid credit control application:

```
mode radius
```

offline-session re-enable

This command is configured to re-enable the offline Gy session after failure.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
[ no ] offline-session re-enable
```

no

Disables the feature. This is the default behavior.

The default configuration is **no offline-session re-enable**.

Usage Guidelines Use this command to re-enable the Offline Gy session back to Online charging, based on indication from PCRF. When **offline-session re-enable** is configured and the PCRF installs/modifies a rule with "Online" AVP value set to 1, then the Offline DCCA will be marked Online.

pending-traffic-treatment

This command controls the pass/drop treatment of traffic while waiting for definitive credit information from the server.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
pending-traffic-treatment { { { forced-reauth | trigger | validity-expired
 } drop | pass } | { noquota { buffer | drop | limited-pass volume | pass
 } } | { quota-exhausted { buffer | drop | pass } } }
default pending-traffic-treatment { forced-reauth | noquota |
quota-exhausted | trigger | validity-expired }
```

default

Configures this command with the default setting.

Default: **drop**

forced-reauth

Sets the Diameter credit control pending traffic treatment to forced reauthorization.

trigger

Sets the Diameter credit control pending traffic treatment to trigger.

validity-expired

Sets the Diameter credit control pending traffic treatment to validity expired.

noquota

Sets the Diameter credit control pending traffic treatment to no quota.

quota-exhausted

Sets the Diameter credit control pending traffic treatment to quota exhausted.

buffer

Specifies to tentatively count/time traffic, and then buffer traffic pending arrival of quota. Buffered traffic will be forwarded and fully charged against the quota when the quota is eventually obtained and the traffic is passed.

drop

Drops any traffic when there is no quota present.

limited-pass *volume*

Enables limited access for subscribers when the OCS is unreachable.

volume specifies the Default Quota size (in bytes) and must be an integer from 1 through 4294967295.

This feature allows the subscriber to use the network when the OCS response is slow. This configuration enables to set a Default Quota size from which the subscriber can consume quota until response from the OCS arrives. The traffic consumed by the subscriber from the Default Quota at the beginning of the session is reported and counted against the quota assigned from the OCS.



Important Default Quota is used only for **noquota** case (Rating Group (RG) seeking quota for the first time) and not for **quota-exhauste**d. Default Quota is not used for subsequent credit requests.

If the Default Quota is NOT exhausted before the OCS responds with quota, traffic is allowed to pass. Initial Default Quota usage is counted against initial quota allocated. If quota allocated is less than the actual usage, the actual usage and request additional quota are reported. If no additional quota is available, the traffic is denied.

If the Default Quota is NOT exhausted before the OCS responds with denial of quota, traffic is blocked after the OCS response. The gateway will report usage on Default Quota even in for CCR-U (FINAL) or CCR-T until the OCS responds.

If the Default Quota is exhausted before the OCS responds, the session is dropped.

The default pending-traffic-treatment for **noquota** is drop. The **default pending-traffic-treatment noquota** command removes any Default Quota limit configured.

pass

Passes all traffic more or less regardless of quota state.

Usage Guidelines

Use this command to set the Diameter credit control pending traffic treatment while waiting for definitive credit information from the server.

This CLI command is different than the **failure-handling** command, which specifies behavior in the case of an actual timeout or error, as opposed to the behavior while waiting. See also the **buffering-limit** command in the Active Charging Service Configuration Mode.

Example

The following command sets the Diameter credit control pending traffic treatment to drop any traffic when there is no quota present:

```
pending-traffic-treatment noquota drop
```

quota

This command sets various time-based quotas in the prepaid credit control service.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

quota { consumption-time *consumption_time* **| holding-time** *holding_time* **| validity-time** *validity_time* **| retry-time** *retry_time* **}**
{ default | no } quota { consumption-time | holding-time | validity-time | retry-time }

consumption-time *consumption_time*

Defines the value to use for the Quota Consumption Time (QCT) in seconds. QCT can be used when time-based quotas are in effect. *consumption_time* must be an integer from 1 through 4000000000.

holding-time *holding_time*

Specifies the Quota Holding Time (QHT) in seconds. The value must be an integer from 1 through 4000000000.

retry-time *retry_time*

Specifies the retry time in seconds for the quota request. The value must be an integer from 0 through 86400. To disable, set to 0. Default: 60

validity-time *validity_time*

Specifies the validity lifetime of the quota, in seconds. The value must be an integer from 1 through 4000000.

Usage Guidelines

Use this command to set the prepaid credit control quotas.

Example

The following command sets the prepaid credit control request holding time to *30000* seconds:

```
quota holding-time 30000
```

quota request-trigger

This command configures the action on the packet that triggers the credit control application to request quota.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
quota request-trigger { exclude-packet-causing-trigger |
include-packet-causing-trigger }
{ default | no } quota request-trigger
default quota request-trigger
```

default

Configures this command with the default setting. Default: **include-packet-causing-trigger**

no

Same as the **default quota request-trigger** command.

Important In 10.0 and later releases, this keyword is deprecated.

exclude-packet-causing-trigger

Excludes the packet causing threshold limit violation trigger.

include-packet-causing-trigger

Includes the packet causing the threshold limit violation trigger.

Usage Guidelines

Use this command to configure action on the packet that triggers the credit control application to request quota, whether the packet should be excluded/included in the utilization information within the quota request.

Example

The following command sets the system to exclude the packets causing threshold limit triggers from accounting of prepaid credit of a subscriber:

```
quota request-trigger exclude-packet-causing-trigger
```

quota time-threshold

This command configures the time threshold limit for subscriber quota in the prepaid credit control service.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

quota time-threshold { *abs_time_value* **| percent** *percent_value* **}**
{ default | no } quota time-threshold

default

Configures this command with the default setting.

Default: Disabled

no

Disables time threshold for prepaid credit control quota.

abs_time_value

Specifies the absolute threshold time (in seconds) for configured time quota in prepaid credit control charging. *abs_time_value* must be an integer from 1 through 86400. To disable this assign 0. Default: 0 (Disabled)

percent_value

Specifies the time threshold value as a percentage of the configured time quota in DCCA. *percent_value* must be an integer from 1 through 100.

Usage Guidelines

Use this command to set the time threshold for prepaid credit control quotas.

Example

The following command sets the prepaid credit control time threshold to *400* seconds:

```
quota time-threshold 400
```

quota units-threshold

This command sets the unit threshold limit for subscriber quota in the prepaid credit control service.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

quota unit-threshold { *abs_unit_value* | percent *percent_value* }
{ default | no } quota units-threshold

default

Configures this command with the default setting.

Default: Disabled

no

Disables unit threshold for DCCA quota.

abs_unit_value

Specifies the absolute threshold value (in units) for the configured units quota in prepaid credit control application. *abs_unit_value* must be an integer from 1 through 4000000000. To disable this assign 0. Default: 0 (Disabled)

percent_value

Specifies the time threshold value as a percentage of the configured units quota in DCCA. *percent_value* must be an integer from 1 through 100.

Usage Guidelines

Use this command to set the units threshold for prepaid credit control quotas.

Example

The following command sets the prepaid credit control time threshold to *160400* units:

```
quota units-threshold 160400
```

quota volume-threshold

This command sets the volume threshold limit for subscriber quota in the prepaid credit control service.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

quota volume-threshold { *abs_vol_value* | percent *percent_value* }
{ default | no } quota volume-threshold

default

Configures this command with the default setting.

Default: Disabled

no

Disables volume threshold for prepaid credit control quota.

abs_vol_value

Specifies the absolute threshold volume (in bytes) to the configured volume quota in prepaid credit control. *abs_vol_value* must be an integer from 1 through 4000000000. To disable this assign 0. Default: 0 (Disabled)

If configured, the Credit Control client will seek re-authorization from the server for the quota when the quota contents fall below the specified threshold.

percent *percent_value*

Specifies the volume threshold value as a percentage of the configured volume quota in prepaid credit control. *percent_value* must be an integer from 1 through 100.

Usage Guidelines

Use this command to set the volume threshold for prepaid credit control quotas.

Example

The following command sets the prepaid credit control volume threshold to *160400* bytes:

```
quota volume-threshold 160400
```

radius usage-reporting-algorithm

This command configures the usage reporting algorithm for RADIUS prepaid using the Diameter Credit-Control Application (DCCA).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

radius usage-reporting-algorithm { cumulative | relative }
default radius usage-reporting-algorithm

default

Configures this command with the default setting.

Default: **cumulative**

cumulative

Reports the total accumulated usage of quota in every accounting interim.

relative

Reports the quota usage per accounting interim (since the previous usage report).

Usage Guidelines

Use this command to configure the usage reporting algorithm for RADIUS prepaid using DCCA.

Example

The following command configures the usage reporting algorithm for RADIUS prepaid using DCCA to *relative*:

radius usage-reporting-algorithm relative

redirect-indicator-received

This command configures the action on buffered packets when a redirect-indicator is received from the RADIUS server.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

redirect-indicator-received { discard-buffered-packet |
reprocess-buffered-packet }
{ default | no } redirect-indicator-received

default

Configures this command with the default setting. Default: **discard-buffered-packet**

no

Disables the redirect-indicator-received configuration.

discard-buffered-packet

Discards the buffered packet.

reprocess-buffered-packet

Redirects the buffered packet on receiving a redirect-indicator from the RADIUS server.

Usage Guidelines

Use this command to configure the action taken on buffered packet when redirect-indicator is received.

Diameter can return a redirect URL but not a redirect indicator, however RADIUS can return a redirect indicator. In this situation, any subsequent subscriber traffic would match ruledefs configured with cca redirect-indicator, and charging actions that have flow action redirect-url should be configured. However, some handsets do not retransmit, so there will be no subsequent packets. On configuring reprocess-buffered-packet, the ruledefs are reexamined to find a new charging action, which may have flow action redirect-url configured.

Example

The following command configures the action taken on buffered packet when redirect-indicator is received to reprocess-buffered-packet:

```
redirect-indicator-received reprocess-buffered-packet
```

redirect-require-user-agent

This command conditionally verifies the presence of user-agents in the HTTP header, based on which HTTP URL redirection will be applied.

Product

GGSN

HA

IPSG

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

[no] redirect-require-user-agent

no

Disables the "user-agent" check in the HTTP header.

Usage Guidelines

Use this command to conditionally verify the presence of configured user-agents in the HTTP header. The user agent is configured using the **redirect user-agent** command in the ACS Configuration Mode. The user agent could be, for example, Mozilla, Opera, Google Chrome, etc.

The default configuration is to enable the "user-agent" check, and compare it with the configured list of supported user-agents. The packet will be redirected only when the user-agent is matched with one of the configured user-agents.

If **no redirect-require-user-agent** is configured, the user-agent check is disabled. The packets will be redirected even if it does not contain a "user-agent" information in the HTTP header.

servers-unreachable

This command configures whether to continue or terminate calls when Diameter server or the OCS becomes unreachable.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

In 12.1 and earlier releases:

servers-unreachable { initial-request { continue | terminate [after-timer-expiry *timeout_period* **] } | update-request { continue | terminate [after-quota-expiry | after-timer-expiry** *timeout_period* **] } }**
no servers-unreachable { initial-request | update-request }

In 12.2 and later releases:

servers-unreachable { behavior-triggers { initial-request | update-request } result-code { any-error | *result-code* **[to** *end-result-code* **] } | transport-failure [response-timeout | tx-expiry] | initial-request { continue [{ [after-interim-time** *timeout_period* **] [after-interim-volume** *quota_value* **] } server-retries** *retry_count* **] | terminate [{ [after-interim-time** *timeout_period* **] [after-interim-volume** *quota_value* **] } server-retries** *retry_count* **| after-timer-expiry** *timeout_period* **] } | update-request { continue [{ [after-interim-time** *timeout_period* **] [**

after-interim-volume *quota_value* **] } server-retries** *retry_count* **] | terminate [{ [after-interim-time** *timeout_period* **] [after-interim-volume** *quota_value* **] } server-retries** *retry_count* **] | after-quota-expiry | after-timer-expiry** *timeout_period* **] } }**
no servers-unreachable { initial-request | update-request }
default servers-unreachable behavior-triggers { initial-request | update-request }

no

Deletes the current servers-unreachable configuration.

In 15.0 and later releases, to remove the error result code configuration, the **no** command syntax is **no servers-unreachable behavior-triggers { initial-request | update-request } result-code { any-error |** *result-code* **[to** *end-result-code* **] }**.

To maintain backward compatibility i.e. in case of **no servers unreachable behavior triggers** configured for error result codes, the default hard coded values are applicable.

behavior-triggers { initial-request | update-request } { result-code { any-error | *result-code* [to *end-result-code*] } | transport-failure [response-timeout | tx-expiry] }

This keyword is used to determine when to apply server-unreachable action. This supports three configurable options to apply server-unreachable action either at transport failure, Tx expiry or at response timeout. Out of these three options, the transport failure is the default option.

- **initial-request**: Specifies the behavior when Diameter server(s)/OCS become unreachable during initial session establishment.
- **update-request**: Specifies the behavior when Diameter server(s)/OCS become unreachable during mid-session.
- **result-code { any-error |** *result-code* **[to** *end-result-code* **] }**: Specifies to configure any Diameter error result code or a range of result codes to trigger entering server unreachable mode.

  result-code must be an integer ranging from 3000 to 5999.
- **transport-failure [response-timeout | tx-expiry]**: This keyword specifies to trigger the behavior either at transport failure or response timeout OR at Transport failure or Tx expiry.

initial-request { continue | terminate [after-timer-expiry *timeout_period*] }

Important This section applies only to 12.1 and earlier releases.

Specifies behavior when Diameter server(s)/OCS become unreachable during initial session establishment.

- **continue**: Specifies to continue call if Diameter server(s) becomes unreachable.
- **terminate**: Specifies to terminate call if Diameter server(s) becomes unreachable.

  after-timer-expiry *timeout_period*: On detecting transport failure, this keyword variable specifies the time limit for which the subscriber session will remain in offline state before the call is terminated.

timeout_period specifies the timeout period, in seconds, and must be an integer from 1 through 4294967295.

initial-request { continue [{ [after-interim-time *timeout_period*] [after-interim-volume *quota_value*] } server-retries *retry_count*] | terminate [{ [after-interim-time *timeout_period*] [after-interim-volume *quota_value*] } server-retries *retry_count*] | after-timer-expiry *timeout_period* }



Important This section applies only to 12.2 and later releases.

Specifies behavior when Diameter server(s)/OCS become unreachable during initial session establishment.

- **continue**: Specifies to continue call if Diameter server(s) becomes unreachable.
- **terminate**: Specifies to terminate call if Diameter server(s) becomes unreachable.
  - **after-interim-time** *timeout_period*: Specifies to continue or terminate call after the interim timeout period expires.

    timeout_period specifies the timeout period, in seconds, and must be an integer from 1 through 4294967295.
  - **after-interim-volume** *quota_value*: Specifies to continue or terminate call on exhaustion of the assigned quota.

    quota_value specifies the volume-based quota value, in bytes, and must be an integer from 1 through 4294967295.

    The **after-interim-volume** and **after-interim-time** can be configured in one of the following ways:
    - **after-interim-volume** *quota_value* **server-retries** *retry_count*
    - **after-interim-time** *timeout_period* **server-retries** *retry_count*
    - **after-interim-volume** *quota_value* **after-interim-time** *timeout_period* **server-retries** *retry_count*
  - **after-timer-expiry** *timeout_period*: On detecting transport failure, this keyword variable specifies the time limit for which the subscriber session will remain in offline state before the call is terminated.

    timeout_period specifies the timeout period, in seconds, and must be an integer from 1 through 4294967295.
  - **server-retries** *retry_count*: Specifies the number of retries that should happen to OCS before allowing the session to terminate/offline.

    retry_count specifies the retries to OCS, and must be an integer from 0 through 65535. If the value 0 is defined for this keyword, the retry to OCS will not happen instead the configured action will be immediately applied.

update-request { continue | terminate [after-quota-expiry | after-timer-expiry *timeout_period*] }



Important This section applies only to 12.1 and earlier releases.

Specifies behavior when Diameter server(s)/OCS become unreachable during mid session.

- **continue**: Specifies to continue call if Diameter server(s) becomes unreachable.
- **terminate**: Specifies to terminate call if Diameter server(s) becomes unreachable.
  - **after-quota-expiry**: Specifies to terminate call on exhaustion of all available quota.
  - **after-timer-expiry** *timeout_period*: On detecting transport failure, this keyword variable specifies the time limit for which the subscriber session will remain in offline state before the call is terminated.

    timeout_period specifies the timeout period, in seconds, and must be an integer from 1 through 4294967295.

update-request { continue [{ [after-interim-time *timeout_period*] [after-interim-volume *quota_value*] } server-retries *retry_count*] | terminate [{ [after-interim-time *timeout_period*] [after-interim-volume *quota_value*] } server-retries *retry_count*] | after-quota-expiry | after-timer-expiry *timeout_period*] }



Important This section applies only to 12.2 and later releases.

Specifies behavior when Diameter server(s)/OCS become unreachable during mid session.

- **continue**: Specifies to continue call if Diameter server(s) becomes unreachable.
- **terminate**: Specifies to terminate call if Diameter server(s) becomes unreachable.
  - **after-interim-time** *timeout_period*: Specifies to continue or terminate call after the interim timeout period expires.

    timeout_period specifies the timeout period, in seconds, and must be an integer from 1 through 4294967295.
  - **after-interim-volume** *quota_value*: Specifies to continue or terminate call on exhaustion of the assigned quota.

    quota_value specifies the volume-based quota value, in bytes, and must be an integer from 1 through 4294967295.

    The **after-interim-volume** and **after-interim-time** can be configured in one of the following ways:
    - **after-interim-volume** *quota_value* **server-retries** *retry_count*
    - **after-interim-time** *timeout_period* **server-retries** *retry_count*
    - **after-interim-volume** *quota_value* **after-interim-time** *timeout_period* **server-retries** *retry_count*
  - **after-quota-expiry**: Specifies to terminate call on exhaustion of all available quota.

- **after-timer-expiry** *timeout_period*: On detecting transport failure, this keyword variable specifies the time limit for which the subscriber session will remain in offline state before the call is terminated.

  timeout_period specifies the timeout period, in seconds, and must be an integer from 1 through 4294967295.

- **server-retries** *retry_count*: Specifies the number of retries that should happen to OCS before allowing the session to terminate/offline.

  retry_count specifies the retries to OCS, and must be an integer from 0 through 65535. If the value 0 is defined for this keyword, the retry to OCS will not happen instead the configured action will be immediately applied.

Usage Guidelines

Use this command to configure whether to continue/terminate calls when Diameter server(s)/OCS are unreachable. This command can be used to verify the functionality of the configurable action if the OCS becomes unreachable.

In 12.1 and earlier releases, the OCS is considered down/unreachable when all transport/TCP connections are down for that OCS.

In 12.2 and later releases, the OCS is declared unreachable when all transport connections are down OR message timeouts happen (for example, a Tx expiry or response timeout, for all available OCS servers) owing to slow response from the OCS (may be due to network congestion or other network related issues).

The following set of actions are performed if the servers become unreachable:

- During initial session establishment:
  - Block traffic: Terminate the session.
  - Continue call: Continue by making the session offline.
  - Pass traffic until timer expiration post which terminates the call: Session would be offline while the timer is running.
  - Pass traffic until interim time expiration post which continues or terminates the call.
  - Pass traffic until interim volume expiration post which continues or terminates the call.
- During mid session:
  - Block traffic: Terminate the session.
  - Continue call: Continue by making the session offline.
  - Run out of session quota post which terminates the call.
  - Pass traffic until timer expiration post which terminates the call: Session would be offline while the timer is running.
  - Pass traffic until interim time expiration post which continues or terminates the call.
  - Pass traffic until interim volume expiration post which continues or terminates the call.

This command works on the same lines as the **failure-handling** command, which is very generic for each of the xxx-requests and applies for Credit-Control-Failure-Handling (CCFH) during:.

1. Application-level (Tx) timeout: Here message is sent out but server does not respond for the configured "pending-timeout" so application does CCFH actions.
2. Diabase-level request timeout: Here message is sent out but server does not respond and Diabase detects timeout of the application message and application does CCFH actions.
3. TCP connection error: Here message is NOT sent out due to no TCP connection and application does CCFH actions.

The **servers-unreachable** CLI command is specifically for TCP connection error. In the event of TCP connection failure, the **failure-handling** and/or **servers-unreachable** commands can be used. This way, the operator has the flexibility to configure CCFH independent of OCS-unreachable feature, that is having two different failure handlings for same request types.



Important Please note that the flexibility to configure CCFH independent of OCS-unreachable feature is applicable only to 12.1 and earlier releases. In 12.2 and later releases, if configured, the **servers-unreachable** takes precedence over the **failure-handling** command.

This command can also be used to control the triggering of behavior based on transport failure, response message timeouts or Tx expiry when OCS becomes unreachable. The OCS could be unreachable due to no TCP connection and the message timeout could be due to network congestion or any other network related issues.

The following are the possible and permissible configurations with respect to behavior triggering:

- **servers-unreachable behavior-triggers { initial-request | update-request } transport-failure**
- **servers-unreachable behavior-triggers { initial-request | update-request } transport-failure response-timeout**
- **servers-unreachable behavior-triggers { initial-request | update-request } transport-failure tx-expiry**

Of these configurations, the first one is considered to be the default configuration and it will take care of backward compatibility with 12.0 implementation.

If the server returns the CC-Failure-Handling AVP, it would apply for transport-failure/response-timeout/tx-expiry when the CLI command **servers-unreachable** is not configured. If the **servers-unreachable** is configured for a set of behavior-triggers, then servers-unreachable configuration will be applied for them. For those behavior-triggers for which servers-unreachable is not configured, the CC-Failure-Handling value provided by the server will be applied.

By default, Result-Code such as 3002 (Unable-To-Deliver), 3004 (Too-Busy) and 3005 (Loop-Detected) falls under delivery failure category and will be treated similar to response-timeout configuration.

Example

The following command configures the duration of *1111* seconds, for the subscriber session to be in offline state, after which the initial request calls will be terminated.

```
servers-unreachable initial-request terminate after-timer-expiry 1111
```

subscription-id service-type

This command enables required Subscription-Ids for various service types.

Product

GGSN

HA

IPSG

PDSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

subscription-id service-type { closedrp | ggsn | ha | ipsg | l2tplns | mipv6ha | pdsn | pgw } { e164 | imsi | nai }
[no] subscription-id service-type { closedrp | ggsn | ha | ipsg | l2tplns | mipv6ha | pdsn | pgw }

default

Configures the default timestamp-rounding setting.

Default: **floor**

closedrp | ggsn | ha | ipsg | l2tplns | mipv6ha | pdsn | pgw { e164 | imsi | nai }

Includes the Subscription-Id for the chosen service type. For example, if ipsg is configured as the keyword option, then the subscription-id is included for the IPSG service.

The following subscription-Id types are available:

- e164 - Include E164 information in the Subscription-Id AVP
- imsi - Include IMSI information in the Subscription-Id AVP
- nai - Include NAI information in the Subscription-Id AVP

Usage Guidelines

Currently, Subscription-Id AVP is encoded in the Gy CCRs based on dictionary and service-type checks. With the new CLI command, customers will have the provision of enabling required Subscription-Id types for various services.

Each service can have a maximum of three Subscription-Id types (e164, imsi & nai) that can be configured through this CLI command. The DCCA specific changes are made in such a way that, if the CLI command is configured for any particular service, then the CLI takes precedence. Else, it falls back to default (hard-coded) values configured for that service.

The advantage of this CLI command is that any further dictionary additions in DCCA can be minimized.

Important The CLI configured for any of the service will contain the most recent Subscription-Id-types configured for that service (i.e. overrides the previous values).

For an instance, if a customer wants IMSI value to be encoded in Gy CCRs (along with E164) for MIPv6HA service, then this CLI command **subscription-id service-type mipv6ha e164 imsi** should be configured in the Credit Control Configuration mode.

If only imsi is configured through the CLI, then Gy CCRs will only have imsi value.

Example

The following command configures imsi type for ggsn service:

```
subscription-id service-type ggsn imsi
```

timestamp-rounding

This command configures how to convert exact time into the units that are used in quotas.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
timestamp-rounding { ceiling | floor | roundoff }
default timestamp-rounding
```

default

Configures the default timestamp-rounding setting.

Default: **floor**

timestamp-rounding ceiling

Round off to the smallest integer greater than the fraction.

If the fractional part of the seconds is greater than 0, add 1 to the number of seconds and discard the fraction.

timestamp-rounding floor

Discard the fractional part of the second.

timestamp-rounding roundoff

Set the fractional part of the seconds to the nearest integer value. If the fractional value is greater than or equal to 0.5, add 1 to the number of seconds and discard the fractional part of second.

Usage Guidelines

Use this command to configure how to convert exact time into the units that are used in quotas for CCA charging.

The specified rounding will be performed before system attempts any calculation. For example using round-off, if the start time is 1.4, and the end time is 1.6, then the calculated duration will be 1 (i.e., 2 – 1 = 1).

Example

The following command sets the CCA timestamp to nearest integer value second (for example, 34:12.23 to 34:12.00):

```
timestamp-rounding roundoff
```

trigger type

This command enables/disables triggering a credit reauthorization when the named values in the subscriber session changes.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* > **credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
[ no ] trigger type { cellid | lac | mcc | mnc | qos | rat | serving-node
 | sgsn | timezone } +
default trigger type
```

default

Configures this command with the default setting.

Default: No triggers.

no

Removes the previously configured trigger type.

cellid

Sets the trigger based on change in cell identity or Service Area Code (SAC).

lac

Sets the trigger based on change in Location Area Code.

mcc

Sets the trigger based on change in Mobile Country Code (MCC).

mnc

Sets the trigger based on change in Mobile Network Code (MNC).

qos

Sets the trigger based on change in the Quality of Service (QoS).

rat

Sets the trigger based on change in the Radio Access Technology (RAT).

serving-node

Sets the trigger based on change in serving node. The serving node change causes the credit control client to ask for a re-authorization of the associated quota.

Typically used as an extension to sgsn trigger in P-GW (SAEGW), however, may also be used alone.

sgsn

Sets the trigger based on change in the IP address of SGSN.

timezone

Sets the trigger based on change in the timezone of UE.

+

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

Usage Guidelines

Use this command to set the credit control reauthorization trigger.

Example

The following command selects a credit control trigger as **lac**:

```
trigger type lac
```

usage-reporting

This command configures the ACS Credit Control usage reporting type.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > ACS Configuration > Credit Control Configuration

active-charging service *service_name* **> credit-control**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax Description

```
usage-reporting quotas-to-report based-on-grant {
report-only-granted-volume }
default usage-reporting quotas-to-report
```

default

Configures this command with the default setting.

Default: Disabled

usage-reporting quotas-to-report based-on-grant

Configures reporting usage only for granted quota.



Note When Gy server is unavailable, no grant (quota) is received. In this case, P-GW sends both CC-OCTET and CC-TIME AVPs in the usage report.

report-only-granted-volume

Suppresses the input and output octets. If the Granted-Service-Unit (GSU) AVP comes with CC-Total-Octets, then the device will send total, input and output octets in Used-Service-Unit (USU) AVP. If it comes with Total-Octets, the device will send only Total-Octets in USU.

Usage Guidelines

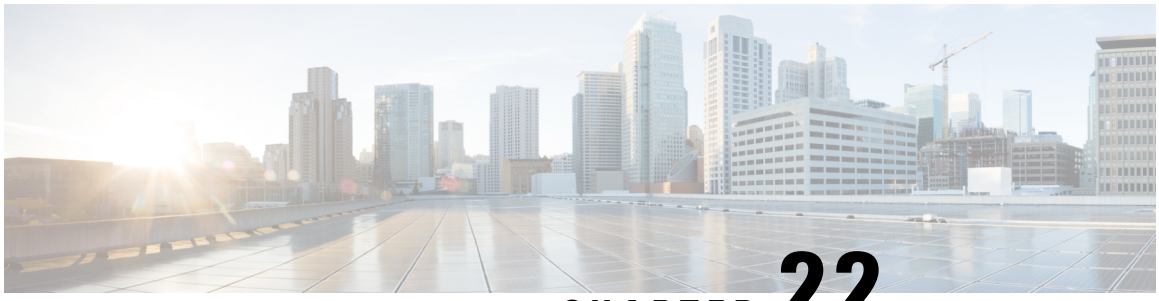
Use this command to configure reporting usage only for granted quota. On issuing this command, the Used-Service-Unit AVP will report quotas based on grant i.e, only the quotas present in the Granted-Service-Unit AVP.

With this command only the units for which the quota was granted by the DCCA server will be reported irrespective of the reporting reason.

Example

The following command configures to report usage based only on granted quota:

```
usage-reporting quotas-to-report based-on-grant
```



CHAPTER 22

Credit Control Service Configuration Mode Commands

The Credit Control Service Configuration Mode is used to create and manage Credit Control Service.

Command Modes

Exec > Global Configuration > Context Configuration > Credit Control Service Configuration

configure > context *context_name* **> credit-control-service** *service_name*

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

- diameter dictionary, on page 803
- diameter endpoint, on page 804
- end, on page 805
- exit, on page 805
- failure-handling, on page 805
- request timeout, on page 806

diameter dictionary

This command configures the Diameter dictionary to be used for this Credit Control Service instance.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Credit Control Service Configuration

configure > context *context_name* **> credit-control-service** *service_name*

Syntax Description

```
diameter dictionary { custom1 | standard }
default diameter dictionary
```

default

Configures the default setting.

dictionary { custom1 | standard }

Specifies the Diameter dictionary to be used.

custom1: Specifies the custom dictionary **custom1**.

standard: Specifies the standard dictionary.

Usage Guidelines Use this command to configure the Diameter dictionary to be used for this Credit Control Service instance.

Example

The following command configures the standard Diameter dictionary:

```
diameter dictionary standard
```

diameter endpoint

This command configures the Diameter Credit Control Interface Endpoint.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Credit Control Service Configuration

configure > context *context_name* **> credit-control-service** *service_name*

Syntax Description

```
diameter endpoint endpoint_name
{ default | no } diameter endpoint
```

default

Configures the default setting.

no

Removes the previous Diameter endpoint configuration.

endpoint_name

Specifies the Diameter endpoint name as an alpha and/or numeric string of 1 through 63 characters.

Usage Guidelines Use this command to configure the Diameter Credit Control Interface Endpoint.

Example

The following command configures the Diameter Credit Control Interface Endpoint named *test135*:

```
diameter endpoint test135
```

end

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.

failure-handling

This command configures the Diameter failure handling behavior.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Credit Control Service Configuration

configure > **context** *context_name* > **credit-control-service** *service_name*

Syntax Description

```
failure-handling { initial-request | terminate-request | update-request
} { diameter-result-code result_code [ to result_code ] | peer-unavailable |
request-timeout } action { continue | retry-and-continue |
retry-and-terminate | terminate }
{ default | no } failure-handling { initial-request | terminate-request
| update-request } { diameter-result-code result_code [ to result_code ] |
peer-unavailable | request-timeout }
```

default

Configures the default setting.

no

Removes the previous failure handling configuration.

initial-request | terminate-request | update-request

initial-request: Specifies failure handling for Initial Request.

terminate-request: Specifies failure handling for Terminate Request.

update-request: Specifies failure handling for Update Request.

diameter-result-code | peer-unavailable | request-timeout

diameter-result-code *result_code* **[to** *result_code* **]**: Specifies Diameter result code(s) for failure handling.

result_code must be an integer from 3000 through 9999.

to *result_code*: Specifies the range of Diameter result codes.

peer-unavailable: Specifies failure handling for peer being unavailable.

request-timeout: Specifies failure handling for request timeouts.

Default:???

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

Specifies the failure handling action.

continue: Continue the session without credit control.

retry-and-continue: Retry and, even if credit control is not available, continue.

retry-and-terminate: Retry and then terminate.

terminate: Terminate the session.

Default:???

Usage Guidelines

Use this command to configure the Diameter failure handling behavior.

Example

The following command configures initial request failure handling behavior for Diameter result codes *3001* to *4001* with terminate action:

```
failure-handling initial-request diameter-result-code 3001 to 4001 action
 terminate
```

request timeout

This command configures the timeout period for Diameter requests.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Credit Control Service Configuration

configure > context *context_name* **> credit-control-service** *service_name*

Syntax Description

request timeout *timeout*
{ default | no } request timeout

default

Configures the default setting.

no

Removes the previous request timeout configuration.

timeout

Specifies the timeout period in seconds. The value must be an integer from 1 through 300.

Usage Guidelines

Use this command to configure the Diameter request timeout value, after which the request is deemed to have failed. This timeout is an overall timeout, and encompasses all retries with the server(s).

Example 1

The following command configures the timeout period to *150* seconds:

request timeout 150

Example 2

The following example explains the expected behavior of Response timeout configured on P-GW diameter endpoint with first CCRI Max-Wait-Time AVP:

```
If(request-timeout < response-timeout)
{
   Maximum-waittime = request-timeout;
}
else{
Maximum-waittime = response-timeout;
}

Config 1 : Req-timeout = 100; resp-timeout = 7

  Request-timeout = 100%10 = 10
  Response-timeout = 7

Maximum-waitime = 7milliseconds


Config 2: Req-timeout = 100; resp-timeout = 11

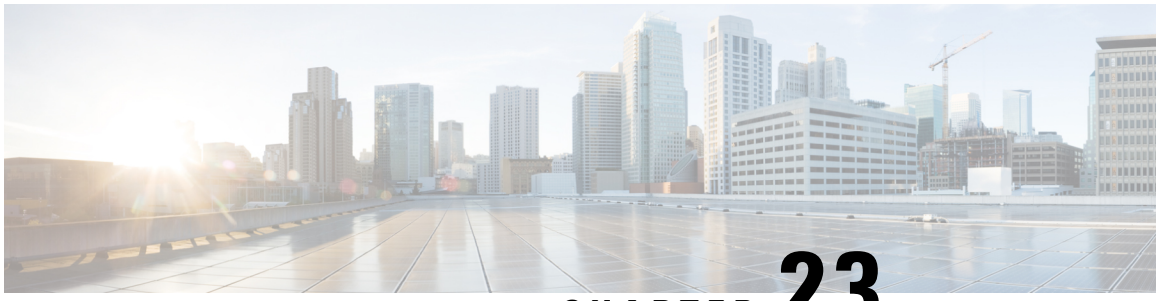
  Request-timeout = 100%10 = 10
```

```
  Response-timeout = 11

Maximum-waitime = 10milliseconds
```



Note The P-GW assigns a Minimum timer value to the Maximum time AVP in the CCR-I message. If the configured response time out value is observed through the Maximum time AVP then under the **ims auth-service** configure the **no request timeout** option. For both the **diameter-endpoint** and **request-timeout** CLI, the range must be an integer from 1 to 300.



CHAPTER 23

CRP Configuration Mode Commands

The CUPS Redundancy Protocol (CRP) Configuration Mode is used to configure BGP status monitoring on the Control Plane or User Plane.

Command Modes

Exec > Global Configuration > Context Configuration > CRP Configuration

configure > context *context_name* **> cups-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

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

- CRP Configuration Mode Commands, on page 809
- node-type, on page 810
- monitor bgp context, on page 810
- end, on page 811

CRP Configuration Mode Commands

The CUPS Redundancy Protocol (CRP) Configuration Mode is used to configure BGP status monitoring on the Control Plane or User Plane.

Command Modes

Exec > Global Configuration > Context Configuration > CRP Configuration

configure > context *context_name* **> cups-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

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

node-type

Enters CUPS Redundancy Protocol Configuration Mode on the Control Plane (CP) or User Plane (UP) on the chassis in this context.

Product

All

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > CRP Configuration

configure > context *context_name* **> cups-redundancy-protocol**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
node-type { control-plane | user-plane }
```

Usage Guidelines

Enters CUPS Redundancy Protocol Configuration Mode on the Control Plane (CP) or User Plane (UP) on the chassis.

Example

The following command enables CRP Configuration Mode on the User Plane:

```
node-type user-plane
```

monitor bgp context

Configures Border Gateway Protocol (BGP) monitoring on the Control Plane (CP) or User Plane (UP). This command is configured in the CUPS Redundancy Protocol (CRP) Configuration Mode.

Product

All

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > CRP Configuration

configure > context *context_name* **> cups-redundancy-protocol > user-plane**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crp-up)#
```

Syntax Description

```
[ no ] monitor bgp context bgp-session-context-name [
nexthop-router-ipv4-address | nexthop-router-ipv6-address ] { vrf
bgp-session-vrf-name } { group group-number { 1-10 } }
```

no

Disables BGP status monitoring on UP.

bgp context *bgp-session-context-name*

Specifies the context where BGP session with the peer is running. Specifies the context string.

nexthop-router-ipv4-address | nexthop-router-ipv6-address

Specifies the BGP peer IPv4 or IPv6 address to monitor.

vrf *bgp-session-vrf-name*

Specifies the BGP VPN Routing and Forwarding (VRF) instance.

group *group-number* 1-10

Specifies the group ID for the monitors. Valid values range from 1 to 10. The default value is 0, which implies that grouping is disabled for the BGP monitor being configured.

Usage Guidelines

Configures Border Gateway Protocol (BGP) monitoring on the Control Plane or User Plane (UP).

Example

The following command enables BGP monitoring on the User Plane:

```
monitor bgp context one 192.51.100.2 vrf abc group 2
```

end

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

Product

All

Privilege

Security Administrator, Administrator

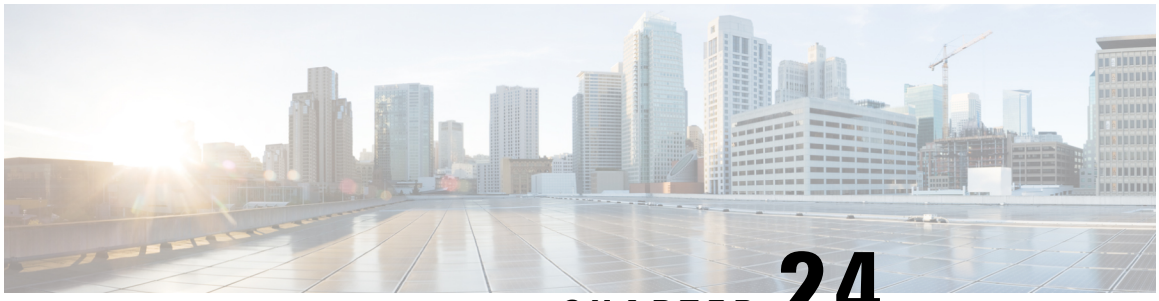
Syntax Description

```
end
```

Usage Guidelines

Use this command to return to the Exec mode.

end



CHAPTER 24

Crypto Group Configuration Mode Commands

The Crypto Group Configuration Mode is used to configure crypto (tunnel) groups that provide fail-over redundancy for IPSec tunnels to packet data networks (PDNs).

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Group Configuration

configure > context *context_name* **> crypto group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-grp)#
```

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

- end, on page 813
- exit, on page 814
- match address, on page 814
- match ip pool, on page 815
- switchover, on page 817

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 address

Associates an access control list (ACL) with the crypto group.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product
ePDG
FA
GGSN
HA
HeNBGW
HNBGW
HSGW
MME
P-GW
PDSN
S-GW
SAEGW
SCM
SecGW
SGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > Crypto Group Configuration

configure > **context** *context_name* > **crypto group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-grp)#
```

Syntax Description

`[ no ] match address` *`acl_name`* **`[`** *`preference`* **`]`**

no

Deletes a previously configured ACL association.

match address *acl_name*

Specifies the name of the ACL being matched to the crypto group entered as an alphanumeric string of 1 through 47 characters.

preference

The priority of the ACL.

The ACL preference is factored when a single packet matches the criteria of more than one ACL. *preference* is an integer from 0 through 4294967295; 0 is the highest priority.

If multiple ACLs are assigned the same priority, the last one entered will be used first.

Important The priorities are only compared for ACLs matched to other groups or to policy ACLs (those applied to the entire context).

Usage Guidelines

IP ACLs are associated with crypto groups using this command. Both the crypto group and the ACLs must be configured in the same context.

ISAKMP crypto maps can then be associated with the crypto group. This allows user traffic matching the rules of the ACL to be handled according to the policies configured as part of the crypto map.

Example

The following command associates an ACL called *corporate_acl* to the crypto group:

```
match address corporate_acl
```

match ip pool

Matches the specified IP pool to the current crypto group. This command can be used multiple times to match more than one IP pool.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.



Important The **match ip pool** command is not supported within a crypto group on the ASR 5500 platform.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Group Configuration

configure > context *context_name* **> crypto group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-grp)#
```

Syntax Description

[no] match ip pool pool-name *pool_name*

no

Deletes the matching statement for the specified IP pool from the crypto group.

match ip pool pool-name *pool_name*

Specifies the name of an existing IP pool that should be matched entered as an alphanumeric string of 1 through 31 characters.

Usage Guidelines

Use this command to set the names of IP pools that should be matched in the current crypto group.

Example

The following command sets a rule for the current crypto group that will match an IP pool named *ippool1*:

```
match ip pool pool-name ippool1
```

switchover

Configures the fail-over properties for the crypto group as part of the Redundant IPSec Fail-Over feature.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Group Configuration

configure > context *context_name* **> crypto group** *group_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-grp)#
```

Syntax Description

```
[ no ] switchover auto [ do-not-revert ]
```

no

Disables the automatic switchover of tunnels. This applies to switching primary-to-secondary and secondary-to-primary.

switchover auto

Allows the automatic switchover of tunnels. Default: Enabled

do-not-revert

Disables the automatic switchover of secondary tunnels to primary tunnels. Default: Disabled

Usage Guidelines

This command configures the fail-over options for the Redundant IPSec Fail-over feature.

If the automatic fail-over options are disabled, tunneled traffic must be manually switched to the alternate tunnel (or manually activated if no alternate tunnel is configured and available) using the following command in the Exec Mode:

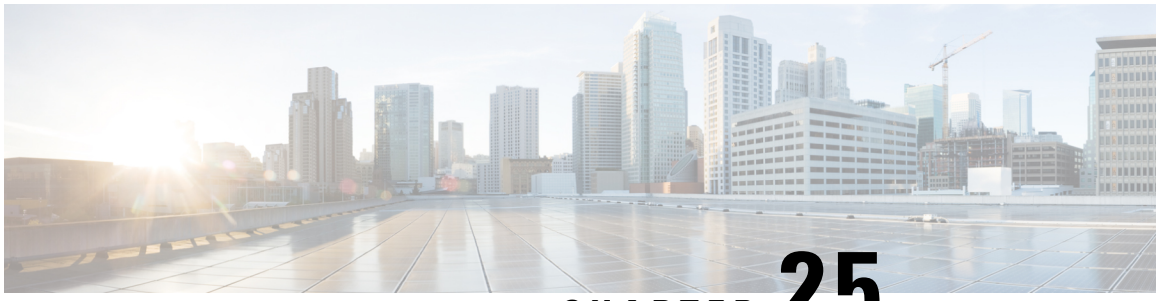
```
crypto-group group_name activate { primary | secondary }
```

For a definition of this command, see the **crypto-group** section of the Exec Mode Commands chapter of this guide.

Example

The following command disables the automatic secondary-to-primary switchover:

```
switchover auto do-not-revert
```



CHAPTER 25

Crypto Map IPSec Dynamic Configuration Mode Commands

Modification(s) to an existing dynamic crypto map configuration will not take effect until the related security association has been cleared. Refer to the description of the **clear crypto security-association** command in the *Exec Mode Commands* chapter for more information.

Command Modes

The Crypto Map IPSec Dynamic Configuration Mode is used to configure IPSec tunnels that are created as needed to facilitate subscriber sessions using Mobile IP or L2TP.

Exec > Global Configuration > Context Configuration > Crypto Map Dynamic Configuration

configure > context *context_name* **> crypto map** *policy_name* **ipsec-dynamic**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-dynamic-map)#
```

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

- end, on page 819
- exit, on page 820
- set, on page 820

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.

set

Configures parameters for the dynamic crypto map.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Crypto Map Dynamic Configuration

configure > **context** *context_name* > **crypto map** *policy_name* **ipsec-dynamic**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-dynamic-map)#
```

Syntax Description

set { control-dont-fragment { clear-bit | copy-bit | set-bit } | ikev1 natt [keepalive *sec* **] | ip mtu** *bytes* **| pfs { group1 | group2 | group5} | phase1-idtype { id-key-id | ipv4-address } [mode { aggressive | main }] | phase2-idtype { ipv4-address | ipv4-address-subnet} | security-association lifetime { keepalive | kilo-bytes** *kbytes* **| seconds** *secs* **} | transform-set** *transform_name* **[transform-set** *transform_name2...* **transform-set** *transform_name6* **] }**

no set { ikev1 natt | pfs | security-association lifetime {keepalive | kilo-bytes | seconds } | phase1-idtype | phase2-idtype | transform-set *transform_name* **[transform-set** *transform_name2...* **transform-set** *transform_name6* **] }**

no

Deletes the specified parameter or resets the specified parameter to the default value.

control-dont-fragment { clear-bit | copy-bit | set-bit }

Controls the don't fragment (DF) bit in the outer IP header of the IPSec tunnel data packet. Options are:

- **clear-bit**: Clears the DF bit from the outer IP header (sets it to 0).
- **copy-bit**: Copies the DF bit from the inner IP header to the outer IP header. This is the default action.
- **set-bit**: Sets the DF bit in the outer IP header (sets it to 1).

ikev1 natt [keepalive *sec*]

Enables IPSec NAT Traversal.

keepalive *sec*: The time to keep the NAT connection alive in seconds. *sec* must be an integer of from 1 through 3600.

ip mtu *bytes*

Specifies the IP Maximum Transmission Unit (MTU) in bytes as an integer from 576 to 2048.

mode { aggressive | main }

Configures the IKE negotiation mode as AGRESSIVE or MAIN.

pfs { group1 | group2 | group5 }

Specifies the modp Oakley group (also known as the Diffie-Hellman [D-H] group) that is used to determine the length of the base prime numbers that are used for Perfect Forward Secrecy (PFS).

- **group1**: Diffie-Hellman Group1 (768-bit modp)
- **group2**:- Diffie-Hellman Group2 (1024-bit modp)
- **group5**:- Diffie-Hellman Group5 (1536-bit modp)

phase1-idtype { id-key-id | ipv4-address } [mode { aggressive | main }]

Sets the IKE negotiations Phase 1 payload identifier.

Default: ipv4-address

id-key-id: Use ID_KEY_ID as the Phase 1 payload identifier.

ipv4-address: Use IPV4_ADDR as the Phase 1 payload identifier.

mode { aggressive | main }: Specify the IKE mode.

phase2-idtype { ipv4-address | ipv4-address-subnet }

Sets the IKE negotiations Phase 2 payload identifier.

Default: ipv4-address-subnet

ipv4-address: Use IPV4_ADDR as the Phase 2 payload identifier.

ipv4-address-subnet: Use IPV4_ADDR_SUBNET as the Phase 2 payload identifier.

security-association lifetime { keepalive | kilo-bytes *kbytes* | seconds *secs* }

Defaults:

- **keepalive**: Disabled
- **kilo-bytes**: 4608000 kbytes
- **seconds**: 28800 seconds

This keyword specifies the parameters that determine the length of time an IKE Security Association (SA) is active when no data is passing through a tunnel. When the lifetime expires, the tunnel is torn down. Whichever parameter is reached first expires the SA lifetime.

- **keepalive**: The SA lifetime expires only when a keepalive message is not responded to by the far end.
- **kilo-bytes**: This specifies the amount of data in kilobytes to allow through the tunnel before the SA lifetime expires; entered as an integer from 2560 through 4294967294.
- **seconds**: The number of seconds to wait before the SA lifetime expires; entered as an integer from 1200 through 86400.



Important If the dynamic crypto map is being used in conjunction with Mobile IP and the Mobile IP renewal timer is less than the crypto map's SA lifetime (either in terms of kilobytes or seconds), then the **keepalive** parameter **must** be configured.

transform-set *transform_name* [transform-set *transform_name2 ...* transform-set *transform_name6*]

Specifies the name of a transform set configured in the same context that will be associated with the crypto map. Refer to the command **crypto ipsec transform-set** for information on creating transform sets.

You can repeat this keyword up to 6 times on the command line to specify multiple transform sets.

trasnform_name is the name of the transform set entered as an alphanumeric string from 1 through 127 characters that is case sensitive.

Usage Guidelines

Use this command to set parameters for a dynamic crypto map.

Example

The following command sets the PFS group to Group1:

```
set pfs group1
```

The following command sets the SA lifetime to *50000* KB:

```
set security-association lifetime kilo-bytes 50000
```

The following command sets the SA lifetime to *10000* seconds:

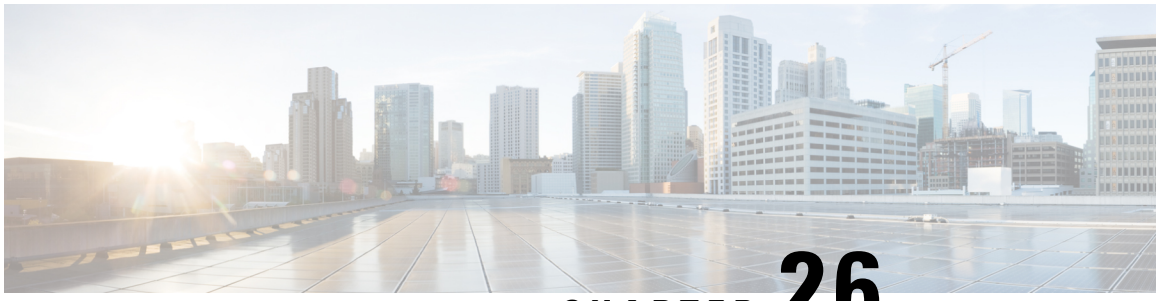
```
set security-association lifetime seconds 10000
```

The following command enables the SA to re-key when the tunnel lifetime expires:

```
set security-association lifetime keepalive
```

The following command defines transform sets *tset1* and *tset2*:

```
set transform-set tset1 transform-set tset2
```



CHAPTER 26

Crypto IPSec Configuration Mode Commands

The Crypto IPSec Configuration Mode is used to configure anti-replay window size and properties for system transform sets.

The anti-replay window may be increased to allow the IPSec decryptor to keep track of more than 64 packets.

Transform Sets are used to define IPSec security associations (SAs). IPSec SAs specify the IPSec protocols to use to protect packets.

Command Modes

Exec > Global Configuration > Context Configuration > Crypto IPSec Configuration

configure > context *context_name* **> crypto ipsec**

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

- end, on page 825
- exit, on page 826
- replay window-size, on page 826
- transform-set, on page 827

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.

replay window-size

Configures the IPSec anti-replay window size in packets (RFC 6479).

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Syntax Description

replay window-size*window_size*

window_size

Specifies the size of the anti-replay window in packets. Enter one of the following integers to change the number of packets in the window: 32, 64 (default), 128, 256, 384, 512.

Increasing the anti-replay window size has no impact on throughput and security.

Usage Guidelines

IPSec authentication provides anti-replay protection against an attacker duplicating encrypted packets by assigning a unique sequence number to each encrypted packet. (Security association [SA] anti-replay is a security service in which the receiver can reject old or duplicate packets to protect itself against replay attacks.) The decryptor checks off the sequence numbers that it has seen before. The encryptor assigns sequence numbers in an increasing order. The decryptor remembers the value X of the highest sequence number that it has already seen. N is the window size, and the decryptor also remembers whether it has seen packets having sequence numbers from X-N+1 through X. Any packet with the sequence number X-N is discarded. Currently, N is set at 64, so only 64 packets can be tracked by the decryptor.

At times, however, the 64-packet window size is not sufficient. For example, quality of service (QoS) gives priority to high-priority packets, which could cause some low-priority packets to be discarded even though they could be one of the last 64 packets received by the decryptor. This CLI command allows you to expand the window size, allowing the decryptor to keep track of more than 64 packets.

Example

The following command specifies an IPSec anti-replay window size of 128 packets.

crypto ipsec replay window-size 128

transform-set

Configures a transform set for IPSec policy

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator

Syntax Description

transform-set*tran_set_name* **{ ah hmac { md5-96 | sha1-96 } | esp hmac { md5-96 | none | sha1-96 } } { cipher { 3des-cbc | aes-cbc-128 | aes-cbc-256 | des-cbc } }**

tran_set_name

Specifies the name of the transform set as an alphanumeric stgring of 1 through 127 characters.

ah hmac { md5-96 | sha1-96 }

Specifies the use of Authentication Header (AH) with a hash-based message authentication code (HMAC) to guarantee connectionless integrity and data origin authentication of IP packets.

Hash options are MD5 Message-Digest Algorithm (md5-96) or Secure Hash Standard 1 (sha1-96).

esp hmac { md5-96 | none | sha1-96 }

Specifies the use of Encapsulating Secuirty Payload (ESP) with a hash-based message authentication code (HMAC) to guarantee connectionless integrity and data origin authentication of IP packets.

Hash options are MD5 Message-Digest Algorithm (md5-96), no hash, or Secure Hash Standard 1 (sha1-96).

cipher

If ESP is enabled, this option must be used to set the encapsulation cipher protocol to one of the following:

- **3des-cbc**: Triple Data Encryption Standard (3DES) in chain block (CBC) mode.
- **aes-cbc-128**: Advanced Encryption Standard (AES) in CBC mode with a 128-bit key.
- **aes-cbc-256**: Advanced Encryption Standard (AES) in CBC mode with a 256-bit key.
- **des-cbc**: DES in CBC mode.

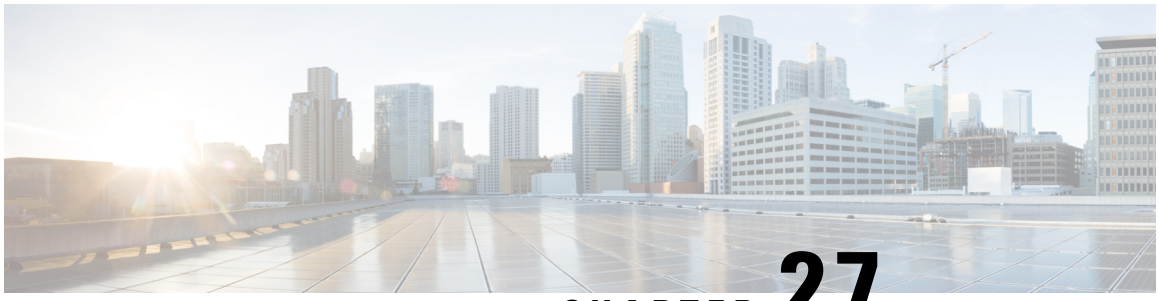
Usage Guidelines

Use this command to configure a transform set that specifies the type of IPSec protcol to use for securing communications.

Example

The following command specifies the use of IPSec AH with HMAC = MD5.

crypto ipsec transform-set tset013 ah hmac md5-96



CHAPTER 27

Crypto Map IPSec Manual Configuration Mode Commands

The Crypto IPSec Map Manual Configuration Mode is used to configure static IPSec tunnel properties.

Modification(s) to an existing crypto map manual configuration will not take effect until the related security association has been cleared. Refer to the description of the **clear crypto security-association** command in the *Exec Mode Commands* chapter for more information.

Important Because manual crypto map configurations require the use of static security keys (associations), they are not as secure as crypto maps that rely on dynamically configured keys. Therefore, they only be used for testing purposes.

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map Manual Configuration

configure > context *context_name* **> crypto map** *map_name* **ipsec-manual**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-manual-map)#
```

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

- end, on page 830
- exit, on page 830
- match address, on page 830
- set control-dont-fragment, on page 832
- set ip mtu, on page 833
- set ipv6 mtu, on page 834
- set peer, on page 835
- set session-key, on page 836
- set transform-set, on page 839

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 address

Matches or associates the crypto map to an access control list (ACL) configured in the same context.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map Manual Configuration

configure > context *context_name* **> crypto map** *map_name* **ipsec-manual**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-manual-map)#
```

Syntax Description

[no] match address *acl_name* **[** *priority* **]**

no

Removes a previously matched ACL.

match address *acl_name*

Specifies the name of the ACL with which the crypto map is to be matched. *acl_name* is an alphanumeric string of 1 through 47 characters that is case sensitive.

priority

Specifies the preference of the ACL. The ACL preference is factored when a single packet matches the criteria of more than one ACL. *priority* is an integer from 0 through 4294967295. 0 is the highest priority. Default: 0

Important The priorities are only compared for ACLs matched to other crypto maps or to policy ACLs (those applied to the entire context).

Usage Guidelines

ACLs matched to crypto maps are referred to as crypto ACLs. Crypto ACLs define the criteria that must be met in order for a subscriber data packet to routed over an IPSec tunnel.

Prior to routing, the system examines the properties of each subscriber data packet. If the packet properties match the criteria specified in the crypto ACL, the system will initiate the IPSec policy dictated by the crypto map.

Example

The following command sets the crypto map ACL to the ACL named *ACLlist1* and sets the crypto maps priority to the highest level.

```
match address ACLlist1 0
```

set control-dont-fragment

Controls the Don't Fragment (DF) bit in the outer IP header of the IPSec tunnel data packet.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map Manual Configuration

configure > context *context_name* **> crypto map** *map_name* **ipsec-manual**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-manual-map)#
```

Syntax Description

`[ default ] set control-dont-fragment { clear-bit | copy-bit | set-bit }`

default

Sets or restores default value assigned to a specified parameter.

clear-bit

Clears the DF bit from the outer IP header (sets it to 0).

copy-bit

Copies the DF bit from the inner IP header to the outer IP header. This is the default action.

set-bit

Sets the DF bit in the outer IP header (sets it to 1).

Usage Guidelines

Use this command to clear, copy, or set the don't fragment (DF) bit in the outer IP header of the IPSec tunnel data packet.

Example

The following command sets the DF bit in the outer IP header.

```
set control-dont-fragment set-bit
```

set ip mtu

Configures the IPv4 Maximum Transmission Unit (MTU) in bytes.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map Manual Configuration

configure > context *context_name* **> crypto map** *map_name* **ipsec-manual**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-manual-map)#
```

Syntax Description

ip mtu *bytes*

ip mtu *bytes*

Specifies the IPv4 MTU in bytes as an integer from 576 to 2048. Default is 1438.

Usage Guidelines

Use this command to set the IPv4 MTU in bytes

Example

The following command configures an IPv4 MTU of 1024 bytes.

```
set ip mtu 1024
```

set ipv6 mtu

Configures the IPv6 Maximum Transmission Unit (MTU) in bytes.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map Manual Configuration

configure > context *context_name* **> crypto map** *map_name* **ipsec-manual**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-manual-map)#
```

Syntax Description

ipv6 mtu *bytes*

ip mtu *bytes*

Specifies the IPv6 MTU in bytes as an integer from 576 to 2048. Default is 1438.

Usage Guidelines

Use this command to set the IPv6 MTU in bytes

Example

The following command configures an IPv6 MTU of 1024 bytes.

```
set ip mtu 1024
```

set peer

Configures the IP address of the peer security gateway that the system will establish the IPSec tunnel with.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map Manual Configuration

configure > context *context_name* **> crypto map** *map_name* **ipsec-manual**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-crypto-manual-map)#`

Syntax Description

[no] set peer *gw_address*

no

Removes a previously configured peer address.

set peer *gw_address*

Specifies the IP address of the peer security gateway with which the IPSec tunnel will be established. The IP address can be in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage Guidelines

Once the manual crypto map is fully configured and applied to an interface, the system will establish an IPSec tunnel with the security gateway specified by this command.

Because the tunnel relies on statically configured parameters, once created, it never expires; it exists until its configuration is deleted.

Example

The following command configures a security gateway address of *192.51.1.100* for the crypto map with which to establish a tunnel.

```
set peer 192.51.1.100
```

set session-key

Configures session key parameters for the manual crypto map.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map Manual Configuration

configure > context *context_name* **> crypto map** *map_name* **ipsec-manual**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-manual-map)#
```

Syntax Description

set session-key { inbound | outbound } { ah *ah_spi* **[encrypted] key** *ah_key* **| esp** *esp_spi* **[encrypted] cipher** *encryption_key* **[encrypted] authenticator** *auth_key* **}**

no set session-key { inbound | outbound }

no

Removes previously configured session key information.

inbound

Specifies that the key(s) will be used for tunnels carrying data sent by the security gateway.

outbound

Specifies that the key(s) will be used for tunnels carrying data sent by the system.

ah *ah_spi*

Configures the Security Parameter Index (SPI) for the Authentication Header (AH) protocol. The SPI is used to identify the AH security association (SA) between the system and the security gateway. *ah_spi* is an integer from 256 through 4294967295.

encrypted

Indicates the key provided is encrypted.

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

key *ah_key*

Configures the key used by the system to de/encapsulate IP packets using Authentication Header (AH) protocol. *ah_key* must be entered as either an alphanumeric string or a hexadecimal number beginning with "0x".

The length of the configured key must match the configured algorithm.

esp *esp_spi*

Configures SPI for the Encapsulating Security Payload (ESP) protocol. The SPI is used to identify the ESP security association (SA) between the system and the security gateway. *esp_spi* is an integer from 256 through 4294967295.

The length of the configured key must match the configured algorithm.

cipher *encryption_key*

Specifies the key used by the system to de/encrypt the payloads of IP packets using the ESP protocol. *encryption_key* must be entered as either an alphanumeric string or a hexadecimal number beginning with "0x".

The length of the configured key must match the configured algorithm.

authenticator *auth_key*

Specifies the key used by the system to authenticate the IP packets once encryption has been performed. *auth_key* must be entered as either an alphanumeric string or a hexadecimal number beginning with "0x".

The length of the configured key must match the configured algorithm.

Usage Guidelines

Manual crypto maps rely on the use of statically configured keys to establish IPSec tunnels. This command allows the configuration of the static keys.

Identical keys must be configured on both the system and the security gateway in order for the tunnel to be established.

The length of the configured key must match the configured algorithm.

This command can be entered up to two time for the same crypto map: once to configure inbound key properties, and once to configure outbound key properties.

Example

The following command configures a manual crypto map with the following session key properties:

- Keys are for tunnels initiated by the system to the security gateway.
- ESP will be used with an SPI of *310*.
- Encryption key is *sd23r9skd0fi3as*.
- Authentication key is *sfd23408imi9yn*.

```
set session-key outbound esp 310 cipher sd23r9skd0fi3as authenticator
sfd23408imi9yn
```

set transform-set

Configures the name of a transform set that the crypto map is associated with.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map Manual Configuration

configure > context *context_name* **> crypto map** *map_name* **ipsec-manual**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-manual-map)#
```

Syntax Description

`[ no ] set transform-set` *`transform_name`*

no

Removes a previously configured transform set association.

set transform-set *transform_name*

Specifies the name of the transform set expressed as an alphanumeric string of 1 through 127 characters that is case sensitive.

Usage Guidelines

System transform sets contain the IPSec policy definitions for crypto maps. Refer to the **crypto ipsec transform-set** command for information on creating transform sets.

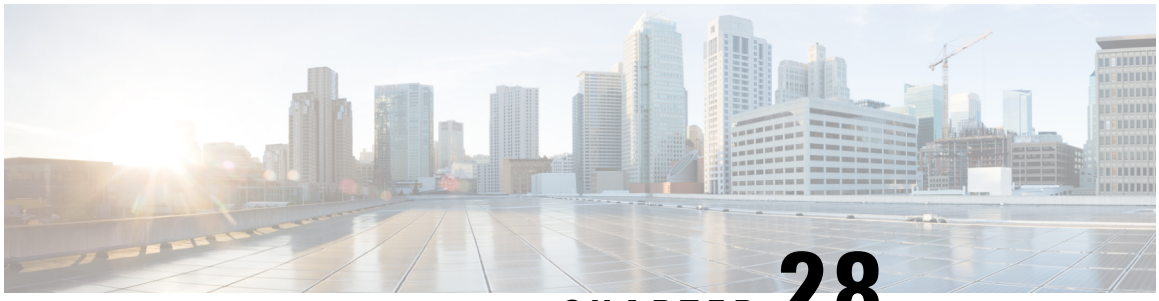


Important Transform sets must be configured prior to configuring session key information for the crypto map.

Example

The following command associates a transform set named *esp_tset* with the crypto map:

```
set transform-set esp_tset
```



CHAPTER 28

Crypto Map IKEv2-IPv4 Configuration Mode Commands

Command Modes

The Crypto Map IKEv2-IPv4 Configuration Mode is used to configure an IKEv2 IPsec policy for secure X3 interface tunneling between a P-GW and a lawful intercept server.

Exec > Global Configuration > Context Configuration > Crypto Map IKEv2-IPv4 Configuration

configure > context *context_name* **> crypto map** *template_name* **ikev2-ipv4**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-ikev2-ipv4-map)#
```

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

- allow-cert-enc cert-hash-url, on page 842
- authentication, on page 842
- blockedlist, on page 844
- ca-certificate list, on page 845
- ca-crl list, on page 846
- certificate, on page 847
- control-dont-fragment, on page 848
- end, on page 849
- exit, on page 849
- ikev2-ikesa, on page 850
- keepalive, on page 852
- match, on page 853
- natt, on page 855
- ocsp, on page 856
- payload, on page 857
- peer, on page 858
- remote-secret-list, on page 859
- permitlist , on page 860

allow-cert-enc cert-hash-url

Enables support for a certificate encoding type other than the default. When enabled hash and URL encoding type are supported in CERT and CERTREQ payloads.

Product

Security gateway products

Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege

Security Administrator

Syntax Description

```
[ no ] allow-cert-enc cert-hash-url
```

no

Disables support for hash and URL encoding type in CERT and CERTREQ payloads.

Usage Guidelines

Enable support for a certificate encoding type other than the default. When enabled hash and URL encoding type are supported in CERT and CERTREQ payloads.

Example

The following command enables hash and URL encoding type in CERT and CERTREQ payloads:

```
allow-cert-enc cert-hash-url
```

authentication

Configures the subscriber authentication method used for this crypto map.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Syntax Description

authentication { local { certificate | pre-shared-key } { encrypted key *value* **| key** *value* **} | min-key-size***min_key_size* **| remote { certificate | pre-shared-key } { encrypted key** *value***| key***value* **}**

[no | default] authentication min-key-size

local | remote

Specifies which authentication method will be used by the crypto map – local or remote.

[no | default] authentication min-key-size

no Disables minimum key size validation feature.

default Sets default key size. Default is 255.

min-key-size*min_key_size*

Specifies Minimum Cert Key size. Default is 255.

min_key_size must be an integer between 255 and 8192.

certificate

Specifies that a certificate will be used by this crypto map for authentication.

pre-shared-key { encrypted key *value* | key *value* }

Specifies that a pre-shared key will be used by this crypto map for authentication.

encrypted key *value*: Specifies that the pre-shared key used for authentication is encrypted and expressed as an alphanumeric string of 1 through 255 characters for releases prior to 15.0, or 16 to 496 characters for release 15.0 and higher.

key *value*: Specifies that the pre-shared key used for authentication is clear text and expressed as an alphanumeric string of 1 through 32 characters for releases prior to 14.0 or 1 through 255 characters for release 14.0 and higher.

Usage Guidelines Use this command to specify the type of authentication performed for IPSEC peers attempting to access the system via this crypto map.

Example

The following command sets the authentication method to an open key value of *6d7970617373776f7264*:

```
authentication pre-shared-key key 6d79706173773776f7264
```

blockedlist

Enables or disables a blockedlist (access denied) for this map.

Product All products supporting IPSec blockedlisting



Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege Security Administrator

Syntax Description In releases prior to StarOS 21.26:

```
[ no ] blacklist
```

From StarOS 21.26 and later releases:

```
[ no ] blockedlist
```

no

Disables blockedlisting for this crypto map. By default blockedlisting is disabled.

Usage Guidelines Use this command to enable blockedlisting for this crypto map. A blockedlist is a list or register of entities that are denied a particular privilege, service, mobility, access or recognition. With blockedlisting, any peer is allowed to connect as long as it does not appear in the list. For additional information on blockedlisting, refer to the *System Administration Guide.*

Example

In releases prior to StarOS 21.26:

The following command enables blacklisting:

```
blacklist
```

From StarOS 21.26 and later releases:

The following command enables blockedlisting:

```
blockedist
```

ca-certificate list

Used to bind an X.509 Certificate Authority (CA) certificate to a crypto map.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Syntax Description

```
ca-certificate list ca-cert-name name [ ca-cert-name  name ]
no ca-certificate
```

no

Unbinds the ca-certificate(s) bound to the crypto map.

ca-cert-name *name*

Binds the named X.509 Certificate Authority (CA) certificate to a crypto map. *name* is an alphanumeric string of 1 through 129 characters.

You can chain multiple(max 4) certificates in a single command instance.

Usage Guidelines

Used to bind an X.509 CA certificate to a map.

Example

Use the following example to add a CA certificate to a list:

```
ca-certificate list ca-cert-name CA_list1
```

ca-crl list

Binds one or more Certificate Authority-Certificate Revocation Lists (CA-CRLs) to this crypto map.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Syntax Description

```
ca-crl list ca-crl-name name [ ca-crl-name name ] +
no ca-crl
```

no

Removes the CA-CRL configuration from this map.

ca-crl-name *name*

Specifies the CA-CRL to associate with this crypto map. *name* must be the name of an existing CA-CRL expressed as an alphanumeric string of 1 through 129 characters.

+ indicates that a list of multiple CA-CRLs can be configured for a crypto map. You can chain multiple (max four) CA-CRLs in a single command instance.

Usage Guidelines

Use this command to associate a CA-CRL name with this crypto map.

CA-CRLs are configured in the Global Configuration Mode. For more information about configuring CA-CRLs, refer to the **ca-crl name** command in the *Global Configuration Mode Commands* chapter.

Example

The following example binds CA-CRLs named *CRL-5* and *CRL-7* to this crypto map:

```
ca-crl list ca-crl-name CRL-5 ca-crl-name CRL-7
```

certificate

Used to bind a single X.509 trusted certificate to a crypto map.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Syntax Description

`[ no ] certificate` *`name`*

no

Unbinds a certificate from crypto map.

name

Specifies the name of a X.509 trusted certificate to bind to a crypto map. *name* is an alphanumeric string of 1 through 129 characters.

Usage Guidelines

Use this command to bind an X.509 certificate to a map.

Example

Use the following example to prevent a certificate from being included in the Auth Exchange payload:

```
no certificate
```

control-dont-fragment

Controls the Don't Fragment (DF) bit in the outer IP header of the IPSec tunnel data packet.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

i

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Syntax Description

control-dont-fragment { clear-bit | copy-bit | set-bit }

clear-bit

Clears the DF bit from the outer IP header (sets it to 0).

copy-bit

Copies the DF bit from the inner IP header to the outer IP header. This is the default action.

set-bit

Sets the DF bit in the outer IP header (sets it to 1).

Usage Guidelines

A packet is encapsulated in IPsec headers at both ends. The new packet can copy the DF bit from the original unencapsulated packet into the outer IP header, or it can set the DF bit if there is not one in the original packet. It can also clear a DF bit that it does not need.

Example

The following command sets the DF bit in the outer IP header:

```
control-dont-fragment set-bit
```

end

Exits the current 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.

ikev2-ikesa

Configures parameters for the IKEv2 IKE Security Associations within this crypto template.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Syntax Description

ikev2-ikesa { allow-empty-ikesa | max-retransmissions *number* **| policy { error-notification [invalid-major-version] [invalid-message-id [invalid-major-version | invalid-syntax]] | invalid-syntax [invalid-major-version] | use-rfc5996-notification } | rekey [disallow-param-change] | retransmission-timeout** *msec* **[exponential] | setup-timer** *sec* **| transform-set list** *name1 name2 name3 name4 name5 name6* **}**
default ikev2-ikesa { allow-empty-ikesa | max-retransmissions | policy error-notification | rekey [disallow-param-change] | setup-timer }

no ikev2-ikesa { allow-empty-ikesa *name* **| policy { error-notification | use-rfc5996-notification } | rekey** *sec* **| transform-set list }**

no ikev2-ikesa

Disables a previously enabled parameter.

allow-empty-ikesa

Default is not to allow-empty-ikesa. Activate to have the IKEv2 stack keep the IKE SA when all the Child SAs have been deleted.

max-retransmissions *number*

Specifies the maximum number of retransmissions of an IKEv2 IKE Exchange Request if a response has not been received. *number* must be an integer from 1 through 8. Default: 5

policy { error-notification [invalid-major-version] [invalid-message-id [invalid-major-version | invalid-syntax]] | invalid-syntax [invalid-major-version] | use-rfc5996-notification }

Specifies the default policy for generating an IKEv2 Invalid Message ID error when PDIF receives an out-of-sequence packet.

error-notification: Sends an Error Notify Message to the MS for Invalid IKEv2 Exchange Message ID and Invalid IKEv2 Exchange Syntax for the IKE_SA_INIT Exchange.

[invalid-major-version]: Sends an Error Notify Message for Invalid Major Version

[invalid-message-id]: Sends an Error Notify Message for Invalid IKEv2 Exchange Message ID.

[invalid-syntax]: Sends an Error Notify Message for Invalid IKEv2 Exchange Syntax.

use-rfc5996-notification: Enables support for TEMPORARY_FAILURE and CHILDSA_NOT_FOUND notify payloads.

rekey [disallow-param-change]

Specifies if IKESA rekeying should occur before the configured lifetime expires (at approximately 90% of the lifetime interval). Default is not to re-key.

The **disallow-param-change** option does not allow changes in negotiation parameters during rekey.

retransmission-timeout *msec*

Specifies the timeout period (in milliseconds) before a retransmission of an IKEv2 IKE exchange request is sent (if the corresponding response has not been received). *msec* must be an integer from 300 to 15000. Default: 500

exponential

Specifies that the subsequent retransmission delays are exponentially increased with a maximum limit of 15000ms.

setup-timer *sec*

Specifies the number of seconds before a IKEv2 IKE Security Association that is not fully established is terminated. *sec* must be an integer from 1 through 3600. Default: 16

transform-set list *name1*

Specifies the name of a context-level configured IKEv2 IKE Security Association transform set. *name1 ...name6*must be an existing IKEv2 IKESA Transform Set expressed as an alphanumeric string of 1 through 127 characters.

The transform set is a space-separated list of IKEv2-IKESA SA transform sets to be used for deriving IKEv2 IKE Security Associations from this crypto template. A minimum of one transform-set is required; maximum configurable is six.

Usage Guidelines

Use this command to configure parameters for the IKEv2 IKE Security Associations within this crypto template.

Example

The following command configures the maximum number of IKEv2 IKESA request retransmissions to *7*:

```
ikev2-ikesa max-retransmissions 7
```

The following command configures the IKEv2 IKESA request retransmission timeout to *400* milliseconds:

```
ikev2-ikesa retransmission-timeout 400
```

The following command configures the IKEv2 IKESA transform set *ikesa43*:

```
ikev2-ikesa transform-set list ikesa43
```

keepalive

Configures keepalive or dead peer detection for security associations used within this crypto template.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Syntax Description

```
keepalive [ interval sec ] [ timeout sec [ num-retry num ]
no keepalive
```

no

Disables keepalive messaging.

interval *sec*

Specifies the amount of time (in seconds) that must elapse before the next keepalive request is sent. *sec* must be an integer from 10 through 3600. Default: 10

timeout *sec*

Specifies the amount of time (in seconds) which must elapse during which no traffic is received from the IKE_SA peer or any CHILD_SAs derived from the IKE_SA for Dead Peer Detection to be initiated. *sec* must be an integer from 10 through 3600. Default: 10

num-retry *num*

Specifies the number of times the system will retry a non-responsive peer before defining the peer as off-line or out-of-service. *num* must be an integer from 1 through 100. Default: 2

Usage Guidelines

Use this command to set parameters associated with determining the availability of peer servers.

Example

The following command sets a keepalive interval to three minutes (*180* seconds):

```
keepalive interval 180
```

match

Matches or associates the crypto map to an access control list (ACL) configured in the same context.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Syntax Description

match address *acl_name* **[** *priority* **]**
no match address *acl_name*

no

Removes a previously matched ACL.

match address *acl_name*

Specifies The name of the ACL with which the crypto map is to be matched. *acl_name* is an alphanumeric string of 1 through 79 characters that is case sensitive.

priority

Specifies the preference of the ACL as integer from 0 through 4294967295. 0 is the highest priority. Default: 0

The ACL preference is factored when a single packet matches the criteria of more than one ACL.

Important The priorities are only compared for ACLs matched to other crypto maps or to policy ACLs (those applied to the entire context).

Usage Guidelines ACLs matched to crypto maps are referred to as crypto ACLs. Crypto ACLs define the criteria that must be met in order for a subscriber data packet to routed over an IPSec tunnel.

Prior to routing, the system examines the properties of each subscriber data packet. If the packet properties match the criteria specified in the crypto ACL, the system will initiate the IPSec policy dictated by the crypto map.

Example

The following command sets the crypto map ACL to the ACL named *acl-list1* and sets the crypto maps priority to the highest level.

```
match address acl-list1 0
```

natt

Configures Network Address Translation - Traversal (NAT-T) for all security associations associated with this crypto template. This feature is disabled by default.

Product All Security Gateway products

Privilege Security Administrator

Syntax Description

```
[ default | no ] natt [ include-header ] [ send-keepalive [ idle-interval idle_secs ] [ interval interval_secs ] ]
```

default

Disables NAT-T for all security associations associated with this crypto template.

no

Disables NAT-T for all security associations associated with this crypto template.

include-header

Includes the NAT-T header in IPSec packets.

send-keepalive [idle-interval *idle_secs*] [interval *interval_secs*]

Sends NAT-Traversal keepalive messages.

idle-interval *idle_secs*: Specifies the number of seconds that can elapse without sending NAT keepalive packets before sending NAT keepalive packets is started. *idle_secs* is an integer from 20 to 86400. Default: 60.

interval *interval_secs*: Specifies the number of seconds between the sending of NAT keepalive packets. *interval_secs* is an integer from 20 to 86400. Default: 60.

Usage Guidelines Use this command to configure NAT-T for security associations within this crypto template.

Example

The following command disables NAT-T for this crypto template:

```
no natt
```

ocsp

Enables use of Online Certificate Status Protocol (OCSP) from a crypto template. OCSP provides a facility to obtain timely information on the status of a certificate.

Product All products supporting IPSec

Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege Security Administrator

Syntax Description

```
ocsp [ nonce | responder-address ipv4_address [ port port_value ] ]
no ocsp [ nonce | responder-address [ port ] ]
default ocsp [ nonce ]
```

no

Disables the use of OCSP.

default

Restores the default value assigned for ocsp nonce.

nonce

Enables sending nonce (unique identifier) in OCSP requests.

responder-address *ipv4_address*

Configures the OCSP responder address that is used when absent in the peer (device) certificate.

ipv4_address is an IPv4 address specified in dotted decimal format.

port *port_value*

Configures the port for OCSP responder.

port_value is an integer value between 1 and 65535. The default port is 8889.

Usage Guidelines

This command enables the use of Online Certificate Protocol (OCSP) from a crypto map/template. OCSP provides a facility to obtain timely information on the status of a certificate.

OCSP messages are exchanged between a gateway and an OCSP responder during a certificate transaction. The responder immediately provides the status of the presented certificate. The status can be good, revoked or unknown. The gateway can then proceed based on the response.

Example

The following command enables OSCP:

```
ocsp
```

payload

Creates a new, or specifies an existing, crypto map payload and enters the Crypto Map Payload Configuration Mode.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Syntax Description

```
payload name match ipv4
no payload name
```

payload *name*

Specifies the name of a new or existing crypto template payload as an alphanumeric string of 1 through 127 characters.

match ipv4

Filters IPSec IPv4 Child Security Association creation requests for subscriber calls using this payload. Further filtering can be performed by applying the following:

Usage Guidelines

Use this command to create a new or enter an existing crypto template payload. The payload mechanism is a means of associating parameters for the Security Association (SA) being negotiated.

Two payloads are required: one each for MIP and IKEv2. The first payload is used for establishing the initial Child SA Tunnel Inner Address (TIA) which will be torn down. The second payload is used for establishing the remaining Child SAs. Note that if there is no second payload defined with home-address as the *ip-address-allocation* then no MIP call can be established, just a Simple IP call.

Currently, the only available match is for ChildSA, although other matches are planned for future releases.

Entering this command results in the following prompt:

[*ctxt_name*]*hostname*(cfg-crypto-<*name*>-ikev2-tunnel-payload)#

Crypto Template IKEv2-IPv4 Payload Configuration Mode commands are defined in the Crypto Template IKEv2-IPv4 Payload Configuration Mode Commands chapter.

Example

The following command configures a crypto template payload called *payload5* and enters the Crypto Template IKEv2-IPv6 Payload Configuration Mode:

```
payload payload5 match ipv4
```

peer

Configures the IP address of a peer IPSec.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Syntax Description

peer *ip_address*
no peer

no

Removes the configured peer IP address.

peer *ip_address*

Specifies the IP address of a peer IPSec server in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage Guidelines

Use this command to specify a peer IPsec peer server. The IPsec peer server can also be the Lawful Intercept server.

Example

The following command configures the system to recognize an IPsec peer server with an IPv6 address of *fe80::200:f8ff:fe21:67cf*:

```
peer fe80::200:f8ff:fe21:67cf
```

remote-secret-list

Enables the use of a Remote Secret List containing up to 1000 pre-shared keys.

Product

All Security Gateway products

Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege

Security Administrator

Syntax Description

remote-secret-list *list_name*
no remote-secret-list

no

Disables use of a Remote Secret List.

list_name

Specifies the name of an existing Remote Secret List as an alphanumeric string of 1 through127 characters.

Usage Guidelines

Enable the use of a Remote Secret List containing up to 1000 pre-shared keys.

Only one active remote-secret-list is supported per system.

For additional information, refer to the *Remote Secret List Configuration Commands* chapter of the *Command Line Interface Reference* and the *System Administration Guide*.

Example

The following command enables a remote-secret-list named *rs-list*:

remote-secret-list rs-list

permitlist

Enables or disables a permitlist (access granted) for this crypto map.

Product

All products supporting IPSec permitlisting .

Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege

Security Administrator

Syntax Description

In releases prior to StarOS 21.26:

[no] whitelist

From StarOS 21.26 and later releases:

[no] permitlist

no

Disables permitlisting for this crypto map. By default permitlisting is disabled.

Usage Guidelines

Use this command to enable permitlisting for this crypto map. A permitlist is a list or register of entities that are being provided a particular privilege, service, mobility, access or recognition. With permitlisting , no peer is allowed to connect unless it appears in the list. For additional information on permitlisting , refer to the *System Administration Guide.*

Example

In releases prior to StarOS 21.26:

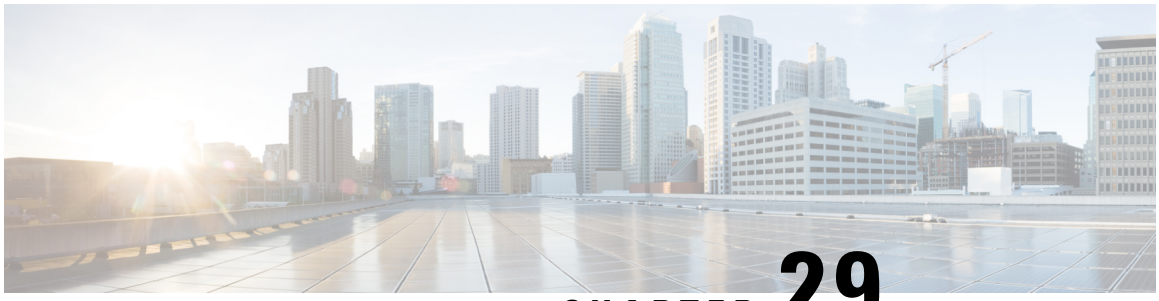
The following command enables whitelisting:

```
whitelist
```

From StarOS 21.26 and later releases:

The following command enables permitlisting:

```
permitlist
```



CHAPTER 29

Crypto Map IPSec IKEv1 Configuration Mode Commands

Modification(s) to an existing IKEv1 crypto map configuration will not take effect until the related security association has been cleared. Refer to the description of the **clear crypto security-association** command in the *Exec Mode Commands* chapter for more information.

Command Modes

The Crypto Map IPSec IKEv1 Configuration Mode is used to configure properties for IPSec tunnels that will be created using the Internet Key Exchange (IKE) that operates within the framework of the Internet Key Exchange version 1 (IKEv1).

Exec > Global Configuration > Context Configuration > Crypto Map IPSec IKEv1 Configuration

configure > context *context_name* **> crypto map** *policy_name* **ipsec-ikev1**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-map)#
```

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

- end, on page 863
- exit, on page 864
- ipsec-on-demux, on page 864
- match address, on page 865
- match crypto group, on page 866
- match ip pool, on page 868
- set, on page 869

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.

ipsec-on-demux

Enable spawning of IPSec manager for this Crypto map on Demux Card.

Product IPSec (IKEv1/IKEv2 ACL Mode)

Privilege Security Administrator

Command Modes Exec > Global Configuration > Context Configuration > Crypto Map IPSec IKEv1 Configuration

configure > context *context_name* **> crypto map** *policy_name* **ipsec-ikev1**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-crypto-map)#`

Syntax Description `[ no ] ipsec-on-demux`

no

Disables the spawning of IPSec manager for Crypto map on Demux Card.

ipsec-on-demux

Enables the spawning of IPSec manager for this Crypto map on Demux Card.

Important If the configuration is removed using no option, then this Crypto map must be removed and added again for this configuration to work.

Example

The following configuration enables spawning of IPSec manager for this Crypto map on Demux Card.

```
ipsec-on-demux
```

match address

Matches or associates the crypto map to an access control list (ACL) configured in the same context.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map IPSec IKEv1 Configuration

configure > context *context_name* **> crypto map** *policy_name* **ipsec-ikev1**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-map)#
```

Syntax Description

`[ no ] match address` *`acl_name priority`*

no

Removes a previously matched ACL.

match address *acl_name*

Specifies the name of the ACL with which the crypto map is to be matched as an alphanumeric string of 1 through 79 characters that is case sensitive.

priority

Specifies the preference of the ACL. The ACL preference is factored when a single packet matches the criteria of more than one ACL.

The preference is an integer value from 0 to 4294967295; 0 is the highest priority. Default: 0

Important The priorities are only compared for ACLs matched to other crypto maps or to policy ACLs (those applied to the entire context).

Usage Guidelines

ACLs matched to crypto maps are referred to as crypto ACLs. Crypto ACLs define the criteria that must be met in order for a subscriber data packet to routed over an IPSec tunnel.

Prior to routing, the system examines the properties of each subscriber data packet. If the packet properties match the criteria specified in the crypto ACL, the system will initiate the IPSec policy dictated by the crypto map.

Example

The following command sets the crypto map ACL to the ACL named *ACLlist1* and sets the crypto maps priority to the highest level.

```
match address ACLlist1 0
```

match crypto group

Matches or associates the crypto map a crypto group configured in the same context.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map IPSec IKEv1 Configuration

configure > context *context_name* **> crypto map** *policy_name* **ipsec-ikev1**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-map)#
```

Syntax Description

`[ no ] match crypto group` *`group_name`* **`{ primary | secondary }`**

no

Deletes a previously configured crypto group association.

match crypto group *group_name*

Specifies the name of the crypto group entered as an alphanumeric string of 1 through 127 characters that is case sensitive.

primary

Specifies that the policies configured as part of this crypto map will be used for the primary tunnel in the Redundant IPSec Tunnel Failover feature.

secondary

Specifies that the policies configured as part of this crypto map will be used for the secondary tunnel in the Redundant IPSec Tunnel Failover feature.

Usage Guidelines

Use this command to dictate the primary and secondary tunnel policies used for the Redundant IPSec Tunnel Failover feature.

At least two policies must be configured to use this feature. One policy must be configured as the primary, the other as the secondary.

Example

The following command associates the crypto map to a crypto group called *group1* and dictates that it will serve as the primary tunnel policy:

```
match crypto group group1 primary
```

match ip pool

Matches the specified IP pool to the current IKEv1 crypto map. This command can be used multiple times to change more than one IP pool.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Important The **match ip pool** command is not supported on the ASR 5500 platform.

Product

ePDG
FA
GGSN
HA
HeNBGW
HNBGW
HSGW
MME
P-GW
PDSN
S-GW
SAEGW
SCM
SecGW
SGSN

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map IPSec IKEv1 Configuration

configure > **context** *context_name* > **crypto map** *policy_name* **ipsec-ikev1**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-map)#
```

Syntax Description

[no] match ip pool pool-name *pool_name* **[destination-network** *ip_address* **[/***mask* **]**

no

Delete the matching statement for the specified IP pool from the crypto map.

match ip pool pool-name *pool_name*

Specifies the name of an existing IP poolthat should be matched as an alphanumeric string of 1 through 31 characters.

destination-network *ip_address* [*/mask*]

Specifies the IP address of the destination network in IPv4 dotted-decimal or IPV6 colon-separated-hexadecimal notation.

/mask specifies the subnet mask bits (representing the subnet mask). This variable must be entered in IPv4 dotted-decimal or !Pv6 colon-separated-hexadecimal CIDR notation.

An IP pool attached to the crypto map can have multiple IPSec tunnels according to the destination of the packet being forwarded to internet.

Important Each invocation of this command will add another destination network to the IP pool, with a maximum of eight destination networks per crypto map.

Usage Guidelines

Use this command to set the names of IP pools that should be matched in the current crypto map.

Important If an IP address pool that is matched to a IKEv1 crypto map is resized, removed, or added, the corresponding security association must be cleared in order for the change to take effect. Refer to the **clear crypto** command in the Exec mode for information on clearing security associations.

Example

The following command sets a rule for the current crypto map that will match an IP pool named *ippool1*:

```
match ip pool pool-name ippool1
```

set

Configures parameters for the dynamic crypto map.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map IPSec IKEv1 Configuration

configure > context *context_name* **> crypto map** *policy_name* **ipsec-ikev1**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-map)#
```

Syntax Description

set { bgp *peer_address* **| control-dont-fragment { clear-bit | copy-bit | set-bit } | ikev1 natt [keepalive** *sec* **] | ip mtu** *bytes* **| ipv6 mtu** *bytes* **| mode { aggressive | main } | peer** *peer_address* **| pfs { group1 | group2 | group5 } | phase1-idtype { id-key-id | ipv4-address [mode { aggressive | main }] | phase2-idtype { ipv4-address | ipv4-address-subnet } | security-association lifetime { disable-phase2-rekey | keepalive | kilo-bytes** *kbytes* **| seconds** *secs* **} transform-set** *transform_name* **[transform-set** *transform_name2 ...* **transform-set** *transform_name6* **]**

no set { ikev1 natt | pfs | phase1-idtype | phase2-idtype | security-association lifetime { disable-phase2-rekey | keepalive | kilo-bytes | seconds } | transform-set *transform_name* **[transform-set** *transform_name2 ...* **transform-set** *transform_name6* **]**

bgp *peer_address*

Specifies the IP address of the BGP peer in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

control-dont-fragment { clear-bit | copy-bit | set-bit }

Controls the don't fragment (DF) bit in the outer IP header of the IPSec tunnel data packet. Options are:

- **clear-bit**: Clears the DF bit from the outer IP header (sets it to 0).
- **copy-bit**: Copies the DF bit from the inner IP header to the outer IP header. This is the default action.
- **set-bit**: Sets the DF bit in the outer IP header (sets it to 1).

ikev1 natt [keepalive *time*]



Important NAT Traversal (NATT) for IKEv1 IPSec session is not supported.

Specifies IKE parameters.

natt: Enables IPSec NAT Traversal.

keepalive *time*: The time to keep the NAT connection alive in seconds. *time* must be an integer of from 1 through 3600.

ip mtu *bytes*

Specifies the IPv4 Maximum Transmission Unit (MTU) in bytes as an integer from 576 to 2048.

ipv6 mtu *bytes*

Specifies the IPv6 Maximum Transmission Unit (MTU) in bytes as an integer from 576 to 2048.

mode { aggressive | main }

Configures the IKE negotiation mode as AGRESSIVE or MAIN.

peer *peer_address*

Specifies the peer IP address of a remote gateway in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

pfs { group1 | group2 | group5 }

Specifies the modp Oakley group (also known as the Diffie-Hellman [D-H] group) that is used to determine the length of the base prime numbers that are used for Perfect Forward Secrecy (PFS).

- **group1**: Diffie-Hellman Group1 (768-bit modp)
- **group2**: Diffie-Hellman Group2 (1024-bit modp)
- **group5**: Diffie-Hellman Group5 (1536-bit modp)

phase1-idtype { id-key-id | ipv4-address [mode { aggressive | main }]

Sets the IKE negotiations Phase 1 payload identifier. Default: id-key-id

id-key-id: ID KEY ID

ipv4-address: ID IPV4 Address

- **mode**: Configures IKE mode
- **aggressive**: IKE negotiation mode: AGGRESSIVE
- **main**: IKE negotiation mode: MAIN

phase2-idtype { ipv4-address | ipv4-address-subnet }

Sets the IKE negotiations Phase 2 payload identifier.

Default: ipv4-address-subnet

- **ipv4-address**: Use IPV4_ADDR as the Phase 2 payload identifier.
- **ipv4-address-subnet**: Use IPV4_ADDR_SUBNET as the Phase 2 payload identifier.

security-association lifetime { disable-phase2-rekey | keepalive | kilo-bytes *kbytes* | seconds *secs* }

Defaults:

- **disable-phase2-rekey**: Rekeying is enabled by default
- **keepalive**: Disabled
- **kilo-bytes:** 4608000 kbytes
- **seconds:** 28800 seconds

Specifies the parameters that determine the length of time an IKE Security Association (SA) is active when no data is passing through a tunnel. When the lifetime expires, the tunnel is torn down. Whichever parameter is reached first expires the SA lifetime.

- **disable-phase2-rekey**: If this keyword is specified, the Phase2 SA is not rekeyed when the lifetime expires.
- **keepalive**: The SA lifetime expires only when a keepalive message is not responded to by the far end.
- **kilo-bytes**: This specifies the amount of data (n kilobytes) to allow through the tunnel before the SA lifetime expires. *kbytes* must be an integer from 2560 through 4294967294.
- **seconds**: The number of seconds to wait before the SA lifetime expires. *secs* must be an integer from 1200 through 86400.



Important If the dynamic crypto map is being used in conjunction with Mobile IP and the Mobile IP renewal timer is less than the crypto map's SA lifetime (either in terms of kilobytes or seconds), then the keepalive parameter must be configured.

transform-set *transform_name* [transform-set *transform_name2 ...* transform-set *transform_name6*]

Specifies the name of a transform set configured in the same context that will be associated with the crypto map. Refer to the command **crypto ipsec transform-set** for information on creating transform sets.

You can repeat this keyword up to 6 times on the command line to specify multiple transform sets.

transform_name is the name of the transform set entered as an alphanumeric string of 1 through 127 characters that is case sensitive.

no

Deletes the specified parameter or resets the specified parameter to the default value.

Usage Guidelines

Use this command to set parameters for a dynamic crypto map.

Example

The following command sets the PFS group to Group1:

```
set pfs group1
```

The following command sets the SA lifetime to *50000* KB:

```
set security-association lifetime kilo-bytes 50000
```

The following command sets the SA lifetime to *10000* seconds:

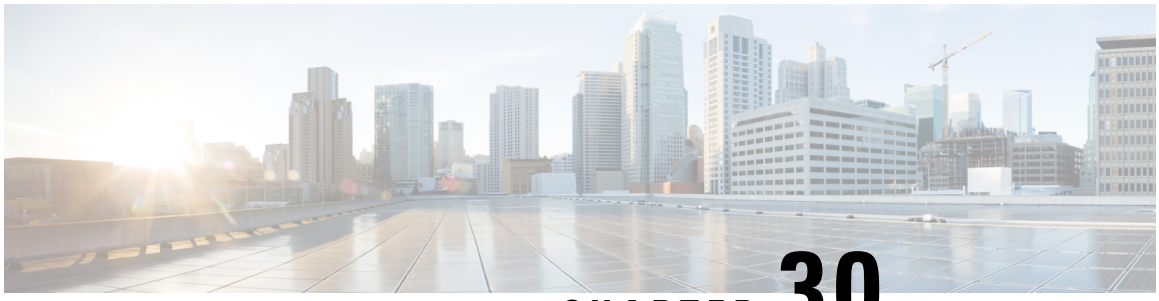
```
set security-association lifetime seconds 10000
```

The following command enables the SA to re-key when the tunnel lifetime expires:

```
set security-association lifetime keepalive
```

The following command defines transform sets *tset1* and *tset2*.

```
set transform-set tset1 transform-set tset2
```



CHAPTER 30

Crypto Map IKEv2-IPv4 Payload Configuration Mode Commands

The Crypto Map IKEv2-IPv4 Payload Configuration Mode is used to assign the correct IPSec transform-set from a list of up to four different transform-sets, and to assign Mobile IP addresses.

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map IKEv2-IPv4 > Crypto Map IKEv2-IPv4 Payload Configuration

configure > context *context_name* **> crypto map** *map_name* **ikev2-ipv4 > payload** *payload_name* **match ipv4**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-ikev2-ipv4-payload)#
```

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

- end, on page 875
- exit, on page 876
- ipsec, on page 876
- lifetime, on page 877
- rekey, on page 878

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.

ipsec

Configures the IPSec transform set to be used for this crypto template payload.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Syntax Description

ipsec transform-set list *transform_set_name transform_set_name transform_set_name transform_set_name*
no ipsec transform-set list

ipsec transform-set list *transform_set_name*

Specifies the context -level IKEv2 IPSec Child Security Association (SA) transform sets to be used in the crypto template payload. This is a space-separated list. Up to four transform sets can be entered. *transform_set_name* is an alphanumeric string of 1 through 127 characters.

Usage Guidelines

Use this command to list the IPSec transform set(s) to use in this crypto template payload.

Example

The following command configures IPSec transform sets named *ipset1* and *ipset2* for use in this crypto template payload:

```
ipsec transform-set list ipset1 ipset2
```

lifetime

Configures the number of seconds and/or kilobytes for IPSec Child SAs derived from this crypto template payload to exist.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Syntax Description

```
lifetime { sec  [ kilo-bytes kbytes ] | kilobytes kbytes }
default lifetime
```

default

Returns the lifetime value to the default setting of 86400 seconds.

sec

Specifies the number of seconds for IPSec Child Security Associations derived from this crypto template payload to exist. *sec* must be an integer from 60 through 604800. Default: 86400

kilo-bytes *kbytes*

Specifies lifetime in kilobytes for IPSec Child Security Associations derived from this Crypto Map. *kbytes* must be an integer from 1 through 2147483648.

Usage Guidelines

Use this command to configure the number of seconds and/or kilobytes for IPSec Child Security Associations derived from this crypto template payload to exist.

Example

The following command configures the IPSec child SA lifetime to be 120 seconds:

```
lifetime 120
```

rekey

Configures child security association rekeying.

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

ePDG

FA

FNG

GGSN

HA

HNBGW

P-GW

PDSN

SAEGW

SCM

SGSN

Privilege

Security Administrator

Syntax Description

```
rekey [ keepalive ]
[ default | no ] rekey
```

default

Returns the feature to the default setting of disabled.

no

Disables this feature.

keepalive

If specified, a session will be rekeyed even if there has been no data exchanged since the last rekeying operation. By default rekeying is only performed if there has been data exchanged since the previous rekey.

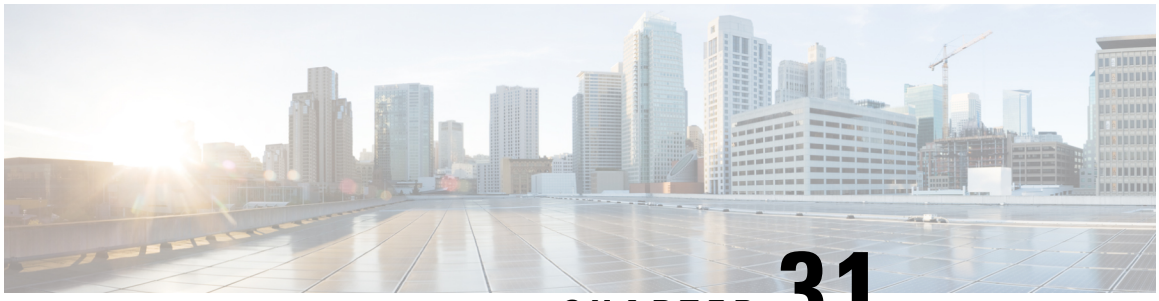
Usage Guidelines

Use this command to enable or disable the ability to rekey IPSec Child SAs after approximately 90% of the Child SA lifetime has expired. The default, and recommended setting, is not to perform rekeying. No rekeying means the P-GW will not originate rekeying operations and will not process CHILD SA rekeying requests from the MS.

Example

The following command disables rekeying:

```
no rekey
```



CHAPTER 31

Crypto Map IKEv2-IPv6 Configuration Mode Commands

Command Modes

The Crypto Map IKEv2-IPv6 Configuration Mode is used to configure an IKEv2 IPsec policy for secure X3 interface tunneling between a P-GW and a lawful intercept server.

Exec > Global Configuration > Context Configuration > Crypto Map IKEv2-IPv6 Configuration

configure > context *context_name* **> crypto map** *map_name* **ikev2-ipv6**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-ikev2-ipv6-map)#
```

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

- allow-cert-enc cert-hash-url, on page 882
- authentication, on page 882
- blockedlist , on page 884
- ca-certificate list, on page 884
- ca-crl list, on page 885
- certificate, on page 887
- control-dont-fragment, on page 888
- end, on page 889
- exit, on page 889
- ikev2-ikesa, on page 890
- keepalive, on page 892
- match, on page 893
- ocsp, on page 895
- payload, on page 896
- peer, on page 897
- remote-secret-list, on page 898
- permitlist, on page 899

allow-cert-enc cert-hash-url

Enables support for a certificate encoding type other than the default. When enabled hash and URL encoding type are supported in CERT and CERTREQ payloads.

Product

Security gateway products

Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege

Security Administrator

Syntax Description

```
[ no ] allow-cert-enc cert-hash-url
```

no

Disables support for hash and URL encoding type in CERT and CERTREQ payloads.

Usage Guidelines

Enable support for a certificate encoding type other than the default. When enabled hash and URL encoding type are supported in CERT and CERTREQ payloads.

Example

The following command enables hash and URL encoding type in CERT and CERTREQ payloads:

```
allow-cert-enc cert-hash-url
```

authentication

Configures the subscriber authentication method used for this crypto map.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Syntax Description

`authentication { local | remote } ( certificate | pre-shared-key { encrypted key` *`value`* **`| key`** *`value`* **`}`**

local | remote

Specifies which authentication method will be used by the crypto map – local or remote.

certificate

Specifies that a certificate will be used by this crypto map for authentication.

pre-shared-key { encrypted key *value* | key *value* }

Specifies that a pre-shared key will be used by this crypto map for authentication.

encrypted key *value*: Specifies that the pre-shared key used for authentication is encrypted and expressed as an alphanumeric string of 1 through 255 characters for releases prior to 15.0, or 16 to 444 characters for release 15.0 and higher.

key *value*: Specifies that the pre-shared key used for authentication is clear text and expressed as an alphanumeric string of 1 through 32 characters for releases prior to 14.0 or 1 through 255 characters for release 14.0 and higher.

Usage Guidelines

Use this command to specify the type of authentication performed for subscribers attempting to access the system via this crypto map.

Example

The following command sets the authentication method to an open key value of *6d7970617373776f7264*:

```
authentication pre-shared-key key 6d79706173737 76f7264
```

blockedlist

Enables or disables a blockedlist (access denied) for this map.

Product

All products supporting IPSec blockedlisting

Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege

Security Administrator

Syntax Description

In releases prior to StarOS 21.26:

```
[ no ] blacklist
```

From StarOS 21.26 and later releases:

```
[ no ] blockedlist
```

no

Disables blockedlisting for this crypto map. By default blockedlisting is disabled.

Usage Guidelines

Use this command to enable blockedlisting for this crypto map. A blockedlist is a list or register of entities that are denied a particular privilege, service, mobility, access or recognition. With blockedlisting , any peer is allowed to connect as long as it does not appear in the list. For additional information on blockedlisting , refer to the *System Administration Guide.*

Example

In releases prior to StarOS 21.26:

The following command enables blacklisting:

```
blacklist
```

ca-certificate list

Used to bind an X.509 Certificate Authority (CA) certificate list to a crypto template.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Syntax Description

ca-certificate list ca-cert-name *cert_name* **[ca-cert-name** *cert_name* **] [ca-cert-name** *cert_name* **] ... [ca-cert-name** *cert_name* **]**
no ca-certificate

no

Removes a CA certificate list from the cryto map.

ca-cert-name *cert_name*

Adds the named X.509 CA certificate to a list of CAs associated with a crypto map. *cert_name* is an alphanumeric string of 1 through 129 characters.

You can chain multiple certificates in a single command instance.

Usage Guidelines

Used to bind an X.509 CA certificate list to a crypto map.

Example

Use the following example to add a CA root certificate named *CAS_list1* to a list:

```
ca-certificate list ca-cert-name CA_list1
```

ca-crl list

Binds one or more Certificate Authority-Certificate Revocation Lists (CA-CRLs) to this crypto template.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Syntax Description

ca-crl list ca-crl-name *name* **[ca-crl-name** *name* **] [ca-crl-name** *cacrl_name* **]... [ca-crl-name** *cacrl_name* **]**
no ca-crl

no

Removes the CA-CRL configuration from this template.

ca-crl-name *cacrl_name*

Specifies the CA-CRL to associate with this crypto template. *cacrl_name* must be the name of an existing CA-CRL expressed as an alphanumeric string of 1 through 129 characters. Multiple lists can be configured for a crypto template.

You can chain multiple CA-CRLs in a single command instance.

Usage Guidelines

Use this command to associate a CA-CRL name with this crypto template.

CA-CRLs are configured in the Global Configuration Mode. For more information about configuring CA-CRLs, refer to the **ca-crl name** command in the *Global Configuration Mode Commands* chapter.

Example

The following example binds CA-CRLs named *CRL-5* and *CRL-7* to this crypto template:

```
ca-crl list ca-crl-name CRL-5 ca-crl-name CRL-7
```

certificate

Used to bind a single X.509 trusted certificate to a crypto map.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Syntax Description

```
certificate cert_name [ validate ]
no certificate [ validate ]
```

no

Removes any applied certificate or prevents the certificate from being included in the Auth Exchange response payload.

cert_name

Specifies the name of a X.509 trusted certificate to bind to a crypto map. *name* is an alphanumeric string of 1 through 127 characters.

validate

Enables validation for the self-certificate.

Usage Guidelines

Can be used to bind an X.509 certificate to a template, or include or exclude it from the Auth Exchange response payload.

Example

Use the following example to prevent a certificate from being included in the Auth Exchange payload:

```
no certificate validate
```

control-dont-fragment

Controls the Don't Fragment (DF) bit in the outer IP header of the IPSec tunnel data packet.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege Security Administrator

Syntax Description `control-dont-fragment { clear-bit | copy-bit | set-bit }`

clear-bit

Clears the DF bit from the outer IP header (sets it to 0).

copy-bit

Copies the DF bit from the inner IP header to the outer IP header. This is the default action.

set-bit

Sets the DF bit in the outer IP header (sets it to 1).

Usage Guidelines A packet is encapsulated in IPsec headers at both ends. The new packet can copy the DF bit from the original unencapsulated packet into the outer IP header, or it can set the DF bit if there is not one in the original packet. It can also clear a DF bit that it does not need.

Example

The following command sets the DF bit in the outer IP header:

```
control-dont-fragment set-bit
```

end

Exits the current 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.

ikev2-ikesa

Configures parameters for the IKEv2 IKE Security Associations within this crypto map.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Syntax Description

```
ikev2-ikesa { allow-empty-ikesa | max-retransmissions number  | policy {
error-notification | use-rfc5996-notification }  | rekey [
disallow-param-change ] | retransmission-timeout msec | setup-timer sec |
transform-set list name }
default ikev2-ikesa { allow-empty-ikesa | max-retransmissions | policy
error-notification |  rekey | setup-timer }
no ikev2-ikesa { allow-empty-ikesa |  policy { error-notification |
use-rfc5996-notification } | rekey | transform-set list }
```

default

Restores the selected keyword to its default value.

no

Disables a previously enabled parameter.

allow-empty-ikesa

Default is not to allow-empty-ikesa. Activate to have the IKEv2 stack keep the IKE SA when all the Child SAs have been deleted.

max-retransmissions *number*

Specifies the maximum number of retransmissions of an IKEv2 IKE exchange request if a response has not been received.

number must be an integer from 1 to 8.

Default: 5

policy { error-notification | use-rfc5996-notification }

Notifies error policy.

error-notification: Error Notify Messages will be sent to MS for Invalid IKEv2 Exchange Message ID and Invalid IKEv2 Exchange Syntax for the IKE_SA_INIT Exchange.

use-rfc5996-notification: Enables sending and receive processing for RFC 5996 notifications - TEMPORARY_FAILURE and CHILD_SA_NOT_FOUND.

rekey [disallow=param-change]

Specifies if IKESA rekeying should occur before the configured lifetime expires (at approximately 90% of the lifetime interval).

Default is not to re-key.

The **disallow-param-change** option prevents changes in negotiation parameters during rekey.

retransmission-timeout *msec*

Specifies the timeout period in milliseconds before a retransmission of an IKEv2 IKE exchange request is sent (if the corresponding response has not been received).

msec must be an integer from 300 to 15000.

Default: 500

setup-timer *sec*

Specifies the number of seconds before an IKEv2 IKE Security Association that is not fully established is terminated.

sec must be an integer from 16 to 3600.

Default: 60

transform-set list *name*

A space-separated list of context-level configured IKEv2 IKE Security Association transform sets to be used for deriving IKEv2 IKE Security Associations from this crypto map.

name must be an existing IKEv2 IKESA Transform Set expressed as an alphanumeric string of 1 through 127 characters. A minimum of one transform set is required; maximum configurable is six.

Usage Guidelines

Use this command to configure parameters for the IKEv2 IKE Security Associations within this crypto map.

Example

The following command configures the maximum number of IKEv2 IKESA request retransmissions to *7*:

```
ikev2-ikesa max-retransmissions 7
```

keepalive

Configures keepalive or dead peer detection for security associations used within this crypto template.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator

Syntax Description

```
keepalive [ interval sec ] [ timeout sec ] [ num-retry num ]
default keepalive [ interval ] [ timeout ] [ num-retry ]
no keepalive
```

no

Disables keepalive messaging.

interval *sec*

Specifies the amount of time (in seconds) that must elapse before the next keepalive request is sent. *sec* must be an integer from 10 through 3600. Default: 10

timeout *sec*

Specifies the amount of time (in seconds) which must elapse during which no traffic is received from the IKE_SA peer or any CHILD_SAs derived from the IKE_SA for Dead Peer Detection to be initiated. *sec* must be an integer from 10 through 3600. Default: 10

num-retry *num*

Specifies the number of times the system will retry a non-responsive peer before defining the peer as off-line or out-of-service. *num* must be an integer from 1 through 100. Default: 2

Usage Guidelines

Use this command to set parameters associated with determining the availability of peer servers.

Example

The following command sets a keepalive interval to three minutes (*180* seconds):

```
keepalive interval 180
```

match

Matches or associates the crypto map to an access control list (ACL) configured in the same context.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Syntax Description

```
match address acl_name [ priority ]
no match address
```

no

Removes a previously matched ACL.

match address *acl_name*

Specifies The name of the ACL with which the crypto map is to be matched. *acl_name* is an alphanumeric string of 1 through 79 characters that is case sensitive.

priority

Specifies the preference of the ACL as integer from 0 through 4294967295. 0 is the highest priority. Default: 0

The ACL preference is factored when a single packet matches the criteria of more than one ACL.

Important The priorities are only compared for ACLs matched to other crypto maps or to policy ACLs (those applied to the entire context).

Usage Guidelines

ACLs matched to crypto maps are referred to as crypto ACLs. Crypto ACLs define the criteria that must be met in order for a subscriber data packet to routed over an IPSec tunnel.

Prior to routing, the system examines the properties of each subscriber data packet. If the packet properties match the criteria specified in the crypto ACL, the system will initiate the IPSec policy dictated by the crypto map.

Example

The following command sets the crypto map ACL to the ACL named *acl-list1* and sets the crypto maps priority to the highest level.

```
match address acl-list1 0
```

ocsp

Enables use of Online Certificate Status Protocol (OCSP) from a crypto template. OCSP provides a facility to obtain timely information on the status of a certificate.

Product

All products supporting IPSec

Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege

Security Administrator

Syntax Description

```
ocsp [ nonce | responder-address ipv4_address [ port port_value ] ]
no ocsp [ nonce | responder-address [ port ] ]
default ocsp [ nonce ]
```

no

Disables the use of OCSP.

default

Restores the default value assigned for ocsp nonce.

nonce

Enables sending nonce (unique identifier) in OCSP requests.

responder-address *ipv4_address*

Configures the OCSP responder address that is used when absent in the peer (device) certificate.

ipv4_address is an IPv4 address specified in dotted decimal format.

port *port_value*

Configures the port for OCSP responder.

port_value is an integer value between 1 and 65535. The default port is 8889.

Usage Guidelines

This command enables the use of Online Certificate Protocol (OCSP) from a crypto map/template. OCSP provides a facility to obtain timely information on the status of a certificate.

OCSP messages are exchanged between a gateway and an OCSP responder during a certificate transaction. The responder immediately provides the status of the presented certificate. The status can be good, revoked or unknown. The gateway can then proceed based on the response.

Example

The following command enables OSCP:

ocsp

payload

Creates a new, or specifies an existing, crypto template payload and enters the Crypto Template Payload Configuration Mode.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Syntax Description

payload *name* **match ipv6**
no payload *name*

payload *name*

Specifies the name of a new or existing crypto template payload as an alphanumeric string of 1 through 127 characters.

match ipv6

Filters IPSec IPv6 Child Security Association creation requests for subscriber calls using this payload. Further filtering can be performed by applying the following:

Usage Guidelines

Use this command to create a new or enter an existing crypto template payload. The payload mechanism is a means of associating parameters for the Security Association (SA) being negotiated.

Two payloads are required: one each for MIP and IKEv2. The first payload is used for establishing the initial Child SA Tunnel Inner Address (TIA) which will be torn down. The second payload is used for establishing the remaining Child SAs. Note that if there is no second payload defined with home-address as the *ip-address-allocation* then no MIP call can be established, just a Simple IP call.

Currently, the only available match is for ChildSA, although other matches are planned for future releases.

Entering this command results in the following prompt:

[*ctxt_name*]*hostname*(cfg-crypto-<*name*>-ikev2-tunnel-payload)#

Crypto Template IKEv2-IPv6 Payload Configuration Mode commands are defined in the Crypto Template IKEv2-IPv6 Payload Configuration Mode Commands chapter.

Example

The following command configures a crypto template payload called *payload5* and enters the Crypto Template IKEv2-IPv6 Payload Configuration Mode:

```
payload payload5 match ipv6
```

peer

Configures the IP address of a peer IPSec server.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Syntax Description

```
peer ip_address
no peer
```

no

Removes the configured peer server IP address.

peer *ip_address*

Specifies the IP address of a peer IPSec server in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage Guidelines

Use this command to specify a peer IPsec peer server. The IPsec peer server can also be the Lawful Intercept server.

Example

The following command configures the system to recognize an IPsec peer server with an IPv6 address of *fe80::200:f8ff:fe21:67cf*:

```
peer fe80::200:f8ff:fe21:67cf
```

remote-secret-list

Enables the use of a Remote Secret List containing up to 1000 pre-shared keys.

Product

All Security Gateway products



Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege

Security Administrator

Syntax Description

```
remote-secret-list list_name
no remote-secret-list
```

no

Disables use of a Remote Secret List.

list_name

Specifies the name of an existing Remote Secret List as an alphanumeric string of 1 through127 characters.

Usage Guidelines

Enable the use of a Remote Secret List containing up to 1000 pre-shared keys.

Only one active remote-secret-list is supported per system.

For additional information, refer to the *Remote Secret List Configuration Commands* chapter of the *Command Line Interface Reference* and the *System Administration Guide*.

Example

The following command enables a remote-secret-list named *rs-list*:

```
remote-secret-list rs-list
```

permitlist

Enables or disables a permitlist (access granted) for this crypto map.

Product

All products supporting IPSec permitlisting

Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege

Security Administrator

Syntax Description

In releases prior to StarOS 21.26:

```
[ no ] whitelist
```

From StarOS 21.26 and later releases:

```
[ no ] permitlist
```

no

Disables permitlisting for this crypto map. By default permitlisting is disabled.

Usage Guidelines

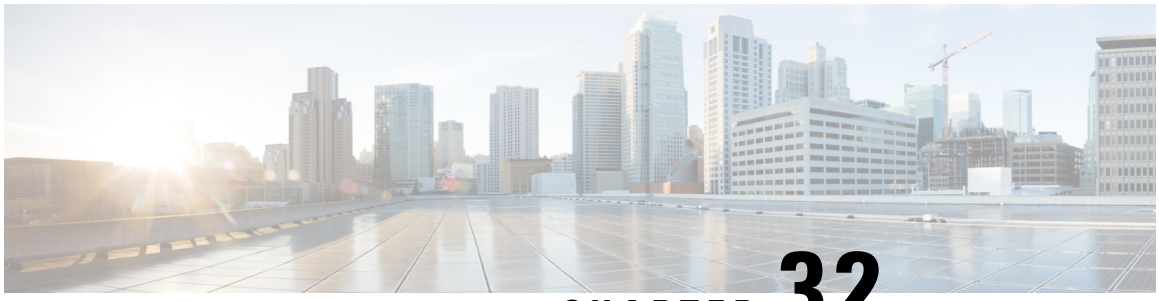
Use this command to enable permitlisting for this crypto map. A permitlist is a list or register of entities that are being provided a particular privilege, service, mobility, access or recognition. With permitlisting, no peer is allowed to connect unless it appears in the list. For additional information on permitlisting, refer to the *System Administration Guide.*

Example

In releases prior to StarOS 21.26:

The following command enables whitelisting:

whitelist



CHAPTER 32

Crypto Map IKEv2-IPv6 Payload Configuration Mode Commands

The Crypto Map IKEv2-IPv6 Payload Configuration Mode is used to assign the correct IPSec transform-set from a list of up to four different transform-sets, and to assign Mobile IP addresses.

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map IKEv2-IPv6 Configuration > Crypto Map IKEv2-IPv6 Payload Configuration

configure > context *context_name* **> crypto map** *map_name* **ikev2-ipv6 > payload** *payload_name* **match ipv6**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-ikev2-ipv6-payload)#
```



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

- end, on page 901
- exit, on page 902
- ipsec, on page 902
- lifetime, on page 903
- rekey, on page 905

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.

ipsec

Configures the IPSec transform sets to be used for this crypto map payload.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map IKEv2-IPv6 Configuration > Crypto Map IKEv2-IPv6 Payload Configuration

configure > context *context_name* **> crypto map** *map_name* **ikev2-ipv6 > payload** *payload_name* **match ipv6**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-ikev2-ipv6-payload)#
```

Syntax Description

ipsec transform-set list *transform_set_name* **[** *transform_set_name* **] [** *transform_set_name* **] [** *transform_set_name* **]**
no ipsec transform-set list

no

Disables the transform set list.

ipsec transform-set list *transform_set_name*

Specifies the context-level name of the IKEv2 IPsec Child Security Association (SA) transform setto be used in the crypto map payload. This is a space-separated list. From 1 to 4 transform sets can be entered. *transform_set_name* is an alphanumeric string of 1 through 127 characters.

Usage Guidelines

Use this command to list the IPSec transform set(s) to use in this crypto map payload.

Example

The following command configures IPSec transform sets named *ipset1* and *ipset2* to be used in this crypto template payload:

```
ipsec transform-set list ipset1 ipset2
```

lifetime

Configures the number of seconds and/or kilobytes for IPSec Child SAs derived from this crypto template payload to exist.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map IKEv2-IPv6 Configuration > Crypto Map IKEv2-IPv6 Payload Configuration

configure > context *context_name* **> crypto map** *map_name* **ikev2-ipv6 > payload** *payload_name* **match ipv6**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-ikev2-ipv6-payload)#
```

Syntax Description

```
lifetime { sec [ kilo-bytes kbytes ] | kilobytes kbytes }
default lifetime
```

default

Returns the lifetime value to the default setting of 86400 seconds.

sec

Specifies the number of seconds for IPSec Child Security Associations derived from this crypto template payload to exist. *sec* must be an integer from 60 through 604800. Default: 86400

kilo-bytes *kbytes*

Specifies lifetime in kilobytes for IPSec Child Security Associations derived from this Crypto Map. *kbytes* must be an integer from 1 through 2147483648.

Usage Guidelines

Use this command to configure the number of seconds and/or kilobytes for IPSec Child Security Associations derived from this crypto template payload to exist.

Example

The following command configures the IPSec child SA lifetime to be 120 seconds:

```
lifetime 120
```

rekey

Configures child security association rekeying.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map IKEv2-IPv6 Configuration > Crypto Map IKEv2-IPv6 Payload Configuration

configure > context *context_name* **> crypto map** *map_name* **ikev2-ipv6 > payload** *payload_name* **match ipv6**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-ikev2-ipv6-payload)#
```

Syntax Description

```
rekey [ keepalive ]
[ default | no ] rekey
```

default

Returns the feature to the default setting of disabled.

no

Disables this feature.

keepalive

If specified, a session will be rekeyed even if there has been no data exchanged since the last rekeying operation. By default rekeying is only performed if there has been data exchanged since the previous rekey.

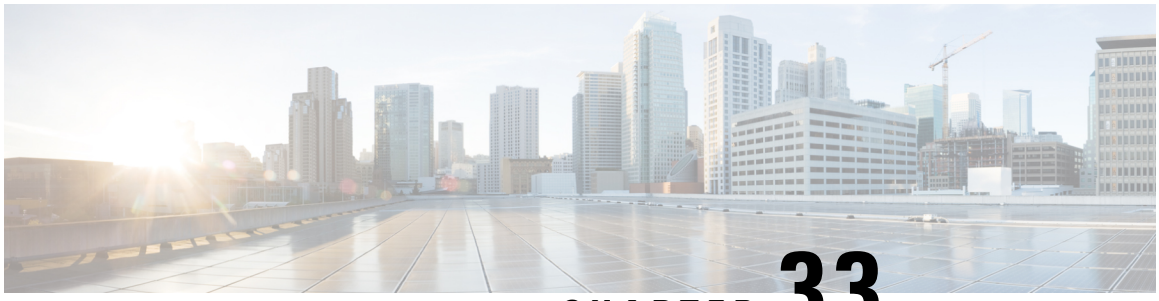
Usage Guidelines

Use this command to enable or disable the ability to rekey IPSec Child SAs after approximately 90% of the Child SA lifetime has expired. The default, and recommended setting, is not to perform rekeying. No rekeying means the P-GW will not originate rekeying operations and will not process CHILD SA rekeying requests from the MS.

Example

The following command disables rekeying:

```
no rekey
```



CHAPTER 33

Crypto Template Configuration Mode Commands

The Crypto Template Configuration Mode is used to configure an IKEv2 IPSec policy. It includes most of the IPSec parameters and IKEv2 dynamic parameters for cryptographic and authentication algorithms. A security gateway service will not function without a configured crypto template. Only one crypto template can be configured per service.

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(crf-crypto-tmp1-ikev2-tunnel)#
```

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

- allow-cert-enc cert-hash-url, on page 908
- allow-custom-fqdn-idr, on page 909
- authentication, on page 909
- blockedlist, on page 911
- ca-certificate list, on page 912
- ca-crl list, on page 913
- certificate, on page 913
- configuration-payload, on page 914
- control-dont-fragment, on page 915
- dns-handling, on page 916
- dos cookie-challenge notify-payload, on page 917
- ecn, on page 918
- end, on page 919
- exit, on page 919
- identity local, on page 919
- ikev2-ikesa, on page 920
- ikev2-ikesa ddos, on page 924
- ikev2-ikesa dscp, on page 926
- ip, on page 927

- ipv6, on page 928
- keepalive, on page 929
- max-childsa, on page 930
- nai, on page 931
- natt, on page 932
- notify-payload, on page 933
- ocsp, on page 934
- payload, on page 935
- peer network, on page 936
- remote-secret-list, on page 937
- server certificate, on page 938
- timeout, on page 938
- vendor-policy, on page 939
- permitlist, on page 940

allow-cert-enc cert-hash-url

Enables support for a certificate encoding type other than the default. When enabled hash and URL encoding type are supported in CERT and CERTREQ payloads.

Product

Security gateway products

Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege

Security Administrator

Syntax Description

```
[ no ] allow-cert-enc cert-hash-url
```

no

Disables support for hash and URL encoding type in CERT and CERTREQ payloads.

Usage Guidelines

Enable support for a certificate encoding type other than the default. When enabled hash and URL encoding type are supported in CERT and CERTREQ payloads.

Example

The following command enables hash and URL encoding type in CERT and CERTREQ payloads:

```
allow-cert-enc cert-hash-url
```

allow-custom-fqdn-idr

Allows non-standard FQDN (Fully Qualified Domain Name) strings in the IDr (Identification - Responder) payload of IKE_AUTH messages received from the UE with the payload type as FQDN.

Product

All services using IKEv2 IPSec

Privilege

Security Administrator

Syntax Description

`[ default | no ] allow-custom-fqdn-idr`

no

Does not allow non-standard FQDN strings in the IDr payload of IKE_AUTH messages received from the UE with the payload type as FQDN.

default

Restores the default setting, which does not allow non-standard FQDN strings in the IDr payload of IKE_AUTH messages received from the UE with the payload type as FQDN.

You can chain multiple CA-CRLs in a single command instance.

Usage Guidelines

Use this command to configure the system to skip the syntax check for the IDr payload in IKE_AUTH messages received from the UE with the payload type as FQDN. This allows non-standard FQDN strings such as APN names in the IDr payload.

Example

The following command configures the system to allow non-standard FQDN strings in the IDr payload of IKE_AUTH messages received from the UE with the payload type as FQDN:

`allow-custom-fqdn-idr`

authentication

Configures the gateway and subscriber authentication methods to be used by this crypto template.

Product

All IPSec-related services

Privilege

Security Administrator

Syntax Description

`authentication` { **`eap-profile`** *`name`* [**`second-phase eap-profile`** *`name`*] | **`local`** { **`certificate`** | **`pre-shared-key`** { **`encrypted key`** *`value`* | **`key`** *`clear_text`* } } | **`min-key-size`** *`min_key_size`* | **`pre-shared-key`** { **`encrypted key`** *`value`* | **`key`** *`clear_text`* [**`second-phase eap-profile`** *`name`*] } | **`remote`** { **`certificate`** | **`eap-profile`** *`name`* [**`second-phase eap-profile`** *`name`*] | **`pre-shared-key`** { **`encrypted key`** *`value`* | **`key`** *`clear_text`* [**`second-phase eap-profile`** *`name`*] } } }

```
no authentication local { certificate |  min-key-size | pre-shared-key }
default authentication  min-key-size
```

default

Returns the command to its default setting.

no

Removes the authentication parameters from the configuration.

eap-profile *name* [second-phase eap-profile *name*]

Specifies that authentication is to be performed using a named Extensible Authentication Protocol (EAP) profile. *name* is an alphanumeric string of 1 through 127 characters. Entering this keyword places the CLI in the EAP Authentication Configuration Mode.

The **second-phase eap-profile** *name* is only required for installations using multiple authentications. *name* must be an alphanumeric string of 1 through 127 characters.

local { certificate | pre-shared-key { encrypted key *value* | key *clear_text* }

Specifies the local authentication method required for services using the crypto template.

certificate: Specifies that the certificate method of authentication must be used for services using the crypto template.

min-key-size: Sets minimum certificate key size. *min_key_size* must be an integer between 255 to 8192. Default is 255.

pre-shared-key { encrypted key *value* **|** **key** *clear_text* **}**: Specifies that a pre-shared key is to be used for services using the crypto template. **encrypted key** *value* configures an encrypted pre-shared key used for authentication. *value* must be an alphanumeric string of 16 through 255 characters for releases prior to 15.0, or 15 through 444 characters for release 15.0 and higher. **key** *clear_text* configures a clear text pre-shared key used for authentication. *clear_text* must be an alphanumeric string of 1 through 255 characters.

pre-shared-key { encrypted key *value* | key *clear_text* }

Specifies that a pre-shared key is to be used for services using the crypto template.

encrypted key *value*: Specifies that the pre-shared key used for authentication is encrypted. *value* must be an alphanumeric string of 1 through 255 characters for releases prior to 15.0, or 15 through 444 characters for release 15.0 and higher.

key *clear_text*: Specifies that the pre-shared key used for authentication is clear text. *clear_text* must be an alphanumeric string of 1 through 255 characters.

remote { certificate | eap-profile *name* [second-phase eap-profile *name*] | pre-shared-key { encrypted key *value* | key *clear_text* }

Specifies the remote authentication method required for services using the crypto template.

certificate: Specifies that the certificate method of remote authentication must be used for services using the crypto template.

eap-profile *name* **[second-phase eap-profile** *name* **]**: Specifies that remote authentication is to be performed using a named EAP profile. *name* must be an alphanumeric string of 1 through 127 characters. Entering this keyword places the CLI in the EAP Authentication Configuration Mode.

The **second-phase eap-profile** *name* is only required for installations using multiple authentications. *name* must be an alphanumeric string of 1 through 127 characters.

pre-shared-key { encrypted key *value* **| key** *clear_text* **}**: Specifies that a pre-shared key is to be used for services using the crypto template. **encrypted key** *value* configures an encrypted pre-shared key used for authentication. *value* must be an alphanumeric string of 1 through 255 characters for releases prior to 15.0, or 15 through 444 characters for release 15.0 and higher. **key** *value* configures a clear text pre-shared key used for authentication. *clear_text* must be an alphanumeric string of 1 through 255 characters.

Usage Guidelines

Use this command to specify the type of authentication performed for subscribers or gateways attempting to access the service using this crypto template.

Entering the **authentication eap-profile** command results in the following prompt:

```
[context_name]hostname(cfg-crypto-tmpl-eap-key)#
```

EAP Authentication Configuration Mode commands are defined in the *EAP Authentication Configuration Mode Commands* chapter.

Example

The following command enables authentication via an EAP profile named *eap23* for subscribers using the service with this crypto template:

```
authentication eap-profile eap23
```

blockedlist

Enables the use of a blockedlist (access denied) file to be used by a security gateway.

Product

All products supporting IPSec blockedlisting

Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege

Security Administrator

Syntax Description

In releases prior to StarOS 21.26:

```
[ no ] blacklist
```

From StarOS 21.26 and later releases:

```
[ no ] blockedlist
```

no

Disables the use of a blacklist.

Usage Guidelines

Enable the use of a previously created blockedlist to deny access to prohibited peers via a security gateway.

A blockedlist is a list or register of entities that are being denied a particular privilege, service, mobility, access or recognition. With blockedlisting , any peer is allowed to connect as long as it does not appear in the list.

Each entry in the blockedlist file should contain the ID type so that the validation is performed for that ID type. In every entry, the ID type and ID value should be separated by a space. Only DOS and UNIX file formatting are supported. For additional information, refer to the *System Administration Guide*.

Example

In releases prior to StarOS 21.26:

The following command enables use of a blacklist:

```
blacklist
```

ca-certificate list

Used to bind an X.509 Certificate Authority (CA) certificate to a crypto template.

Product

All IPSec-related services

Privilege

Security Administrator, Administrator

Syntax Description

```
ca-certificate list ca-cert-name name[ ca-cert-name  name ] [ ca-cert-name
  name ] [ ca-cert-name  name ] [ ca-cert-name  name ]
no ca-certificate
```

no

Unbinds the ca-certificate(s) bound to the crypto template.

ca-cert-name *name*

Binds the named X.509 Certificate Authority (CA) root certificate to a crypto template. *name* is an alphanumeric string of 1 through 129 characters.

You can chain multiple certificates (maximum 4) in a single command instance.

Usage Guidelines

Used to bind an X.509 CA certificate to a template.

Example

Use the following example to add a CA certificate named *CA_list1* to a list:

```
ca-certificate list CA_list1
```

ca-crl list

Binds one or more Certificate Authority-Certificate Revocation Lists (CA-CRLs) to this crypto template.

Product

All IPSec-related services

Privilege

Security Administrator

Syntax Description

```
ca-crl list ca-crl-name name [ ca-crl-name name ]  [ ca-crl-name name ]  [
ca-crl-name name ]  [ ca-crl-name name ]
no ca-crl
```

no

Removes the CA-CRL configuration from this template.

ca-crl-name *name*

Specifies the CA-CRL to associate with this crypto template. *name* must be the name of an existing CA-CRL expressed as an alphanumeric string of 1 through 129 characters. Multiple lists (maximum 4) can be configured for a crypto template.

You can chain multiple CA-CRLs in a single command instance.

Usage Guidelines

Use this command to associate a CA-CRL name with this crypto template.

CA-CRLs are configured in the Global Configuration Mode. For more information about configuring CA-CRLs, refer to the **ca-crl name** command in the *Global Configuration Mode Commands* chapter.

Example

The following example binds CA-CRLs named *CRL-5* and *CRL-7* to this crypto template:

```
ca-crl list ca-crl-name CRL-5 ca-crl-name CRL-7
```

certificate

Used to bind a single X.509 trusted certificate to a crypto template.

Product

All IPSec-related services

Privilege

Security Administrator

Syntax Description

```
certificate name [ validate ]
no certificate [ validate ]
```

no

Removes any applied certificate or prevents the certificate from being included in the Auth Exchange response payload.

name

Specifies the name of a X.509 trusted certificate to bind to a crypto template. *name* is an alphanumeric string of 1 through 129 characters.

validate

Enable validations for the self-certificate.

Usage Guidelines

Can be used to bind an X.509 certificate to a template, or include or exclude it from the Auth Exchange response payload.

Example

Use the following example to prevent a certificate from being included in the Auth Exchange payload:

```
no certificate
```

configuration-payload

This command is used to configure mapping of the configuration payload attributes.

Product

All IPSec-related services

Privilege

Security Administrator

Syntax Description

```
configuration-payload private-attribute-type { imei integer | p-cscf-v4
v4_value | p-cscf-v6 v6_value }
[ no | default ] configuration-payload private-attribute-type { imei |
p-cscf-v4 | p-cscf-v6 }
```

no

Removes mapping of the configuration payload attributes.

default

Restores the defuat value for mapping of the configuration payload attributes.

private-attribute-type

Defines the private payload attribute.

imei *integer*

Defines an International Mobile Equipemnt Identity number as an integer from 16384 to 32767.

p-cscf-v4 *v4_value*

Defines the IPv4 pcscf payload attribute value. Default value is 16384.

v4_value is an integer from 16384 to 32767.

p-cscf-v6 *v6_value*

Defines IPv6 pcscf payload attribute value. Default value is 16390.

v6_value is an integer from 16384 to 32767.

Usage Guidelines

Use this command to configure mapping of the configuration payload attributes.

Example

The following command configures the mapping of the configuration payload attributes p-cscf-v6 to 17001.

```
configuration-payload private-attribute-type p-cscf-v6 17001
```

control-dont-fragment

Controls the Don't Fragment (DF) bit in the outer IP header of the IPSec tunnel data packet.

Product

All IPSec-related services

Privilege

Security Administrator

Syntax Description

```
control-dont-fragment { clear-bit | copy-bit | set-bit }
```

clear-bit

Clears the DF bit from the outer IP header (sets it to 0).

copy-bit

Copies the DF bit from the inner IP header to the outer IP header. This is the default action.

set-bit

Sets the DF bit in the outer IP header (sets it to 1).

Usage Guidelines

A packet is encapsulated in IPSec headers at both ends. The new packet can copy the DF bit from the original unencapsulated packet into the outer IP header, or it can set the DF bit if there is not one in the original packet. It can also clear a DF bit that it does not need.

Example

The following command sets the DF bit in the outer IP header:

```
control-dont-fragment set-bit
```

dns-handling

Adds a custom option to define the ways a DNS address is returned based on proscribed circumstances described below.

Product

PDIF

Privilege

Security Administrator

Syntax Description

```
[ default ] dns-handling { custom | normal }
```

default

Configures the default condition as **normal**. By default, PDIF always returns the DNS address in the config payload in the second authentication phase if one is received from either the configuration or the HA.

dns-handling custom

Configures the PDIF to behave as described in the Usage section below.

dns-handling normal

This is the default action. The service always returns the DNS address in the config payload in the second authentication phase if one is received from either the configuration or the HA.

Usage Guidelines

During IKEv2 session setup, MS may or may not include INTERNAL_IP4_DNS in the Config Payload (CP). PDIF may obtain one or more DNS addresses for the subscriber in DNS NVSE from a proxy-MIP Registration Reply message. If Multiple Authentication is used, these DNS addresses may be also received in Diameter AVPs during the first authentication phase, or in RADIUS attributes in the Access Accept messages during the second authentication phase.

In **normal** mode, by default PDIF always returns the DNS address in the config payload in the second authentication phase if one is received from either the configuration or the HA.

In **custom** mode, depending on the number of INTERNAL_IP4_DNS, PDIF supports the following behaviors:

- If MS includes no INTERNAL_IP4_DNS in Config Payload: PDIF does not return any INTERNAL_IP4_DNS option to MS, whether or not PDIF has received one in DNS NVSE from HA or from local configurations.
- If MS requests one or more INTERNAL_IP4_DNS(s) in Config Payload, and if P-MIP NVSE doesn't contain any DNS address or DNS address not present in any config, PDIF omits INTERNAL_IP4_DNS option to MS in the Config Payload.
- And if P-MIP NVSE includes one DNS address (a.a.a.a / 0.0.0.0), then PDIF sends one INTERNAL_IP4_DNS option in Config Payload back to the MS.
- If the Primary DNS is a.a.a.a and the Secondary DNS is 0.0.0.0, then a.a.a.a is returned (only one instance of DNS attribute present in the config payload).
- If the Primary DNS is 0.0.0.0 and the Secondary DNS is a.a.a.a, then a.a.a.a is returned (only one instance of DNS attribute present in the config payload). PDIF does not take 0.0.0.0 as a valid DNS address that can be assigned to the MS.

- And if P-MIP NVSE includes two DNS addresses (a.a.a.a and b.b.b.b) or configurations exists for these two addresses, then PDIF sends two INTERNAL_IP4_DNSs in the CP for the MS (typically known as primary and secondary DNS addresses).

Example

The following configuration applies the **custom** dns-handling mode:

```
dns-handling custom
```

dos cookie-challenge notify-payload

Configure the cookie challenge parameters for IKEv2 INFO Exchange notify payloads for the given crypto template.

Product

All IPSec-related services

Privilege

Security Administrator

Syntax Description

```
dos cookie-challenge notify-payload [ half-open-sess-count start integer
stop integer]
[ default | no ] cookie-challenge detect-dos-attack
```

default

Default is to disabled condition.

no

Prevents Denial of Service cookie transmission. This is the default condition.

half-open-sess-count start *integer* stop *integer*

The **half-open-sess-count** is the number of half-open sessions per IPSec manager.

A session is considered half-open if a PDIF has responded to an IKEv2 INIT Request with an IKEv2 INIT Response, but no further message was received on that particular IKE SA.

- **start** *integer*: Starts when the current half-open-sess-count exceeds the start count. The start count is an integer from 0 to 100000.
- **stop** *integer*: Stops when the current half-open-sess-count drops below the stop count. The stop count number is an integer from 0 to 100000. It is always less than or equal to the start count number

Important The start count value 0 is a special case whereby this feature is always enabled. In this event, both **start** and **stop** must be 0.

Usage Guidelines This feature (which is disabled by default) helps prevent malicious Denial of Service attacks against the server by sending a challenge cookie. If the response from the sender does not incorporate the expected cookie data, the packets are dropped.

Example

The following example configures the cookie challenge to begin when the half-open-sess-count reaches 50000 and stops when it drops below 20000:

```
dos cookie-challenge notify-payload half-open-sess-count start 50000 stop
 20000
```

ecn

This command enables explicit congestion notification (ECN) in normal mode or compatible mode for the IPsec tunnel over the SWu interface.

Product ePDG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Crypto Template Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(crf-crypto-tmp1-ikev2-tunnel)#
```

Syntax Description **[no] ecn**

no

Enables ECN in compatible mode for IPsec tunnel over SWu interface. The default mode is the compatible mode, supported for backward compatibility.

ecn

Specifies ECN over IPsec tunnel in normal mode.

Usage Guidelines Use this command to enable ECN in normal mode or compatible mode for the IPsec tunnel over SWu interface.

Example

The following command enables ECN in normal mode for the IPsec tunnel:

```
ecn
```

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.

identity local

Configures the identity of the local IPSec Client (IKE ID).

Product All Security Gateway products



Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege Security Administrator

Syntax Description

```
identity local id-type type id name
no identity local
```

no

Resets the ID to the IP address of the interface to which the crypto template is associated (type = IPv4 or IPv6).

id-type *type*

Configures the IKE identity that the local client uses when authenticating to the gateway. Valid values are:

- **der-ans1-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).

id *name*

Specifies the identifier for the local IKE client as an alphanumeric string of 1 through 127 characters.

Usage Guidelines

Use this command to configure the identity of the local IPSec Client.

Example

The following command configures the local IPSec Client.

```
identity local id-type der-asn1-dn id system14
```

ikev2-ikesa

Configures parameters for the IKEv2 IKE Security Associations within this crypto template.

Product

All IPSec-related services

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(crf-crypto-tmp1-ikev2-tunnel)#
```

Syntax Description

ikev2-ikesa { allow-empty-ikesa | cert-sign { pkcs1.5 | pkcs2.0 } | configuration-attribute p-cscf-v6 { iana | private } length { 16 | 17 } | emergency { keepalive [interval *interval* **] timeout** *seconds* **num-retry** *val* **} | fragmentation | idi** *peer_idi_value* **{ common-id | request-eap-identity } | imsi-privacy auth-imsi| ignore-notify-protocol-id | ignore-rekeying-requests | keepalive-user-activity | max-retransmissions** *number* **| mobike [cookie-challenge] | policy { congestion-rejection { notify-status-value** *value* **| notify-error-value** *value* **} | error-notification [invalid-major-version] [invalid-message-id [invalid-major-version | invalid-syntax]] | invalid-syntax [invalid-major-version] | use-rfc5996-notification } | rekey [disallow-param-change] | retransmission-timeout** *msec* **| setup-timer** *sec* **| transform-set list** *name1 name2 name3 name4 name5 name6* **}**

```
default ikev2-ikesa { allow-empty-ikesa | cert-sign |
configuration-attribute p-cscf-v6 { iana | private } length | fragmentation
 | ignore-notify-protocol-id | ignore-rekeying-requests |
keepalive-user-activity | max-retransmissions | mobike | policy
error-notification | rekey [ disallow-param-change ] |
retransmission-timeout | setup-timer }

no ikev2-ikesa { allow-empty-ikesa | auth-method-set | fragmentation  |
idi  peer_idi_value | ignore-notify-protocol-id | ignore-rekeying-requests
| keepalive-user-activity | list name | mobike | policy error-notification
 | rekey }| imsi-privacy auth-imsi
```

default

Restores the configuration to its default value.

no

Disables a previously enabled parameter.

allow-empty-ikesa

Default is not to allow-empty-ikesa. Activate to have the IKEv2 stack keep the IKE SA when all the Child SAs have been deleted.

cert-sign { pkcs1.5 | pkcs2.0 }

Specifies the certificate sign to be used. Default: pkcs1.5

pkcs1.5: Use the Public-Key Cryptography Standards (PKCS) version 1.5, RSA Encryption Standard.

pkcs2.0:: Use the PKCS version 2.0, RSA Encryption Standard.

configuration-attribute p-cscf-v6 { iana | private } length { 16 | 17 }

Specifies the P-CSCF IPv6 configuration attribute length for both IANA and private attribute values. As per RFC 7651, the configuration attribute length for IANA is 16 bytes.

Default (iana): 16 bytes

Default (private): 17 bytes

emergency { keepalive [interval *interval*] timeout *seconds* num-retry *val* }

Configures emergency call related parameters.

Keepalive : Configures Keepalive Functionality (Dead Peer Detection) to be enabled for all emergency Security Associations derived from this Crypto Template and this will override generic keep alive configuration for emergency calls.

interval : The number of seconds which must elapse during which no traffic is received from the given IKE_SA peer or any CHILD_SAs derived from the IKE_SA for Dead Peer Detection to be initiated (Default: 3). - integer 2..3600

timeout : Configures the Keepalive (Dead Peer Detection) Timeout in seconds. This value configures the number of seconds which must elapse after a Keepalive has been sent, and no response has been received before another keepalive is sent.

seconds : The number of seconds which must elapse after a Keepalive has been sent, and no response has been received, before another Keepalive is send. Default is 3 seconds and the Interval should be between 2 and 3600 seconds.

num-retry : Configure the number of Keepalive (Dead Peer Detection) Retry attempts. If Keepalive (Dead Peer Detection) has been initiated this value configures the number of retry attempts which will be made if no response is received from the peer, before the peer is declared dead.

val : The number of retry attempts which will be made if no response is received from the peer before the peer is declared dead Default is 2 seconds and the Interval should be between 1 and 30 seconds.

fragmentation

Enables IKESA fragmentation (Tx) and re-assembly (Rx).

Default: IKESA fragmentation and re-assembly is allowed.

idi *peer_idi_value* { common-id | request-eap-identity }

Specifies the IDI related configuration to match IDI from peer which enables the ePDG to request the real identity using EAP-Identity Request. *peer_idi_value* is a string of 1 through 127 characters.

request-eap-identity: Requests the EAP-Identity from peer.

common-id: Requests the Common IDi from peer.

imsi-privacy

Configures IMSI Privacy related parameters.

auth-imsi

Enables IKESA to use IMSI for AUTH calculation for IMSI Privacy.

.

ignore-notify-protocol-id

Ignores IKEv2 Informational Exchange Notify Payload Protocol-ID values for strict RFC 4306 compliance.

ignore-rekeying-requests

Ignores received IKE_SA Rekeying Requests.

keepalive-user-activity

Default is no keepalive-user-activity. Activate to reset the user inactivity timer when keepalive messages are received from peer.

max-retransmissions *number*

Specifies the maximum number of retransmissions of an IKEv2 IKE Exchange Request if a response has not been received. *number* must be an integer from 1 through 8. Default: 5

mobike [cookie-challenge]

IKEv2 Mobility and Multihoming Protocol (MOBIKE) allows the IP addresses associated with IKEv2 and tunnel mode IPSec Security Associations to change. A mobile Virtual Private Network (VPN) client could use MOBIKE to keep the connection with the VPN gateway active while moving from one address to another. Similarly, a multi-homed host could use MOBIKE to move the traffic to a different interface if, for instance, the one currently being used stops working.

Default: Disabled

cookie-challenge: Use this keyword to enable the return routability check. The Gateway performs a return routability check when MOBIKE is enabled along with this keyword. A return routability check ensures that the other party can receive packets at the claimed address. Default: Disabled

policy { congestion-rejection { notify-status-value *value* | notify-error-value *value* } | error-notification [invalid-major-version] [invalid-message-id [invalid-major-version | invalid-syntax]] | invalid-syntax [invalid-major-version] | use-rfc5996-notification }

Specifies the default policy for generating an IKEv2 Invalid Message ID error when PDIF receives an out-of-sequence packet.

congestion-rejection: Sends an Error Notify Message to the MS as a reply to an IKE_SA_INIT Exchange when no more IKE_SA sessions can be established.

notify-status-value *value*: Notify Message will be sent to MS as a reply to an IKE_SA_INIT Exchange when no more IKE_SA sessions can be established. *value* is RFC 4306 IKEv2 Private Use Status Range - integer 40960 through 65535.

notify-error-value *value*: Notify Message will be sent to MS as a reply to an IKE_SA_INIT Exchange when no more IKE_SA sessions can be established. *value* is RFC 4306 IKEv2 Private Use Error Range - integer 8192 through 16383.

error-notification: Sends an Error Notify Message to the MS for Invalid IKEv2 Exchange Message ID and Invalid IKEv2 Exchange Syntax for the IKE_SA_INIT Exchange.

invalid-major-version: Sends an Error Notify Message for Invalid Major Version

invalid-message-id: Sends an Error Notify Message for Invalid IKEv2 Exchange Message ID.

invalid-syntax: Sends an Error Notify Message for Invalid IKEv2 Exchange Syntax.

use-rfc5996-notification: Enable sending and receive processing for RFC 5996 notifications - TEMPORARY_FAILURE and CHILD_SA_NOT_FOUND

rekey [disallow-param-change]

Specifies if IKESA rekeying should occur before the configured lifetime expires (at approximately 90% of the lifetime interval). Default is not to re-key.

The **disallow-param-change** option prevents changes in negotiation parameters during rekey.

retransmission-timeout *msec*

Specifies the timeout period (in milliseconds) before a retransmission of an IKEv2 IKE exchange request is sent (if the corresponding response has not been received). *msec* must be an integer from 300 to 15000. Default: 500

setup-timer *sec*

Specifies the number of seconds before a IKEv2 IKE Security Association that is not fully established is terminated. *sec* must be an integer from 1 through 3600. Default: 16

transform-set list *name1*

Specifies the name of a context-level configured IKEv2 IKE Security Association transform set. *name1 ...name6* must be an existing IKEv2 IKESA Transform Set expressed as an alphanumeric string of 1 through 127 characters.

The transform set is a space-separated list of IKEv2-IKESA SA transform sets to be used for deriving IKEv2 IKE Security Associations from this crypto template. A minimum of one transform-set is required; maximum configurable is six.

no ikev2-ikesa imsi-privacy auth-imsi

Reverts to default of IKESA to use IDI for AUTH calculation for IMSI Privacy.

Usage Guidelines

Use this command to configure parameters for the IKEv2 IKE Security Associations within this crypto template.

Example

The following command enables IKESA fragmentation and re-assembly:

```
ikev2-ikesa fragmentation
```

The following command configures the maximum number of IKEv2 IKESA request re-transmissions to *7*:

```
ikev2-ikesa max-retransmissions 7
```

The following command configures the IKEv2 IKESA request retransmission timeout to *400* milli seconds:

```
ikev2-ikesa retransmission-timeout 400
```

The following command configures the IKEv2 IKESA list, consisting of a transform set named as *ikesa43*:

```
ikev2-ikesa transform-set list ikesa43
```

ikev2-ikesa ddos

Configures distributed denial of service (DDoS) mitigation parameters for the IKEv2 IKE Security Associations within this crypto template.

Product

ePDG

HeNBGW

HNBGW

WSG

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(crf-crypto-tmp1-ikev2-tunnel)#
```

Syntax Description

ikev2-ikesa ddos { decrypt-fail-count *failure_count* **| half-open-sa-timer** *half_open_timer_duration* **| ikev2-req-rate** *ikev2_req_rate_count* **[interval** *interval* **]| max-cert-size** *cert_size* **| message-queue-size** *queue_size* **| rekey-rate** *rekey_rate_value* **}**

{ default | no } ikev2-ikesa ddos { decrypt-fail-count | half-open-sa-timer | ikev2-req-rate | max-cert-size | message-queue-size | rekey-rate }

default

Restores the configuration to its default value.

no

Disables a previously enabled configuration.

decrypt-fail-count *failure_count*

Specifies the maximum tolerable consecutive IKE_AUTH message decryption failure count. During session establishment, if IKE_AUTH decryption failure exceeds the configured threshold, the IKEv2 IKE SA tunnel is cleared. If IKE_AUTH decryption failure exceeds the configured threshold after the session is established, alarms are triggered.

Default: 30

failure_count must be an integer between 1 and 100.

half-open-sa-timer *half_open_timer_duration*

Specifies the half-open IKE SA timeout duration. The half-open IKE SA timer starts when an IKE_SA_INIT request is received. If an IKE_AUTH message is not received before the timer expires, the half-open IKEv2 IKE SA is cleared.

Default: 60

half_open_timer_duration must be an integer between 1 and 1800.

ikev2-req-rate *ikev2_req_rate_count* [interval *interval*]

ikev2-req-rate *ikev2_req_rate_count*: Configures the maximum number of IKEv2 requests allowed per configured interval. *ikev2_req_rate_count* must be an integer from 1 to 3000.

Default: 10

interval *interval* : Configures the interval for monitoring IKEv2 requests. *interval* must be an integer from 1 to 300.

Default: 1 second

max-cert-size *cert_size*

Specifies the maximum certificate size for IKE SA. Use this keyword to detect bad certificates from illegitimate URLs in earlier stages, and thus avoid downloading large certificates.

Default: 2048 bytes

cert_size must be an integer between 512 and 8192.

message-queue-size *queue_size*

Specifies the queue size for incoming IKE messages per IKE SA. When the incoming queued IKE messages (per IKE SA) exceeds the specified limit, the IKE messages exceeding the limit are dropped.

Default: 20

queue_size must be an integer between 1 and 50.

rekey-rate *rekey_rate_value*

Specifies the rate at which the rekey request will be processed per second. When the specified number of Child SA rekey requests per second is exceeded, a TEMPORARY_FAILURE notification will be sent to the peer to indicate that the peer must slow down their requests.

Default: 5

rekey_rate_value must be an integer between 1 and 50.

Usage Guidelines

Use this command to configure parameters for Distributed Denial of Service (DDoS) mitigation for the IKEv2 IKE Security Associations within this crypto template.

Example

The following command configures the half-open IKE SA timeout duration to *300* seconds:

```
ikev2-ikesa ddos half-open-sa-timer 300
```

ikev2-ikesa dscp

Configures the Differentiated Services Code Point (DSCP) value in the IPv4 and IPv6 headers of the IKEv2 packets sent to the peer for this crypto template.

Product

ePDG

HeNBGW

HNBGW

SecGW

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(crf-crypto-tmp1-ikev2-tunnel)#
```

Syntax Description

ikev2-ikesa dscp *dscp_hex_value*

default ikev2-ikesa dscp

default

Restores the configuration to its default value.

dscp *dscp_hex_value*

Specifies the DSCP value in the IKEv2 packets sent to the peer.

Default: 0x00

dscp_hex_value must be an hexa-decimal value between 0x00 and 0x3F.

Usage Guidelines

Use this command to configure the Differentiated Services Code Point (DSCP) value in the IPv4 and IPv6 headers of the IKEv2 packets sent to the peer for this crypto template.

Example

The following command configures the DSCP value to *0x2A*:

ikev2-ikesa dscp 0x2A

ip

Configures IPv4 related information.

Product

All IPSec-related services

ePDG

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(crf-crypto-tmp1-ikev2-tunnel)#
```

Syntax Description

ip { fragment { inner | outer } | ikev2-mtu *mtu_size* **| mtu** *size* **}**
default ip { fragment | ikev2-mtu | mtu }

default

Sets / Restores default value assigned for IPv4 related information. The default value for fragment is outer. The default value for ikev2-mtu is 1384. The default value for mtu is 1438.

fragment { inner | outer }

Configures the fragment type when User Payload is IPv4 type and DF bit not set.

Default: outer

inner: Fragments the IPv4 payload and encapsulate in the IPSec tunnel.

outer: Fragment to happen after the IPSec encapsulation.

ikev2-mtu *mtu_size*

Configures MTU size of the IKEv2 Payload for IPv4 tunnel.

mtu_size is an integer between 460 and 1932.

mtu *size*

Configures MTU of the User Payload for IPv4 tunnel.

size is an integer between 576 and 2048.

Usage Guidelines

Use this command to configure IPv4 related information for given ePDG services configured on this system.

For IPSec, use this command to set the Maximum Transmission Unit (MTU) size for the IKEv2 payload over IPv4 tunnels.

Example

The following command sets the IKEv2 MTU size to 1500:

```
ip ikev2-mtu 1500
```

The following command sets the MTU size to 1500:

```
ip mtu 1500
```

ipv6

Configures the MTU (Maximum Transmission Unit) of the user payload for IPv6 tunnels in bytes.

Product

All IPSec-related services

ePDG

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(crf-crypto-tmp1-ikev2-tunnel)#
```

Syntax Description

For ePDG:

ipv6 mtu *size*
default ipv6 mtu

For IPSec:

ipv6 ikev2-mtu *mtu-size*
default ipv6 ikev2-mtu

default

Sets the IPv6 tunnel MTU to its default size.

mtu *size*

Specifies the MTU size of a packet to accommodate IPSec headers added to a packet.

Default:1422

size must be an integer from 1280 through 2048.

ikev2-mtu *mtu_size*

Configures MTU size of the IKEV2 Payload for IPv6 tunnel.

Default: 1364

mtu_size must be an integer from 1144 through 1912.

Usage Guidelines

For ePDG, use this command to increase the MTU size of a packet to accommodate IPSec headers added to a packet and thus avoid sending an ICMP Fragmentation Needed packet.

For IPSec, use this command to set the Maximum Transmission Unit (MTU) size for the IKEv2 payload over IPv6 tunnels.

Example

The following command sets the IKEv2 MTU size to 1500:

```
ipv6 ikev2-mtu 1500
```

The following command sets the MTU size to 1800:

```
ipv6 mtu 1800
```

keepalive

Configures keepalive or dead peer detection for security associations used within this crypto template.

Product

All products supporting IPSec

Privilege

Security Administrator

Syntax Description

keepalive [interval *sec* **]**
default keepalive [interval]
no keepalive

no

Disables keepalive messaging.

interval *sec*

Specifies the amount of time (in seconds) that must elapse before the next keepalive request is sent. *sec* must be an integer from 10 through 3600. Default: 10

Usage Guidelines

Use this command to set parameters associated with determining the availability of peer servers.

Example

The following command sets a keepalive interval to three minutes (*180* seconds):

```
keepalive interval 180
```

max-childsa

Defines a soft limit for the number of child Security Associations (SAs) per IKEv2 policy.

Product

All products supporting IPSEcv2

Privilege

Security Administrator

Syntax Description

```
max-childsa integer [ overload-action { ignore | terminate } ]
```

max-childsa *integer*

Specifies a soft limit for the maximum number of Child SAs per IKEv2 policy as an integer from 1 to 4 for releases prior to 15.0, or 1 to 5 for 15.0 and higher. Default = 2.

overload-action { ignore | terminate }

Specifies the action to be taken when the specified soft limit for the maximum number of Child SAs is reached. The options are:

- **ignore**: The IKEv2 stack ignores the specified soft limit for Child SAs.
- **terminate**: The IKEv2 stack rejects any new Child SAs if the specified soft limit is reached.

Usage Guidelines

Two maximum Child SA values are maintained per IKEv2 policy. The first is a system-enforced maximum value, which is four Child SAs per IKEv2 policy. The second is a configurable soft maximum value, which can be a value between one and four. This command defines the soft limit for the maximum number of Child SAs per IKEv2 policy.

Example

The following command specifies a soft limit of four Child SAs with the overload action of terminate.

```
max-childsa 4 overload-action terminate
```

nai

Configures the Network Access Identifier (NAI) parameters to be used for the crypto template IDr (recipient's identity).

Product



Important This command is deprecated from 15.0 and later releases.

All Security Gateway products

Privilege

Security Administrator

Syntax Description

```
nai { idr name [ id-type { der-asn1-dn | der-asn1-gn | fqdn | ip-addr |
key-id | rfc822-addr } ] | use-received-idr }
default nai idr
no nai { idr | use-received-idr }
```

default

Configures the default command **no nai idr**. As a result, the default behavior is for the PDIF-service IP address to be sent as the IDr value of type ID_IP_ADDR.

no

no nai idr configures the value whereby the service IP address is sent as the IDr value with the type ID_IP_ADDR. This is the default condition.

idr *name*

Specifies the name of the IDr crypto template as an alphanumeric string of 1 through 79 characters.

id-type { der-asn1-dn | der-asn1-gn | 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)
- **der-asn1-gn**: configures NAI Type DER_ASN1_GN (Distinguished Encoding Rules, ASN.1 encoding, General 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).

use-received-idr

Specifies that the received IDr be used in the crypto template.

Usage Guidelines The configured IDr is sent to the MS in the first IKEv2 AUTH response.

Example

The following command configures the NAI IDr to the default condition.

```
default naiidr idr
```

natt

Configures Network Address Translation - Traversal (NAT-T) for all security associations associated with this crypto template. This feature is disabled by default.



Important IKEv2 ACL with NAT-T is not supported.

Product All Security Gateway products

Privilege Security Administrator

Syntax Description

```
[ default | no ] natt [ include-header ] [ send-keepalive [ idle-interval
 idle_secs ] [ interval interval_secs ] ]
```

default

Disables NAT-T for all security associations associated with this crypto template.

no

Disables NAT-T for all security associations associated with this crypto template.

include-header

Includes the NAT-T header in IPSec packets.

send-keepalive [idle-interval *idle_secs*] [interval *interval_secs*]

Sends NAT-Traversal keepalive messages.

idle-interval *idle_secs*: Specifies the number of seconds that can elapse without sending NAT keepalive packets before sending NAT keepalive packets is started. *idle_secs* is an integer from 20 to 86400. Default: 60.

interval *interval_secs*: Specifies the number of seconds between the sending of NAT keepalive packets. *interval_secs* is an integer from 60 to 86400. Default: 240.

Usage Guidelines Use this command to configure NAT-T for security associations within this crypto template.

Example

The following command disables NAT-T for this crypto template:

```
no natt
```

notify-payload

This command configures the parameters to be sent in NOTIFY payload.

Product

All products supporting IPSec OCSP

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(crf-crypto-tmp1-ikev2-tunnel)#
```

Syntax Description

```
notify-payload { device-id | error-message-type { network-permanent |
network-transient-major | network-transient-minor | ue }| pdn-type-allowed
 | base value }

default notify-payload { device-id | error-message-type { network-permanent
 | network-transient-major | network-transient-minor | ue } base }

no notify-payload device-id
```

default

Sets / restores default value assigned for the parameters to be sent in NOTIFY payload.

no

If previously configured, removes the configuration.

device-id

Enables ePDG to request for the IMEI or IMEI SV information using the DEVICE_IDENTITY notify payload in the IKE_AUTH_RESP message from the UE, if the UE does not share this information in the first IKE_AUTH_REQ message in the configuration attributes.

Default: Enabled

error-message-type

This command configures the type of notify error message.

Error Categories:

- **network-permanent**: Configures the value for permanent network errors. Default is 11000.

- **network-transient-major**: Configures the value for major transient network errors. Default is 10500.
- **network-transient-minor**: Configures the value for minor transient network errors. Default is 10000.
- **ue**: Configures the value for UE related errors. Default is 9000.

pdn-type-allowed

This command enables the IP type notification.

base *value*: Configures the base value for the chosen error category. Only private range supported 8192-16383.

value must be an integer between 8192 and 16383.

Usage Guidelines

Use this command to configure the parameters to be sent in NOTIFY payload.

Example

The following command configures the notify payload parameter **error-message-type network-transient-minor base** to value 10000.

```
notify-payload error-message-type network-transient-minor base 10000
```

ocsp

Enables use of Online Certificate Status Protocol (OCSP) from a crypto template. OCSP provides a facility to obtain timely information on the status of a certificate.

Product

All products supporting IPSec

Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege

Security Administrator

Syntax Description

```
ocsp [ nonce | responder-address ipv4_address [ port port_value ] ]
no ocsp [ nonce | responder-address [ port ] ]
default ocsp [ nonce ]
```

no

Disables the use of OCSP.

default

Restores the default value assigned for ocsp nonce.

nonce

Enables sending nonce (unique identifier) in OCSP requests.

responder-address *ipv4_address*

Configures the OCSP responder address that is used when absent in the peer (device) certificate.

ipv4_address is an IPv4 address specified in dotted decimal format.

port *port_value*

Configures the port for OCSP responder.

port_value is an integer value between 1 and 65535. The default port is 8889.

Usage Guidelines

This command enables the use of Online Certificate Protocol (OCSP) from a crypto map/template. OCSP provides a facility to obtain timely information on the status of a certificate.

OCSP messages are exchanged between a gateway and an OCSP responder during a certificate transaction. The responder immediately provides the status of the presented certificate. The status can be good, revoked or unknown. The gateway can then proceed based on the response.

Example

The following command enables OSCP:

```
ocsp
```

payload

Creates a new, or specifies an existing, crypto template payload and enters the Crypto Template Payload Configuration Mode.

Product

All Security Gateway products

Privilege

Security Administrator

Syntax Description

```
[ no ] payload name match childsa [ match { any | ipv4 | ipv6 } ]
```

no

Removes a currently configured crypto template payload.

payload *name*

Specifies the name of a new or existing crypto template payload as an alphanumeric string of 1 through 127 characters.

match { any | ipv4 | ipv6 }

Filters IPSec Child Security Association creation requests for subscriber calls by applying the following options:

- **any**: Configures this payload to be applicable to IPSec Child Security Association requests for IPv4 and/or IPv6.

- **ipv4**: Configures this payload to be applicable to IPSec Child Security Association requests for IPv4 only.
- **ipv6**: Configures this payload to be applicable to IPSec Child Security Association requests for IPv6 only.

Usage Guidelines

Use this command to create a new or enter an existing crypto template payload. The payload mechanism is a means of associating parameters for the Security Association (SA) being negotiated.

Two payloads are required: one each for MIP and IKEv2. The first payload is used for establishing the initial Child SA Tunnel Inner Address (TIA) which will be torn down. The second payload is used for establishing the remaining Child SAs. Note that if there is no second payload defined with home-address as the *ip-address-allocation* then no MIP call can be established, just a Simple IP call.

Currently, the only available match is for ChildSA, although other matches are planned for future releases. Omitting the second match parameter for either IPv4 or IPv6 will make the payload applicable to all IP address pools.

Crypto Template Payload Configuration Mode commands are defined in the *Crypto Template IKEv2-Dynamic Payload Configuration Mode Commands* chapter.

Example

The following command configures a crypto template payload called *payload5* and enters the Crypto Template Payload Configuration Mode:

```
payload payload5 match childsa
```

peer network

Configures a list of allowed peer addresses on this crypto template.

Product

All IPSec-related services

Privilege

Security Administrator

Syntax Description

```
peer network ip_address /mask [ encrypted pre-shared-key encrypt_key |
pre-shared-key key ]
no peer network ip_address/ mask
```

no

Removes the specified peer network IP address from this crypto template.

peer network *ip_address* [/*mask*]

Specifies the IP address of the peer network in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Maximum of four peer networks can be configured per template.

/*mask* specifies the subnet mask bits. *mask* is an integer value from 1 to 32 for IPv4 addresses and 1 to 128 for IPv6 addresses (CIDR notation).

encrypted pre-shared-key *encrypt_key*

Specifies that an encrypted pre-shared key is to be used for IPSec authentication for the address range. *encrypt_key* must be an alphanumeric string or hexadecimal sequence from 16 to 212.

pre-shared-key *key*

Specifies that a clear text pre-shared key is to be used for IPSec authentication for the address range. *key* must be an alphanumeric string or hexadecimal sequence from 1 to 32.

Usage Guidelines

Use this command to configure a list or range of allowed peer network IP addresses for this template.

Example

The following command configures a set of IP addresses with starting address of 10.2.3.4 and a bit mask of 8:

```
peer network 10.2.3.4/8
```

remote-secret-list

Enables the use of a Remote Secret List containing up to 1000 pre-shared keys.

Product

All Security Gateway products

Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege

Security Administrator

Syntax Description

```
remote-secret-list list_name
no remote-secret-list
```

no

Disables use of a Remote Secret List.

list_name

Specifies the name of an existing Remote Secret List as an alphanumeric string of 1 through127 characters.

Usage Guidelines

Enable the use of a Remote Secret List containing up to 1000 pre-shared keys.

Only one active remote-secret-list is supported per system.

For additional information, refer to the *Remote Secret List Configuration Commands* chapter of the *Command Line Interface Reference* and the *System Administration Guide*.

Example

The following command enables a remote-secret-list named *rs-list*:

remote-secret-list rs-list

server certificate

Configure server certificate for a given Crypto Template.

Product

ePDG

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic**

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(crf-crypto-tmp1-ikev2-tunnel)#

Syntax Description

server-certificate *certificate_name* **ca-certificate-list** *ca_certificate_list_name*

no server-certificate *certificate_name* [**validate**]

certificate_name

configures server certificate for a given Crypto Template, certificate name should a string of size between 1 and 128.

ca_certificate_list_name

configures server certificate list name for a given Crypto Template, certificate name should a string of size between 1 and 128.

Usage Guidelines

Use the below command to configure server certificate for a given Crypto Template:

Example

The following command configures Server Certificate 20 and CA Certificate List 10:

server-certificate *20* **ca-certificate-list** *10*

timeout

Sets the OCSP Certificate Server timeout interval in seconds. This is the interval within which the response from an external OCSP or HASH-url server should be received.

Product ePDG

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > Crypto Template Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(crf-crypto-tmp1-ikev2-tunnel)#
```

Syntax Description

```
timeout cert-server timeout_value
 default timeout cert-server
```

default

Sets / Restores default value assigned for Certificate Server timeout in seconds. Default is 20 seconds.

timeout_value

Specifies the timeout value in seconds which is an integer between 1 through 60.

Usage Guidelines Use this command to configure Certificate Server timeout in seconds.

Example

The following command configures Certificate Server timeout as 50 seconds:

```
timeout cert-server 50
```

vendor-policy

Associate a vendor policy to this crypto template.

Product ePDG

HeNBGW

HNBGW

WSG

Privilege Security Administrator

Command Modes Exec > Global Configuration > Context Configuration > Crypto Template Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(crf-crypto-tmp1-ikev2-tunnel)#
```

Syntax Description

vendor-policy *policy_name*

no vendor-policy

no

Removes association of the vendor policy to this crypto template.

policy_name

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

Usage Guidelines

Use this command to associate a vendor policy to this crypto template.

Example

The following command associates a vendor policy named *atlpcy* to this crypto template:

vendor-policy atlpcy

permitlist

Enables the use of an existing permitlist (access permitted) file by a security gateway.

Product

All products supporting IPSec permitlisting

Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege

Security Administrator

Syntax Description

In releases prior to StarOS 21.26:

[no] whitelist

From StarOS 21.26 and later releases:

[no] permitlist

no

Disables the use of a permitlist.

Usage Guidelines

Enable the use of a previously created permitlist to allow privileged peers access via a security gateway.

A permitlist is a list or register of entities that are being provided a particular privilege, service, mobility, access or recognition. With permitlisting, no peer is allowed to connect unless it appears in the list.

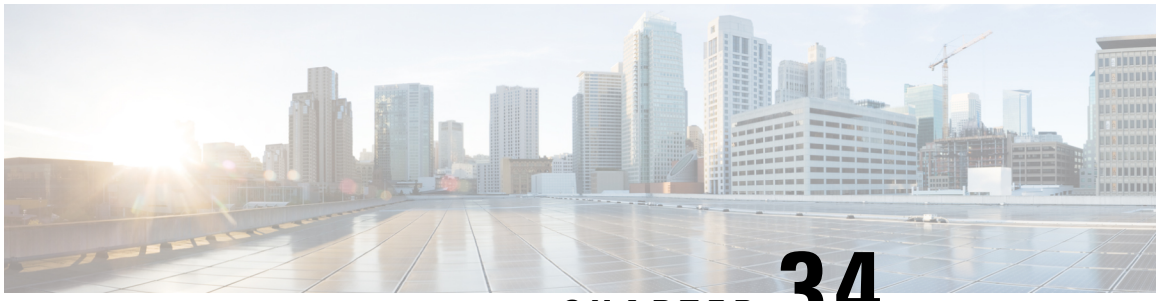
Each entry in the permitlist file should contain the ID type so that the validation is performed for that ID type. In every entry, the ID type and ID value should be separated by a space. Only DOS and UNIX file formatting are supported. For additional information, refer to the *System Administration Guide*.

Example

In releases prior to StarOS 21.26:

The following command enables the use of a whitelist:

whitelist



CHAPTER 34

Crypto Template IKEv2-Dynamic Payload Configuration Mode Commands

The Crypto Template IKEv2-Dynamic Payload Configuration Mode is used to assign the correct IPSec transform-set from a list of up to four different transform-sets, and to assign Mobile IP addresses. There should be two payloads configured. The first must have a dynamic addressing scheme from which the ChildSA gets a TIA address. The second payload supplies the ChildSA with a HoA, which is the default setting for *ip-address-allocation*.

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic > payload** *payload_name* **match childsa match { any | ipv4 | ipv6 }**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#
```

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

- end, on page 943
- exit, on page 944
- ignore-rekeying-requests, on page 944
- ip-address-allocation, on page 945
- ipsec transform-set, on page 946
- lifetime, on page 946
- maximum-child-sa, on page 947
- rekey, on page 948
- tsi , on page 949
- tsr , on page 950

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.

ignore-rekeying-requests

Ignores CHILD SA rekey requests from the Packet Data Interworking Function (PDIF).

Product All Security Gateway products

Privilege Security Administrator

Command Modes Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic > payload** *payload_name* **match childsa match { any | ipv4 | ipv6 }**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#
```

Syntax Description **ignore-rekeying-requests**

Usage Guidelines Prevents creation of a CHILD SA based on this crypto template.

Example

The following command prevents creation of a CHILD SA based on this crypto template:

ignore-rekeying-requests

ip-address-allocation

Configures IP address allocation for subscribers using this crypto template payload. Configure two payloads per crypto template. The first must have a dynamic address to assign a tunnel inner address (TIA) to the ChildSA. The second payload is configured after a successful MAnaged IP (MIP) initiation and can use the default Home Address (HoA) option.

Product

All Security Gateway products

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic > payload** *payload_name* **match childsa match { any | ipv4 | ipv6 }**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#`

Syntax Description

`ip-address-allocation { dynamic | home-address }`
`default ip-address-allocation`

default

Sets IP address allocation to the home-address.

ip-address-allocation dynamic

Specifies that the IP address for the subscriber is allocated from a dynamic IP pool.

ip-address-allocation home-address

The IP address for the subscriber is allocated by the Home Agent. This is the default setting for this command.

Usage Guidelines

Use this command to configure how ChildSA payloads are allocated IP addresses for this crypto template.

Example

The following command is for the first ChildSA and will ensure that it gets a TIA address from an IP address pool:

`ip-address-allocation dynamic`

The following command is for the second ChildSA and will ensure that it gets a HoA address from the HA:

`default ip-address-allocation`

ipsec transform-set

Configures the IPSec transform set to be used for this crypto template payload.

Product

All Security Gateway products

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic > payload** *payload_name* **match childsa match { any | ipv4 | ipv6 }**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#
```

Syntax Description

[no] ipsec transform-set list *name* **[***name2* **] [***name3* **] [***name4* **]**

no

Specifies the IPSec transform set to be deleted. This is a space-separated list. From 1 to 4 transform sets can be entered. *name* must be an alphanumeric string of 1 through 127 characters.

name

Specifies the context configured IPSec transform set name to be used in the crypto template payload. This is a space-separated list. From 1 to 4 transform sets can be entered. *name* must be an alphanumeric string of 1 through 127 characters.

Usage Guidelines

Use this command to list the IPSec transform set(s) to use in this crypto template payload.

Example

The following command configures IPSec transform sets named *ipset1* and *ipset2* to be used in this crypto template payload:

```
ipsec transform-set list ipset1 ipset2
```

lifetime

Configures the number of seconds for IPSec Child SAs derived from this crypto template payload to exist.

Product

All Security Gateway products

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic > payload** *payload_name* **match childsa match { any | ipv4 | ipv6 }**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#
```

Syntax Description

```
lifetime { sec [ kilo-bytes kbytes ] | kilo-bytes kbytes }
default lifetime
```

sec

Specifies the number of seconds for IPSec Child Security Associations derived from this crypto template payload to exist. *sec* must be an integer from 60 through 604800. Default: 86400

kilo-bytes *kbytes*

Specifies lifetime in kilobytes for IPSec Child Security Associations derived from this crypto template payload. *kbytes* must be an integer from 1 through 2147483647.

default lifetime

Sets the lifetime to its default value of 86400 seconds.

Usage Guidelines

Use this command to configure the number of seconds and/or kilobytes for IPSec Child Security Associations derived from this crypto template payload to exist.

Example

The following command configures the IPSec child SA lifetime to be *120* seconds:

```
lifetime 120
```

maximum-child-sa

Configures the maximum number of IPSec child security associations that can be derived from a single IKEv2 IKE security association.

Product

All Security Gateway products

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic > payload** *payload_name* **match childsa match { any | ipv4 | ipv6 }**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#
```

Syntax Description

maximum-child-sa *num*
default maximum-child-sa

maximum-child-sa *num*

Specifies the maximum number of IPSec child security associations that can be derived from a single IKEv2 IKE security association. *num* must be 1. Default: 1

default maximum-child-sa

Sets the maximum number of Child SAs to its default value of 1.

Usage Guidelines

Use this command to configure the maximum number of IPSec child security associations that can be derived from a single IKEv2 IKE security association.

Example

The following command configures the maximum number of child SAs to 1:

maximum-child-sa 1

rekey

Configures IPSec Child Security Association rekeying.

Product

All Security Gateway products

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic > payload** *payload_name* **match childsa match { any | ipv4 | ipv6 }**

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(cfg-crypto-tmpl-ikev2-tunnel-payload)#

Syntax Description

[no] rekey [keepalive]

no

Disables this feature.

keepalive

If specified, a session will be rekeyed even if there has been no data exchanged since the last rekeying operation. By default, rekeying is only performed if there has been data exchanged since the previous rekey.

Usage Guidelines

Use this command to enable or disable the ability to rekey IPSec Child SAs after approximately 90% of the Child SA lifetime has expired. The default, and recommended setting, is not to perform rekeying. No rekeying

means the PDIF will not originate rekeying operations and will not process CHILD SA rekeying requests from the UE.

Example

The following command disables rekeying:

```
no rekey
```

tsi

Configures the IKEv2 Traffic Selector-Initiator (TSi) payload address options.

Product

All Security Gateway products

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic > payload** *payload_name* **match childsa match { any | ipv4 | ipv6 }**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#
```

Syntax Description

tsi start-address { any end-address any | endpoint end-address endpoint }

any end-address any

Configures the TSi payload to allow all IP addresses.

endpoint end-address endpoint

Configures the TSi payload to allow only the Mobile endpoint address. (Default)

Usage Guidelines

On receiving a successful IKE_SA_INIT Response from PDIF, the MS sends an IKE_ AUTH Request for the first EAP-AKA authentication. If the MS is capable of doing multiple-authentication, it includes the MULTI_AUTH_SUPPORTED Notify payload in the IKE_AUTH Request. MS also includes an IDi payload containing the NAI, SA, TSi, TSr, and CP (requesting IP address and DNS address) payloads.

Example

Use the following example to configure a TSi payload that allows all addresses:

```
tsi start-address any end-address any
```

tsr

Configures the IKEv2 Traffic Selector-Responder (TSr) payload address options.

Product

All Security Gateway products

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic > payload** *payload_name* **match childsa match { any | ipv4 | ipv6 }**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#
```

Syntax Description

[no] tsr start-address *ip address* **end-address** *ip address*

no

Disables the specified tsr address range.

start-address *ip address*

Specifies the starting IP address of the TSr payload in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

See the limitations listed in the *Usage* section.

end-address *ipv4 address*

Specifies the ending IP address of the TSr payload in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

See the limitations listed in the *Usage* section.

Usage Guidelines

This command is used to specify an IP address range in the single TSr payload that the PDG/TTG returns in the last IKE_AUTH message. This TSr is Child SA-specific.

This command is subject to the following limitations:

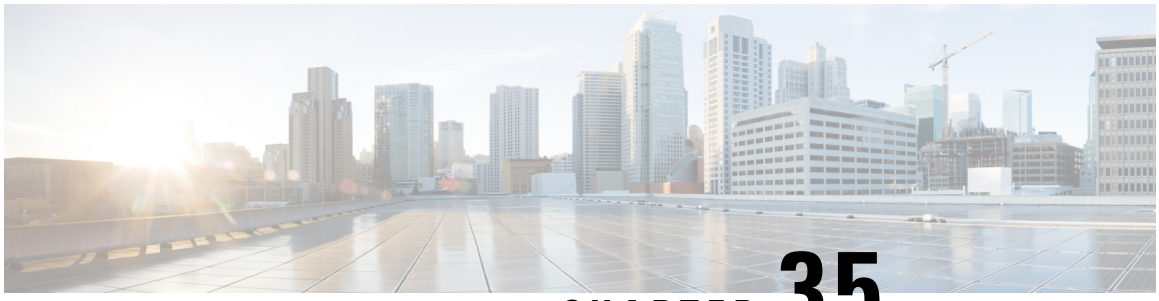
- The configuration is restricted to a maximum of four TSrs per payload and per childsa.
- Overlapping TSrs are not allowed either inside the same payload or across different payloads.
- When a TSr is configured via this command, only the configured TSr will be considered for narrowing-down. For example, if one IPv4 TSr is configured, and the gateway receives an IPv6 TSr, the gateway will reject the call with a TS_UNACCEPTABLE notification.
- The UE/PEER must send both INTERNAL_IP4_ADDRESS and INTERNAL_IP6_ADDRESS in the Configuration Payload, whenever it needs both IPv4 and IPv6 addresses in TSrs. Otherwise, the gateway will respond back with only one type depending upon the type of address received in the Configuration Payload. For example,.if the gateway receives only INTERNAL_IP4_ADDRESS in the Configuration Payload but both IPv4 and IPv6 addresses are in the TSrs, the GW will narrow down only the IPv4 address, and ignore the IPv6 TSrs.

- IPv4 TSrs are not allowed inside IPv6 payloads.
- IPv6 TSrs are not allowed inside IPv4 payloads.

Example

Use the following example to configure a TSr payload that specifies an IPv4 address range for the payload:

```
tsr start-address 10.2.3.4 end-address 10.2.3.155
```



CHAPTER 35

Crypto Template IKEv2-Vendor Configuration Mode Commands

The Crypto Template IKEv2-Vendor Configuration Mode is used to configure an IKEv2 IPSec policy for a vendor. It includes most of the IPSec parameters and IKEv2 dynamic parameters for cryptographic and authentication algorithms.

Command Modes Exec > Global Configuration > Context Configuration > Crypto Template IKEv2-Vendor Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-vendor**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmp1-ikev2-vendor)#
```

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

- configuration-payload, on page 953
- do show, on page 954
- end, on page 955
- exit, on page 955
- ikev2-ikesa, on page 955
- keepalive, on page 957
- payload, on page 958

configuration-payload

This command is used to configure mapping of the configuration payload attributes for a crypto vendor template.

Product All IPSec-related services

Privilege Security Administrator

Command Modes Exec > Global Configuration > Context Configuration > Crypto Template IKEv2-Vendor Configuration

configure > **context** *context_name* > **crypto template** *template_name* **ikev2-vendor**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmp1-ikev2-vendor)#
```

Syntax Description

```
configuration-payload private-attribute-type { imei integer | p-cscf-v4
v4_value | p-cscf-v6 v6_value }
remove configuration-payload private-attribute-type { imei | p-cscf-v4 |
 p-cscf-v6 }
```

remove

Removes mapping of the configuration payload attributes.

private-attribute-type

Defines the private payload attribute.

imei *integer*

Defines an International Mobile Equipemnt Identity number. Default value is 16391.

integer must be an integer from 16384 to 32767.

p-cscf-v4 *v4_value*

Defines the IPv4 pcscf payload attribute value. Default value is 16384.

v4_value is an integer from 16384 to 32767.

p-cscf-v6 *v6_value*

Defines IPv6 pcscf payload attribute value. Default value is 16390.

v6_value is an integer from 16384 to 32767.

Usage Guidelines

Use this command to configure mapping of the configuration payload attributes for a crypto vendor template.

Example

The following command configures the mapping of the configuration payload attributes p-cscf-v6 to 17001.

```
configuration-payload private-attribute-type p-cscf-v6 17001
```

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.

ikev2-ikesa

Configures parameters for the IKEv2 IKE Security Associations within this vendor template.

Product All IPSec-related services

Privilege Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template IKEv2-Vendor Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-vendor**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmp1-ikev2-vendor)#
```

Syntax Description

```
ikev2-ikesa { fragmentation | ignore-rekeying-requests | mobike [
cookie-challenge ] | rekey [ disallow-param-change ] | transform-set list
 name1 [ name2 [ name3 [ name4 [ name5 [ name6 ] ] ] ] ] }
remove ikev2-ikesa { fragmentation | ignore-rekeying-requests | mobike |
 rekey | transform-set list }
```

remove

Disables a previously enabled ikev2-ikesa configuration.

fragmentation

Enables IKESA fragmentation (Tx) and re-assembly (Rx).

Default: IKESA fragmentation and re-assembly is allowed.

ignore-rekeying-requests

Ignores received IKE_SA Rekeying Requests.

mobike [cookie-challenge]

IKEv2 Mobility and Multihoming Protocol (MOBIKE) allows the IP addresses associated with IKEv2 and tunnel mode IPSec Security Associations to change. A mobile Virtual Private Network (VPN) client could use MOBIKE to keep the connection with the VPN gateway active while moving from one address to another. Similarly, a multi-homed host could use MOBIKE to move the traffic to a different interface if, for instance, the one currently being used stops working. Default: Disabled

cookie-challenge: Use this keyword to enable the return routability check. The Gateway performs a return routability check when MOBIKE is enabled along with this keyword. A return routability check ensures that the other party can receive packets at the claimed address. Default: Disabled

rekey [disallow-param-change]

Specifies if IKESA rekeying should occur before the configured lifetime expires (at approximately 90% of the lifetime interval). Default is not to re-key.

The **disallow-param-change** option prevents changes in negotiation parameters during rekey.

transform-set list

Specifies the name of a context-level configured IKEv2 IKE Security Association transform set.

name1 through *name6* must be an existing IKEv2 IKESA Transform Set expressed as an alphanumeric string of 1 through 127 characters.

The transform set is a space-separated list of IKEv2-IKESA SA transform sets to be used for deriving IKEv2 IKE Security Associations from this crypto template. A minimum of one transform-set is required; maximum configurable is six.

Usage Guidelines Use this command to configure parameters for the IKEv2 IKE Security Associations within this vendor template.

Example

The following command enables IKESA fragmentation and re-assembly:

```
ikev2-ikesa fragmentation
```

The following command configures the IKEv2 IKESA list, consisting of transform sets named *ikesa43* and *ikesa326*:

```
ikev2-ikesa transform-set list ikesa43 ikesa326
```

keepalive

Configures keepalive or dead peer detection for security associations used within this vendor template.

Product All products supporting IPSec

Privilege Security Administrator

Command Modes Exec > Global Configuration > Context Configuration > Crypto Template IKEv2-Vendor Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-vendor**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmp1-ikev2-vendor)#
```

Syntax Description **keepalive [interval** *seconds* **[timeout** *timeout_seconds* **[num-retry** *retry_seconds* **]]]**

{ no | remove } keepalive

no

Disables keepalive messaging.

remove

Removes previously configured keepalive messaging.

interval *sec*

Specifies the duration (in seconds) after which the next keepalive request is sent.

sec must be an integer from 10 through 3600.

Default: 3600 seconds

timeout *timeout_seconds*

Specifies the duration (in seconds) after which keepalive times out.

timeout_seconds must be an integer from 10 through 3600. Default: 10

num-retry *retry_seconds*

Specifies the total number of times to resend the keepalive request after timing out.

retry_seconds must be an integer from 1 through 100. Default: 2

Usage Guidelines Use this command to set parameters associated with determining the availability of peer servers.

Example

The following command sets a keepalive interval to three minutes (**180** seconds) with a timeout value of 1 minute (**60** seconds):

```
keepalive interval 180 timeout 60
```

payload

Creates a new, or specifies an existing, crypto template vendor payload, and enters the Crypto Template IKEv2 Vendor Payload Configuration Mode.

Product All Security Gateway products

Privilege Security Administrator

Command Modes Exec > Global Configuration > Context Configuration > Crypto Template IKEv2-Vendor Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-vendor**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-vendor)#
```

Syntax Description **[remove] payload** *payload_name*

no

Removes a previously configured crypto template IKEv2 vendor payload.

vendor_payload

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

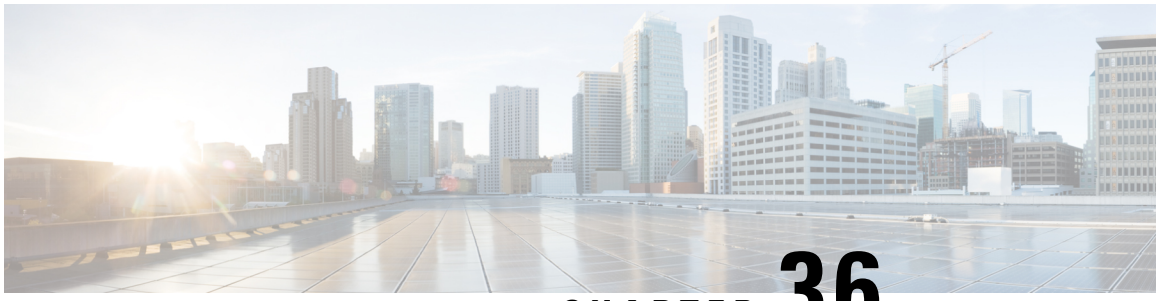
Usage Guidelines Use this command to create a new or enter an existing crypto template IKEv2 vendor payload. The payload mechanism is a means of associating parameters for the Security Association (SA) being negotiated.

Crypto Template IKEv2 Vendor Payload Configuration Mode commands are defined in the *Crypto Template IKEv2-Vendor Payload Configuration Mode Commands* chapter.

Example

The following command configures a crypto template IKEv2 vendor payload called *payload5* and enters the Crypto Template IKEv2 Vendor Payload Configuration Mode:

```
payload payload5
```



CHAPTER 36

Crypto Template IKEv2-Vendor Payload Configuration Mode Commands

The Crypto Template IKEv2-Vendor Payload Configuration Mode is used to assign the correct IPSec transform-set from a list of up to four different transform-sets, and to assign Mobile IP addresses. There should be two payloads configured. The first must have a dynamic addressing scheme from which the ChildSA gets a TIA address. The second payload supplies the ChildSA with a HoA, which is the default setting for *ip-address-allocation*.

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template IKEv2-Vendor Configuration > Crypto Template IKEv2-Vendor Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-vendor > payload** *payload_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-vendor-payload)#
```

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

- do show, on page 961
- end, on page 962
- exit, on page 962
- ignore-rekeying-requests, on page 962
- ipsec, on page 963
- lifetime, on page 964
- rekey, on page 965

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.

ignore-rekeying-requests

Ignores CHILD SA rekey requests from the Packet Data Interworking Function (PDIF).

Product All Security Gateway products

Privilege Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template IKEv2-Vendor Configuration > Crypto Template IKEv2-Vendor Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-vendor > payload** *payload_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(cfg-crypto-tmp1-ikev2-vendor-payload)#`

Syntax Description

`[ remove ] ignore-rekeying-requests`

remove

If previously configured, removes the ignore-rekeying-requests configuration.

Usage Guidelines

Prevents creation of a CHILD SA based on this crypto vendor template.

Example

The following command prevents creation of a CHILD SA based on this crypto vendor template:

`ignore-rekeying-requests`

ipsec

Configures the IPSec transform set to be used for this crypto template vendor payload.

Product

All Security Gateway products

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template IKEv2-Vendor Configuration > Crypto Template IKEv2-Vendor Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-vendor > payload** *payload_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(cfg-crypto-tmp1-ikev2-vendor-payload)#`

Syntax Description

`ipsec transform-set list` *`name`* **`[`***`name2`***`] [`***`name3`***`] [`***`name4`***`]`**

`remove ipsec transform-set list`

remove

Specifies the IPSec transform set to be deleted.

name

Specifies the context configured IPSec transform set name to be used in the crypto template vendor payload. This is a space-separated list. A maximum of 4 transform sets can be entered.

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

Usage Guidelines Use this command to list the IPSec transform set(s) to use in this crypto template vendor payload.

Example

The following command configures IPSec transform sets named *ipset1* and *ipset2* to be used in this crypto template vendor payload:

```
ipsec transform-set list ipset1 ipset2
```

lifetime

Configures the number of seconds for IPSec Child SAs derived from this crypto template vendor payload.

Product All Security Gateway products

Privilege Security Administrator

Command Modes Exec > Global Configuration > Context Configuration > Crypto Template IKEv2-Vendor Configuration > Crypto Template IKEv2-Vendor Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-vendor > payload** *payload_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmp1-ikev2-vendor-payload)#
```

Syntax Description

```
lifetime { sec [ kilo-bytes kbytes ] | kilo-bytes kbytes | seqno sequence }

remove lifetime
```

remove

Removes the previously enabled lifetime configuration.

sec

sec must be an integer from 60 through 604800. Default: 86400

kilo-bytes *kbytes*

Specifies lifetime in kilobytes for IPSec Child Security Associations derived from this crypto template vendor payload.

kbytes must be an integer from 1 through 2147483647.

seqno *sequence*

Specifies lifetime in sequence number for IPSec Child Security Associations derived from this crypto vendor template.

sequence must be an integer from 10 through 4293918720.

Usage Guidelines Use this command to configure the number of seconds and/or kilobytes, or sequence number for IPSec Child Security Associations derived from this crypto template vendor payload.

Example

The following command configures the IPSec child SA lifetime to be *120* seconds:

```
lifetime 120
```

rekey

Configures IPSec Child Security Association rekeying.

Product All Security Gateway products

Privilege Security Administrator

Command Modes Exec > Global Configuration > Context Configuration > Crypto Template IKEv2-Vendor Configuration > Crypto Template IKEv2-Vendor Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-vendor > payload** *payload_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmp1-ikev2-vendor-payload)#
```

Syntax Description

```
rekey [ keepalive ]
```

```
remove rekey
```

remove

Removes a previously enabled rekey configuration.

keepalive

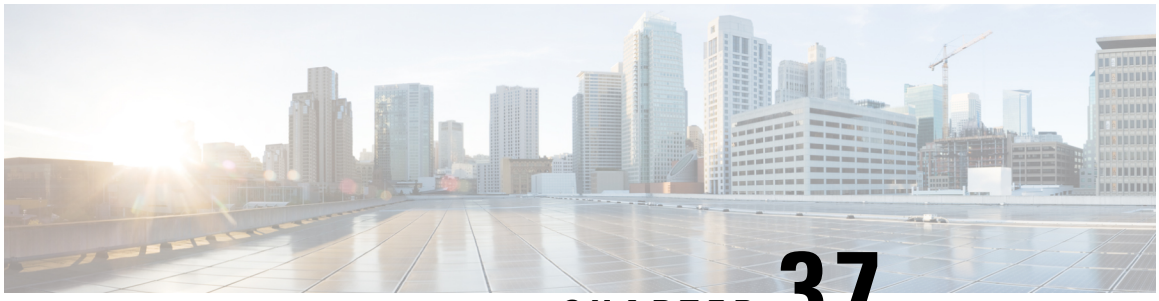
If specified, a session will be rekeyed even if there has been no data exchanged since the last rekeying operation. By default, rekeying is only performed if there has been data exchanged since the previous rekey.

Usage Guidelines Use this command to enable or disable the ability to rekey IPSec Child SAs after approximately 90% of the Child SA lifetime has expired. The default, and recommended setting, is not to perform rekeying. No rekeying means the PDIF will not originate rekeying operations and will not process CHILD SA rekeying requests from the UE.

Example

The following command disables rekeying:

```
remove rekey
```



CHAPTER 37

Crypto IPSec Transform Set Configuration Mode Commands

The Crypto IPSec Transform Set Configuration Mode is used to configure properties for system transform sets.

Transform Sets are used to define IPSec security associations (SAs). IPSec SAs specify the IPSec protocols to use to protect packets.

Command Modes

Exec > Global Configuration > Context Configuration > Crypto IPSec Transform Set Configuration

configure > context *context_name* **> crypto ipsec transform-set** *transform_set_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-crypto-trans)#`

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

- end, on page 967
- exit, on page 968
- mode, on page 968

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.

mode

Configures the IPSec encapsulation mode for an existing or new transform set. For a new transform set, you must specify transform set parameters as described for the **crypto ipsec transform-set** command in the *Context Configuration Mode Commands* chapter.

Product

PDSN

HA

GGSN

PDIF

Privilege

Security Administrator

Syntax Description

```
mode { transport | tunnel }
```

transport

Specifies that the transform set only protects the upper layer protocol data portions of an IP datagram, leaving the IP header information unprotected. Default: Disabled

Important This mode should only be used if the communications end-point is also the cryptographic end-point.

tunnel

Specifies that the transform set protects the entire IP datagram.

This mode should be used if the communications end-point is different from the cryptographic end-point as in a VPN. Default: Enabled

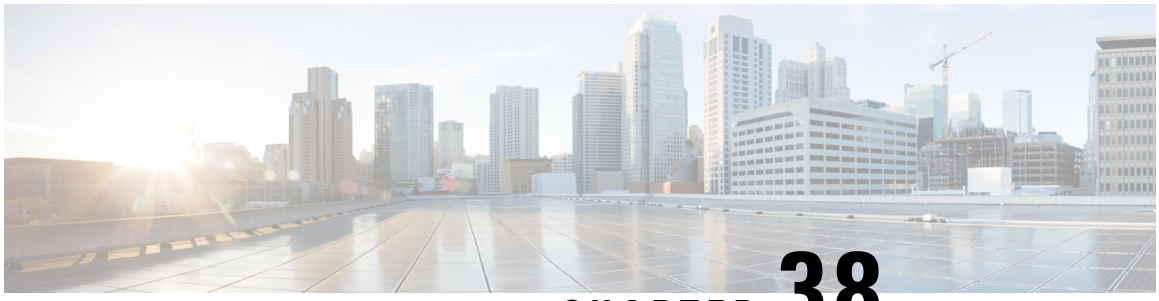
Usage Guidelines

This command specifies the encapsulation mode for the transform set.

Example

The following command configures the transforms set's encapsulation mode to transport:

```
mode transport
```



CHAPTER 38

Crypto Vendor Policy Configuration Mode Commands

The Crypto Vendor Policy Configuration Mode can be used to assign priorities to vendors for cryptographic configurations. A maximum of 32 vendor policies can be configured.

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Vendor Policy Configuration

configure > context *context_name* **> crypto vendor-policy** *policy_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-crypto-vendor-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 971
- end, on page 972
- exit, on page 972
- precedence, on page 972

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.

precedence

Use this command to associate a vendor ID with a vendor template, and set precedence for it.

Product ePDG

Privilege Security Administrator

Command Modes Exec > Global Configuration > Context Configuration > Crypto Vendor Policy Configuration

configure > context *context_name* **> crypto vendor-policy** *policy_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-vendor-policy)#
```

Syntax Description

precedence *precedence_value* **vendor-id** *id* **vendor-template** *template_name*

no precedence *precedence_value*

no

Restores the configuration to its default value.

precedence_value

precedence_value must be an integer from 1 through 64.

vendor-id *id*

Specifies the vendor ID to match the vendor template.

id must be an alphanumeric string from 1 to 256 characters.

vendor-template *template_name*

Specifies the vendor template to associate with the vendor ID.

template_name must be an alphanumeric string from 1 to 127 characters.

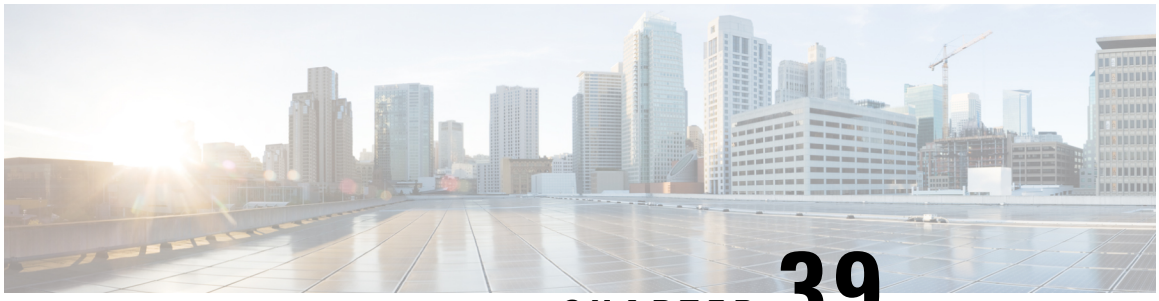
Usage Guidelines

Use this command to associate a vendor ID with a vendor template, and set precedence for it. A maximum of 64 vendor templates can be associated with a vendor policy.

Example

The following command associate a vendor ID called **atl23** and associate it to a vendor template called **atlcryptpl** with the precedence value of **2** :

```
precedence 2 vendor-id atl23 vendor-template atlcryptpl
```



CHAPTER 39

CSS Delivery Sequence Configuration Mode Commands

The CSS Delivery Sequence Configuration Mode is used to configure the order in which traffic is delivered to Content Service Steering (CSS) services and their associated content servers.

Important This is a restricted configuration mode. In 9.0 and later releases, this configuration mode is deprecated.

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

- end, on page 975
- exit, on page 975
- recovery, on page 976
- server-interface, on page 976

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.

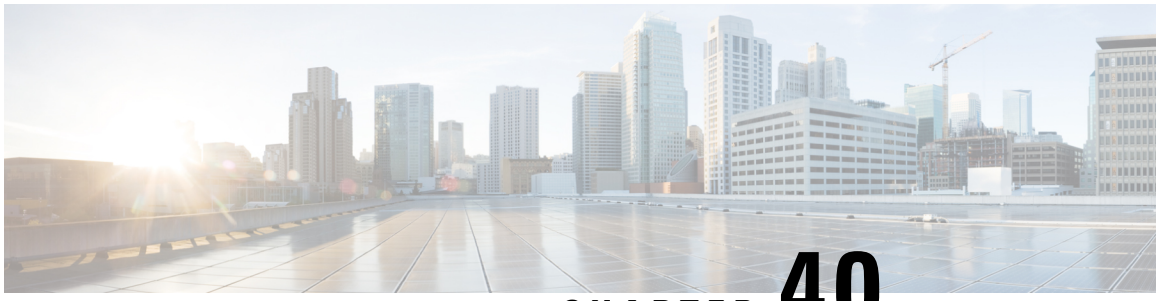
Product	All
Privilege	Security Administrator, Administrator
Syntax Description	`exit`
Usage Guidelines	Use this command to return to the parent configuration mode.

recovery

In 9.0 and later releases, this command is deprecated.

server-interface

In 9.0 and later releases, this command is deprecated.



CHAPTER 40

DDN APN Profile Configuration Mode Commands

Command Modes

DDN APN Profile Configuration Mode provides commands that support downlink data notification (DDN) access point name (APN) support on the S-GW and SAEGW. A Voice over LTE (VoLTE) license must be installed to access DDN APN Profile Configuration Mode.

Exec > Global Configuration > DDN APN Profile Configuration

configure > ddn-apn-profile *ddn_apn_profile_name*

Entering the above command sequence results in the following prompt:

```
[local] host_name (ddn-apn-profile profile_name)#
```

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

- end, on page 977
- exit, on page 977
- isr-sequential-paging, on page 978
- qci, on page 978

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.

isr-sequential-paging

This command initiates paging first towards the last known RAT, then towards the other RAT for the Idle Mode Signaling Reduction (ISR) feature.

Product SGW

SAEGW

Privilege Administrator, Security Administrator

Command Modes Exec > Global Configuration > DDN APN Profile Configuration

configure > ddn-apn-profile *ddn_apn_profile_name*

Entering the above command sequence results in the following prompt:

```
[local] host_name (ddn-apn-profile profile_name)#
```

Syntax Description **[remove] isr-sequential-paging**

remove

Removes the ISR sequential paging configuration from the DDN APN Profile.

isr-sequential-paging

Enables the ISR sequential paging configuration for the DDN APN Profile.

Usage Guidelines usage

Example

Use the following example to enable ISR sequential paging on the S-GW or SAEGW:

isr-sequential-paging

qci

This command configures various DDN parameters for a quality of class identifier (QCI) in a DDN APN Profile.

Product SGW

Privilege

Administrator, Security Administrator

Command Modes

Exec > Global Configuration > DDN APN Profile Configuration

configure > ddn-apn-profile *ddn_apn_profile_name*

Entering the above command sequence results in the following prompt:

```
[local] host_name (ddn-apn-profile profile_name)#
```

Syntax Description

qci *qci_number* **ddn { failure-action pkt-drop-timer** *duration_seconds* **| ignore-ddn-timers | min-buf-size** *size_kb*
[remove] qci *qci_number*

remove qci *qci_number*

Removes the DDN configuration for the specified QCI value.

qci

Specifies the quality of class identifier (QCI) to be configured. Valid entries are from 1 to 254. A maximum of 4 QCI values are supported for configuration per ddn-apn-profile.

ddn

Specifies a DDN parameter to be configured.

failure-action pkt-drop-timer *duration_seconds*

This is the time for which no data for UE is buffered. This timer activates the moment a DDN failure is received. This value supersedes the one configured at sgw-service level. When a DDN failure is received, the minimum of the pkt-drop-timer configured for all QCIs having data is started.

ignore-ddn-timers

If the DDN Delay timer is started and data arrives on a bearer with a QCI for which this flag is set, then the S-GW will stop that timer and send the DDN. The **ignore-ddn-timers** configuration is applicable only to the DDN delay timer. This helps to send DDN for preferential bearers immediately on receiving new data. This is '0' by default and does not affect any DDN timers.

min-buf-size *size_kb*

This is the buffer allocated for storing data packets for each bearer when the UE is in the idle state. This field is used to set higher buffer value for preferential bearers. Valid entries are from 2 to 4 KB. The default is 2 KB.



Important Set this field to a value higher than 2KB only for QCI values corresponding to preferential bearers (like VoLTE). If the default buffer size of all QCI values is increased, it would decrease the system performance due to higher memory consumption and such a configuration is NOT recommended.

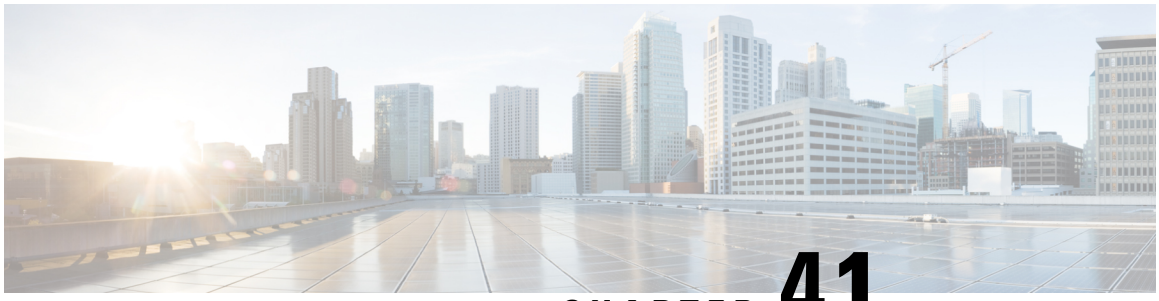
Usage Guidelines

Use this command to configure various DDN parameters for a specified QCI.

Example

The following example configures the minimum buffer size as 3 KB for QCI 3.

```
qci 3 ddn min-buf-size 3
```



CHAPTER 41

Decor Profile Configuration Mode Commands

The Decor Profile Configuration Mode is used to create and configure the DECOR profile. The DECOR profile represents the Dedicated Core Network (DCN) as deployed by the operator.

Command Modes

Exec > Global Configuration > Decor Profile Configuration

configure > decor-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-decor-profile-<profile_name>)#`

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

- dcn-id, on page 981
- description, on page 982
- dns, on page 983
- do show, on page 983
- end, on page 984
- exit, on page 984
- mmegi, on page 984
- plmn-id, on page 985
- served-dcn, on page 986
- ue-usage-types, on page 987

dcn-id

Important The **dcn-id** CLI command introduced with the DECOR feature is not fully qualified in this release. It is available only for testing purposes.

This command allows you to configure the dedicated core network (DCN) identifier for the specified decor-profile.

Product MME

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Decor Profile Configuration

configure > decor-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-decor-profile-profile_name)#`

Syntax Description

dcn-id *dcn_id*
no dcn-id

no

Removes the specified DCN identifier from decor-profile.

dcn-id *dcn_id*

Configures the DCN identifier for the specified decor-profile. *dcn_id* is an integer from 0 to 65535.

Usage Guidelines Use this configuration to configure the DCN identifier for the specified decor-profile.

Example

The following command configures the DCN ID as *12345*:

dcn-id 12345

description

Allows you to enter descriptive text for this configuration.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Decor Profile Configuration

configure > decor-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-decor-profile-profile_name)#`

Syntax Description

description *text*
no description

no

Clears the description for this configuration.

text

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

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

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

dns

This command allows you to configure the service parameters to select peer nodes for the specified decor-profile.

Product MME

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Decor Profile Configuration

configure > decor-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-decor-profile-profile_name)#`

Syntax Description

```
dns service-param ue-usage-type
no dns service-param
```

no

Removes the service parameter configuration from decor-profile.

service-param

Configures the service parameter types used for DNS peer lookup.

ue-usage-type

Configures the UE Usage type that will be used for DNS service parameter.

Usage Guidelines Use this configuration to configure the UE Usage Type or DCN-ID for S-GW / P-GW / MME / S4-SGSN / MMEGI lookup using DNS.

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.

mmegi

This command allows you to configure an MME Group Identifier (MMEGI) of the configured dedicated core network (DCN).

Product MME

Privilege Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Decor Profile Configuration

configure > decor-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-decor-profile-profile_name)#`

Syntax Description

`[ no ] mmegi { mmegi_value | dns }`

no

Removes the specified MMEGI value.

mmegi { *mmegi_value* | dns }

Identifies the MMEGI of the configured DCN. *mmegi_value* is an integer value from 32768 to 65535.

dns: Enables DNS for MMEGI retrieval using UE Usage Type

Usage Guidelines

Use this configuration to configure the MME Group Identifier (MMEGI) value of the configured DCN. In 21.6 and later releases, DNS-based MMEGI selection is supported.

A new MME is selected from the MMEGI. If no valid MME can be obtained from the MMEGI, the MME is selected from a common core network.

Example

The following command configures the MMEGI value as *38888*:

`mmegi 38888`

plmn-id



Important The **plmn-id** CLI command introduced with the DECOR feature is not fully qualified in this release. It is available only for testing purposes.

This command allows you to configure the PLMN identifier for the specified decor-profile.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Decor Profile Configuration

configure > decor-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-decor-profile-profile_name)#`

Syntax Description

plmn-id mcc *mcc_id* **mnc** *mnc_id*
no plmn-id

no

Removes the specified PLMN identifier from decor-profile.

plmn-id mcc *mcc_id* mnc *mnc_id*

Configures the PLMN identifier for the specified decor-profile.

mcc *mcc_id*: Configures the mobile country code (MCC) for the specified decor-profile. *mcc_id* is a 3-digit number between 000 to 999.

mnc *mnc_id*: Configures the mobile network code (MNC) for the specified decor-profile. *mnc_id* is a 2- or 3-digit number between 00 to 999.

Usage Guidelines

Use this configuration to configure the PLMN identifier for the specified decor-profile. This supports network sharing with different MMEGIs for different PLMNs.

Example

The following command configures the PLMN identifier with MCC of *555* and MNC of *20*:

```
plmn-id mcc 555 mnc 20
```

served-dcn



Important The **served-dcn** CLI command introduced with the DECOR feature is not fully qualified in this release. It is available only for testing purposes.

This command allows you to configure the MME that is serving the dedicated core network (DCN) and its relative capacity.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Decor Profile Configuration

configure > **decor-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-decor-profile-profile_name)#
```

Syntax Description

served-dcn [relative-capacity *capacity* **]**
no served-dcn

no

Removes the specified configuration from decor-profile.

served-dcn [relative-capacity *capacity*]

Configures the MME that is serving the DCN.

relative-capacity *capacity*: Sets the relative capacity of the DCN. *capacity* must be an integer from 0 to 255. The default relative-capacity is 255.

Usage Guidelines

Use this configuration to configure the MME that is serving the DCN and relative capacity.

These values are sent by MME to eNodeB during S1 Setup Response to indicate DCN-IDs served by the MME and their relative capacity.

Example

The following command configures the served DCN with relative capacity set to *100*:

```
served-dcn relative-capacity 100
```

ue-usage-types

This command allows you to configure the number of UE Usage Types in the dedicated core network (DCN).

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Decor Profile Configuration

configure > decor-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-decor-profile-profile_name)#
```

Syntax Description

[no] ue-usage-types *num_ue_usage_types* **+**

no

Removes the specified MMEGI value.

ue-usage-types *num_ue_usage_types*

Specifies the number of UE Usage Types in the dedicated core network. *num_ue_usage_types* is an integer from 0 to 255.

A maximum number of 20 UE Usage Types are supported per DCN.

+

Multiple UE usage types can be entered (up to 20 in a single line, separated by spaces).

Usage Guidelines

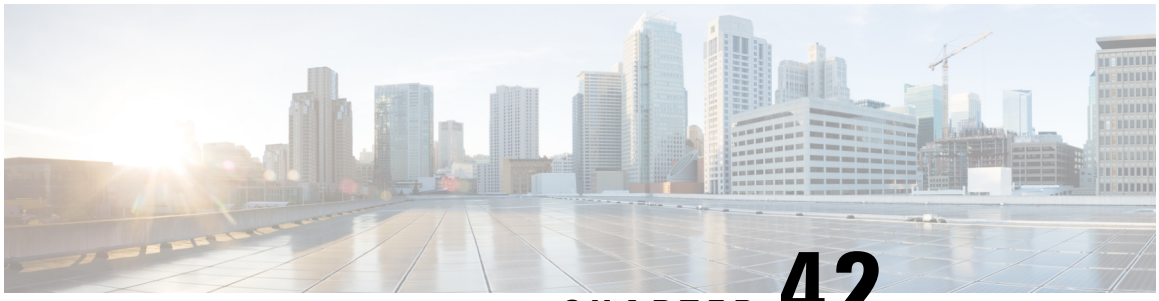
Use this command to configure the the number of UE Usage Types in the DCN.

The UE Usage Type is a subscription information parameter stored in the HSS, used by the serving network to select the DCNs that must serve the UE. The operator can configure DCNs and its serving UE Usage Type as required. Multiple UE Usage Types can be served by the same DCN. The HSS provides the UE Usage Type value in the subscription information of the UE to the MME/SGSN/MSC.

Example

The following command configures *25* UE Usage Types:

```
ue-usage-types 25
```



CHAPTER 42

DHCP Client Profile Configuration Mode Commands

The Dynamic Host Configuration Protocol (DHCP) Client Profile Configuration Mode is used to create and manage DHCP client profile parameters. DHCP client profiles are associated with APNs.

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Client Profile Configuration

configure > context *context_name* **> dhcp-client-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-client-profile)#
```

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

- client-identifier, on page 989
- dhcpv6-client-unicast, on page 990
- disable, on page 991
- enable, on page 992
- end, on page 993
- exit, on page 993
- request, on page 993

client-identifier

Configures the client-identifier which is sent to the external DHCP server.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Client Profile Configuration

configure > context *context_name* **> dhcp-client-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-client-profile)#
```

Syntax Description

```
client-identifier { imsi | msisdn }
default client-identifier
```

default

Specifies that the subscriber's IMSI be included in the client-identifier option of relevant DHCP messages.

imsi

Specifies that the subscriber's IMSI be included in the client-identifier option of relevant DHCP messages.

Important The **imsi** option is not supported in this release.

msisdn

Specifies that the subscriber's MSISDN be included in the client-identifier option of relevant DHCP messages.

Usage Guidelines

Use this command to configure which information is included in the DHCP client-identifier option of DHCP messages to external DHCP servers.

Example

The following command specifies that a subscriber's MSISDN be included in the DHCP client-identifier option of DHCP messages to external DHCP servers:

```
client-identifier msisdn
```

dhcpv6-client-unicast

Configures the client unicast address which is sent to the external DHCP server.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Client Profile Configuration

configure > context *context_name* **> dhcp-client-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-client-profile)#
```

Syntax Description

dhcpv6-client-unicast

dhcpv6-client-unicast

Enables client to send messages on unicast address towards the server.

Usage Guidelines

Use this command to send messages on unicast address towards the server.

Example

The following command specifies that messages are sent on unicast address to external DHCP servers:

dhcpv6-client-unicast

disable

Disables the specified options on the DHCP client.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Client Profile Configuration

configure > context *context_name* **> dhcp-client-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-client-profile)#
```

Syntax Description

disable { dhcp-message-spray | rapid-commit-dhcpv4 | rapid-commit-dhcpv6 | user-class-option }

dhcp-message-spray

Disables DHCP client from spraying a DHCP message to all configured DHCP servers in the PDN.

rapid-commit-dhcpv4

Disables support of the rapid commit feature for DHCPv4 client functionality.

rapid-commit-dhcpv6

Disables support of the rapid commit feature for DHCPv6 client functionality.

user-class-option

Disables sending the "User_Class_Option" in the DHCPv6 messages from P-GW/GGSN to the external DHCPv6 server during DHCPv6 Prefix Delegation Setup.

Usage Guidelines

Use this command to disable options on the DHCP client.

Example

The following command disables support of the rapid commit feature for DHCPv6 client functionality:

```
disable rapid-commit-dhcpv6
```

enable

Enables the specified options on the DHCP client.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Client Profile Configuration

configure > context *context_name* **> dhcp-client-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-client-profile)#
```

Syntax Description

```
enable { dhcp-message-spray | rapid-commit-dhcpv4 | rapid-commit-dhcpv6
| user-class-option { imsi | msisdn } }
```

dhcp-message-spray

Enables DHCP client to spray a DHCP message to all configured DHCP servers in the PDN.

By default, this is disabled. With rapid commit, there can only be one server to which this can be sent.

rapid-commit-dhcpv4

Enables support of the rapid commit feature for DHCPv4 client functionality.

By default, this is enabled.

rapid-commit-dhcpv6

Enables support of the rapid commit feature for DHCPv6 client functionality.

By default, this is enabled.

user-class-option { imsi | msisdn }

Enables P-GW/GGSN to send USER_CLASS_OPTION in DHCPv6 messages to external DHCPv6 server during Prefix Delegation Setup.

imsi: Triggers sending the "User_Class_Option" with UE's IMSI in the DHCPv6 Request message from P-GW to the external DHCPv6 server during DHCPv6 Prefix Setup (for network behind UE).

msisdn: Triggers sending the "User_Class_Option" with UE's MSISDN in the DHCPv6 Request message from P-GW to the external DHCPv6 server during DHCPv6 Prefix Setup (for network behind UE).

By default, this is enabled.

Usage Guidelines Use this command to enable options on the DHCP client.

Example

The following command enables support of the rapid commit feature for DHCPv6 client functionality:

```
enable rapid-commit-dhcpv6
```

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.

request

Configures DHCP options which can be requested by the DHCP client.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Client Profile Configuration

configure > context *context_name* **> dhcp-client-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-client-profile)#
```

Syntax Description

```
[ default ] request dhcp-option { dns-address | netbios-server-address |
 sip-server-address }
no { dns-address | netbios-server-address | sip-server-address }
```

default

Returns the command to its default setting.

no

Disables a DHCP option requested by the DHCP client.

dhcp-option { dns-address | netbios-server-address | sip-server-address }

The following DHCP options can be requested by the DHCP client:

- **dns-address**: request for DNS address
- **netbios-server-address**: request for NetBIOS server address
- **sip-server-address**: request for SIP server address

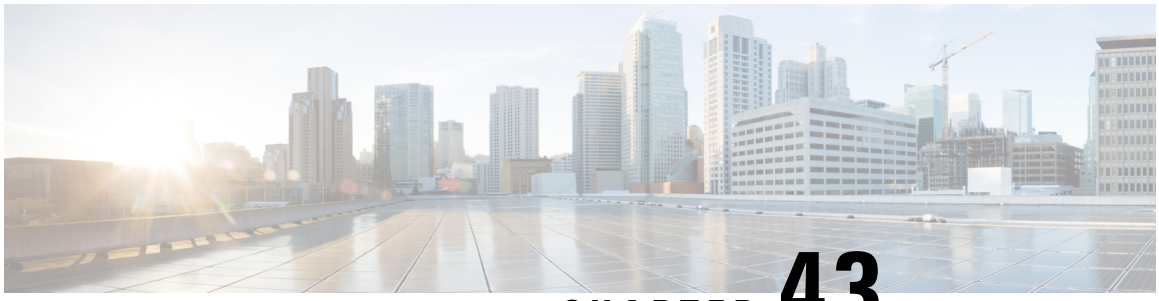
Usage Guidelines

Use this command to enable/disable options which can be requested by the DHCP client.

Example

The following command enables the DHCP client to request DNS address:

```
request dhcp-option dns-address
```



CHAPTER 43

DHCP Server Profile Configuration Mode Commands

The Dynamic Host Configuration Protocol (DHCP) Server Profile Configuration Mode is used to create and manage DHCP server profile parameters. DHCP server profiles are associated with APNs.

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Server Profile Configuration

configure > context *context_name* **> dhcp-server-profile** *profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-dhcp-server-profile)#`

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

- dhcpv6-server-preference, on page 995
- disable, on page 996
- enable, on page 997
- end, on page 998
- exit, on page 998
- process, on page 999

dhcpv6-server-preference

Specifies the waiting time for DHCPv6 client before response.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Server Profile Configuration

configure > **context** *context_name* > **dhcp-server-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-server-profile)#
```

Syntax Description

```
dhcpv6-server-preference pref_value
default dhcpv6-server-preference
```

default

Returns the command to its default setting of 0.

pref_value

Specifies the DHCP server preference value as an integer from 1 through 255. If a DHCP server responds with a preference value of 255, DHCPv6 client need not wait any longer.

Default: 0

Usage Guidelines

According to RFC-3315, DHCPv6 client should wait for a specified amount of time before considering responses to its queries from DHCPv6 servers. Use this command to specify the waiting time (DHCP server preference value) for DHCPv6 client before response.

Example

The following command sets the DHCP server preference value to *200*:

```
dhcpv6-server-preference 200
```

disable

Disables the specified options on the DHCP server.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Server Profile Configuration

configure > **context** *context_name* > **dhcp-server-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-server-profile)#
```

Syntax Description

```
disable { dhcpv6-server-reconf | dhcpv6-server-unicast |
rapid-commit-dhcpv4 | rapid-commit-dhcpv6 }
```

dhcpv6-server-reconf

Disables support for reconfiguration messages from the DHCPv6 server.

dhcpv6-server-unicast

Disables server unicast option for DHCPv6 server.

rapid-commit-dhcpv4

Disables support of the rapid commit feature for DHCPv4 server functionality.

rapid-commit-dhcpv6

Disables support of the rapid commit feature for DHCPv6 server functionality.

Usage Guidelines

Use this command to disable options on the DHCP server.

Example

The following command disables support of the rapid commit feature for DHCPv6 server functionality:

```
disable rapid-commit-dhcpv6
```

enable

Enables the specified options on the DHCP server.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Server Profile Configuration

configure > context *context_name* **> dhcp-server-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-server-profile)#
```

Syntax Description

```
enable { dhcpv6-server-reconf | dhcpv6-server-unicast | rapid-commit-dhcpv4
 | rapid-commit-dhcpv6 }
```

dhcpv6-server-reconf

Enables support for reconfiguration messages from the DHCPv6 server.

By default, this is disabled.

dhcpv6-server-unicast

Disables server unicast option for DHCPv6 server.

By default, this is disabled.

rapid-commit-dhcpv4

Enables support of the rapid commit feature for DHCPv4 server functionality.

By default, this is disabled.

rapid-commit-dhcpv6

Enables support of the rapid commit feature for DHCPv6 server functionality.

By default, this is disabled; this is done to ensure that if there are multiple DHCPv6 servers in a network, with rapid-commit-option, they would all end up reserving resources for the UE.

Usage Guidelines Use this command to enable options on the DHCP server.

Example

The following command enables support of the rapid commit feature for DHCPv6 server functionality:

```
enable rapid-commit-dhcpv6
```

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.

process

Configures what order the configuration options should be processed for a given client request.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Server Profile Configuration

configure > context *context_name* **> dhcp-server-profile** *profile_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-dhcp-server-profile)#`

Syntax Description

process dhcp-option-from { AAA | LOCAL | PDN-DHCP } priority *priority*
default process dhcp-option-from

default

AAA (priority 1) is preferred over **PDN-DHCP** (priority 2) which is preferred over **LOCAL** (priority 3) configuration.

dhcp-option-from { AAA | LOCAL | PDN-DHCP }

For a given client request, configuration values can be obtained from the following:

- **AAA**
- **LOCAL**
- **PDN-DHCP**

priority *priority*

Specifies the priority for **dhcp-option-from** options.

priority is an integer from 1 through 3. 1 is the highest priority.

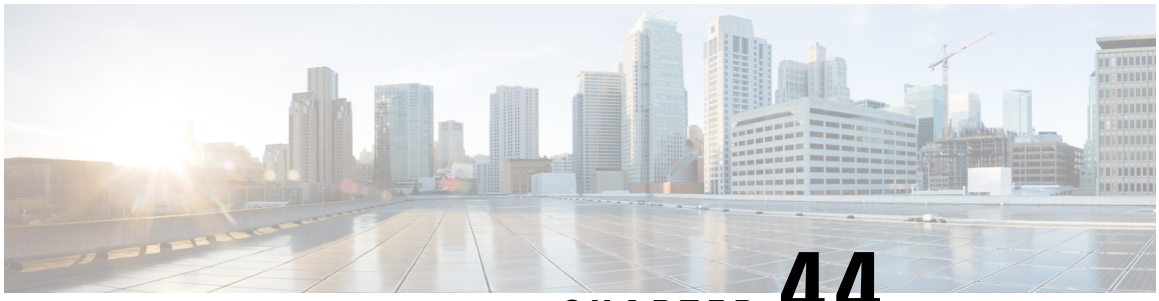
Usage Guidelines

Use this command to configure what order the configuration options should be processed for a given client request.

Example

The following command sets configuration options from a PDN DHCP server at the highest priority of *1* for a given client request:

process dhcp-option-from PDN-DHCP priority 1



CHAPTER 44

DHCP Service Configuration Mode Commands

The Dynamic Host Control Protocol (DHCP) Configuration Mode is used to create and manage DHCP service instances for the current context.

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context *context_name* **> dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-dhcp-service)#`

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

- allow, on page 1002
- bind, on page 1003
- default, on page 1005
- dhcp chaddr-validate, on page 1006
- dhcp client-identifier, on page 1007
- dhcp deadtime, on page 1009
- dhcp detect-dead-server, on page 1010
- dhcp ip vrf, on page 1011
- dhcp server, on page 1012
- dhcp server selection-algorithm, on page 1014
- end, on page 1015
- exit, on page 1015
- lease-duration, on page 1015
- lease-time, on page 1016
- max-retransmissions, on page 1017
- retransmission-timeout, on page 1018
- T1-threshold, on page 1019
- T2-threshold, on page 1019

allow

Allows the specified options on the DHCP service.

Product

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > **context** *context_name* > **dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

`[ no ] allow { dhcp-client rapid-commit | dhcp-inform | dhcp-parameter-request-list-option { router | subnet-mask } | dhcp-relay-agent-auth-suboption | dhcp-relay-agent-option | dhcp-server rapid-commit }`

no

Disables an option on the DHCP service.

dhcp-client rapid-commit

Enables support of the rapid commit feature for DHCP client functionality, as defined in RFC 4039.

dhcp-inform

Enables the sending of DHCP inform after configuration for address recovery.

dhcp-parameter-request-list-option { router | subnet-mask }

Enables the sending of DHCP parameter request list option in all outgoing messages.

router: Send DHCP parameter request list option with router flag in all outgoing messages.

subnet-mask: Send DHCP parameter request list option with subnet mask flag in all outgoing messages.

dhcp-relay-agent-auth-suboption

Enables the sending of DHCP relay agent authentication suboption in all outgoing messages.

dhcp-relay-agent-option

Enables the sending of DHCP relay agent option in all outgoing messages.

dhcp-server rapid-commit

Enables support of the rapid commit feature for DHCP server functionality, as defined in RFC 4039.

Usage Guidelines Use this command to enable/disable options on the DHCP service.

Example

The following command enables support of the rapid commit feature for DHCP server functionality:

```
allow dhcp-server rapid-commit
```

bind

Binds the DHCP service to a logical IP interface facilitating the system's connection to the DHCP server. This command also configures traffic from the specified DHCP service bind address to use the specified Multiple Protocol Label Switching (MPLS) labels.

Product

ASN-GW

eWAG

GGSN

HA

P-GW

SAEGW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > **context** *context_name* > **dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

```
bind address ip_address [ nexthop-forwarding-address nexthop_ip_address [
mpls-label input in_mpls_label_value output out_mpls_label_value1 [
out_mpls_label_value2 ] ] ]
no bind address ip_address
```

no

Removes a previously configured binding.

address *ip_address*

Specifies the IP address of an interface in the current context through which communication with the DHCP server occurs.

ip_address must be expressed in IPv4 dotted-decimal notation.

Important In the case of DeWAG service, this IP address must be the same as the IP address configured with the **dhcp server** CLI command under the same DHCP Service Configuration mode. Also, this IP address must match the DeWAG service's IP address so that the WLC can relay the DHCP unicast packets to the DeWAG service IP address and are processed by this DHCP service.

nexthop-forwarding-address *nexthop_ip_address*

Specifies the next hop gateway address for in MPLS network to which the packets with MPLS labels will be forwarded.

nexthop_ip_address must be expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Important In the case of DeWAG service, this option must not be configured.

mpls-label input *in_mpls_label_value*

Specifies the MPLS label to identify inbound traffic destined for the configured DHCP service bind address *ip_address*.

in_mpls_label_value is the MPLS label that will identify inbound traffic destined for the configured DHCP service and must be an integer from 16 through 1048575.

Important This keyword is license-enabled and available with valid MPLS feature license only.

Caution For DHCP over MPLS feature to work in StarOS 9.0 onward the **dhcp ip vrf** command must be configured in DHCP service. Without **dhcp ip vrf** command the DHCP service using MPLS labels will not be started as a part of a DHCP over MPLS configuration. In release 9.0 onward this keyword is a critical parameter for the DHCP-Service. Any change in its value will result in DHCP-service restart and clearing of the existing calls.

Important In the case of DeWAG, this option must not be configured.

output *out_mpls_label_value1* [*out_mpls_label_value2*]

Adds the MPLS label to the outbound traffic sent from the configured DHCP service bind address *ip_address*. The labels *out_mpls_label_value1* and *out_mpls_label_value2* identify the MPLS labels to be added to packets sent from the specified dhcp service bind address.

out_mpls_label_value1 is the inner output label and must be an integer from 16 through 1048575.

out_mpls_label_value2 is the outer output label and must be an integer from 16 through 1048575.

Important This keyword is license-enabled and available with valid MPLS feature license only.

Important In the case of DeWAG, this option must not be configured.

Usage Guidelines

Use this command to associate or tie the DHCP service to a specific logical IP address previously configured in the current context and bound to a port. Once bound, the logical IP address or interface is used in the giaddr field of the DHCP packets.

When this command is executed, the DHCP service is started and begins the process of requesting addresses from the DHCP server and storing them in cache memory for allocation to PDP contexts.

This command can also be used to configure MPLS labels for inbound and outbound traffic through this DHCP address.

Only one interface can be bound to a service.

For DHCP over MPLS feature to work in StarOS 9.0 onward **dhcp ip vrf** command must be configured in DHCP service. Without **dhcp ip vrf** command the DHCP service using MPLS labels will not be started.

Caution As a part of DHCP over MPLS configuration, the **mpls-label input** keyword in the **bind address** command is also a critical parameter for the DHCP-Service. Any change in its value will result in DHCP-service restart and clearing of the existing calls.

Example

The following command binds the DHCP service to the interface with an IP address of 1*192.51.1.210*:

```
bind address 192.51.1.210
```

default

Restores DHCP service parameters to their factory default settings.

Product

GGSN

ASN-GW

HA

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > **context** *context_name* > **dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

```
default { T1-threshold | T2-threshold | dhcp { chaddr-validate |
client-identifier | deadtime | detect-dead-server { consecutive-failures
 } | server selection-algorithm } | lease-duration | max-retransmissions
 | retransmission-timeout }
```

dhcp { deadtime | detect-dead-server { consecutive-failures } | server-selection-algorithm }

Restores the following DHCP parameters to their respective default settings:

- **deadtime**: Default 10 minutes
- **detect-dead-server** { **consecutive-failures** }: Default 5
- **server-selection-algorithm**: Default First-server

lease-duration

Restores the lease-duration parameter to its default setting of 86400 seconds.

max-retransmissions

Restores the max-retransmissions parameter to its default setting of 5.

retransmission-timeout

Restores the retransmission-timeout parameter to its default setting of 3000 milli-seconds.

T1-threshold

Restores the T1-threshold parameter to its default setting of 50%.

T2-threshold

Restores the T2-threshold parameter to its default setting of 88%.

Usage Guidelines

After system parameters have been modified, this command is used to set/restore specific parameters to their default values.

Example

The following command restores the DHCP deadtime parameter to its default setting of 10 minutes:

```
default dhcp deadtime
```

dhcp chaddr-validate

Configures the behavior of the client hardware address (chaddr) validation in DHCP messages.

Product

GGSN

HA

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context *context_name* **> dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-dhcp-service)#`

Syntax Description

`[ default | no ] dhcp chaddr-validate`

default

Validates the chaddr value received in a DHCPACK message with the chaddr value sent in a DHCPREQUEST message.

no

Disables validation of the chaddr value received in DHCPACK message with the chaddr value sent in a DHCPREQUEST message.

Important The chaddr information value in the DHCPACK message will be parsed but not be validated against the value maintained with client. The chaddr information value in DHCPACK will be ignored and not be stored internally.

Usage Guidelines

Use this command to configure behavior relating to the validation of chaddr information validation in the DHCPACK messages.

Example

The following command specifies that the chaddr will not be validated in the DHCP messages:

`no dhcp chaddr-validate`

dhcp client-identifier

Configures the behavior relating to inclusion of a client identifier DHCP option in DHCP messages.

Product

GGSN

HA

HNB-GW

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context *context_name* **> dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

dhcp client-identifier { ike-id | link-layer-identifier | mac-address | msisdn | none }
default dhcp client-identifier

default

Sets the behavior of DHCP client identifier to default – do not to include client identifier option in any DHCP message.

ike-id

Important In Release 20 and later, HNBGW is not supported. This keyword must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Specifies the Internet Key Exchange Protocol version 2 id of HNB as the DHCP client-identifier option in any DHCP message to DHCP server in Discover and Request messages.

Important This keyword is HNB-GW license controlled.

link-layer-identifier

Specifies the subscribers link-layer-identifier as the DHCP client-identifier option in the DHCP message,

mac-address

Specifies the subscribers mac-address as the DHCP client-identifier option in any DHCP message.

msisdn

Specifies that the subscriber's MSISDN be included in the client-identifier option of the relevant DHCP messages. Default: disabled

Important This keyword is GGSN and P-GW/SAEGW license controlled.

none

Specifies that DHCP client-identifier option would not be included in any DHCP messages. This is the default behavior. Default: enabled

Usage Guidelines

Use this command to configure behavior relating to inclusion or exclusion of DHCP client identifier option from DHCP messages.

Example

The following command specifies that DHCP client-identifier option be excluded from DHCP messages:

```
dhcp client-identifier none
```

dhcp deadtime

Configures the amount of time that the system waits prior to re-communicating with a DHCP server that was previously marked as down.

Product

GGSN

ASN-GW

HA

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context *context_name* **> dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

dhcp deadtime *max_time*

max_time

Specifies the maximum amount of time (in minutes) to wait before communicating with a DHCP server that was previously unreachable. *max_time* is an integer value from 1 through 65535. Default: 10

Usage Guidelines

If the system is unable to communicate with a configured DHCP server, after a pre-configured number of failures the system marks the server as being down.

This command specifies the amount of time that the system waits prior to attempting to communicate with the downed server.



Important If all DHCP servers are down, the system will immediately treat all DHCP servers as active, regardless of the deadtime that is specified.

Refer to the **dhcp detect-dead-server** and **max-retransmissions** commands for additional information on the process the system uses to mark a server as down.

Example

The following command configures the system to wait *20* minutes before attempting to re-communicate with a dhcp server that was marked as down:

```
dhcp deadtime 20
```

dhcp detect-dead-server

Configures the number of consecutive communication failures that could occur before the system marks a DHCP server as down.

Product

GGSN

ASN-GW

HA

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context *context_name* **> dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

dhcp detect-dead-server consecutive-failures *max_number*

consecutive-failures *max_number*

Specifies the number of failures that could occur before marking a DHCP server as down as an integer from 1 through 1000. Default: 5

Usage Guidelines

This command works in conjunction with the *max-retransmissions* parameter to set a limit to the number of communication failures that can occur with a configured DHCP server.

The *max-retransmissions* parameter limits the number of attempts to communicate with a server. Once that limit is reached, the system treats it as a single failure. This parameter limits the number of consecutive failures that can occur before the system marks the server as down and communicate with the server of next highest priority.

If all of the configured servers are down, the system ignores the detect-dead-server configuration and attempt to communicate with highest priority server again.

If the system receives a message from a DHCP server that was previously marked as down, the system immediately treats it as being active.

Example

The following command configures the system to allow *8* consecutive communication failures with a DHCP server before it marks it as down:

```
dhcp detect-dead-server consecutive-failures 8
```

dhcp ip vrf

Enables DHCP-over-MPLS support and associates the specific DHCP service with a pre-configured Virtual Routing and Forwarding (VRF) Context instance for virtual routing and forwarding.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > **context** *context_name* > **dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

dhcp ip vrf *vrf_name*
no dhc ip vrf

no

Removes/disassociates configured IP Virtual Routing and Forwarding (VRF) context instance.

vrf_name

Specifies the name of a pre-configured VRF context instance to be associated with a DHCP service. *vrf_name* is the name of a pre-configured VRF context configured in Context Configuration mode and associated with the IP Pool used by the DHCP service.

Usage Guidelines

Use this command to enable the DHCP-over-MPLS support and to associate/disassociate a pre-configured VRF context to a DHCP service for this feature.

By default the VRF is NULL, which means that DHCP service is bound with binding address given by **bind address** command only.

VRF is not a critical parameter for the DHCP Service but bind address is a critical parameter for DHCP Service, and while starting DHCP Service, if this command is configured, then the bind address should be present in that VRF, and If this command is not configured, bind address should be present in the context where DHCP Service is configured.

For the DHCP over MPLS feature to work in StarOS 9.0 onward this command must be configured in the DHCP service. Without this command the DHCP service using MPLS labels will not be started.

Caution As a part of this configuration the **mpls-label input** keyword in the **bind address** command is also a critical parameter for the DHCP-Service. Any change in its value will result in DHCP-service restart and clearing of the existing calls.

Example

Following command associates VRF context instance *dhcp_vrf1* with this DHCP service:

```
dhcp ip vrf dhcp_vrf1
```

dhcp server

Configures DHCP servers with which the DHCP service is to communicate.

Product

ASN-GW

eWAG

GGSN

HA

HNB-GW

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > **context** *context_name* > **dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

```
dhcp server { ip_address | port port_num [ priority priority ]
no dhcp server ip_address
default dhcp port
```

default

Sets the default value of UDP port on DHCP server; 67 for DHCP messaging.

no

Deletes a previously configured DHCP server.

ip_address

Specifies the IP address of the DHCP server expressed in IPv4 dotted-decimal notation.



Important In the case of DeWAG service, this IP address must be the same as the IP address configured with the **bind address** CLI command under the same DHCP Service Configuration mode.

port *port_num*

Specifies the port number to send DHCP messages to non-standard UDP ports of the server if multiple servers are configured.

port_num is an integer from 0 through 65535.



Important In Release 20 and later, HNBGW is not supported. This keyword must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.



Important While configuring HNB-GW for DHCP proxy support, operator must define 61610 as UDP port for DHCP server. The source port used by HNBGW will be standard DHCP port, irrespective of the server port that is configured.

priority *priority*

Specifies the priority of the server if multiple servers are configured.

priority is an integer from 1 through 1000. 1 is the highest priority.



Important In the case of DeWAG, this option must not be configured.

Usage Guidelines

Use this command to configure the DHCP server(s) that the system is to communicate with. Multiple servers can be configured each with their own priority. Up to 20 DHCP servers can be configured.

All DHCP messages are sent/received on UDP port 67.



Important If a server is removed, all calls having an IP address allocated from the server will be released.

Example

The following command configures a DHCP server with an IP address of *192.51.1.200* and a priority of *1*:

```
dhcp server 192.51.1.200 priority 1
```

dhcp server selection-algorithm

Specifies the algorithm used to select DHCP servers with which to communicate when multiple servers are configured.

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

GGSN

ASN-GW

HA

HNB-GW

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context *context_name* **> dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

dhcp server selection-algorithm { first-server | round-robin | use-all }

first-server

Uses the first-server algorithm. This algorithm dictates that the system select the DHCP servers according to their priority starting with the highest priority server. The system communicates with the server of the next highest priority only when the previous server is unreachable. Default: Enabled

round-robin

Uses the round-robin algorithm. This algorithm dictates that the system communicates with the servers in a circular queue according to the server's configured priority starting with the highest priority server. The next request is communicated with the next highest priority server, and so on until all of the servers have been used. At this point, the system starts from the highest priority server. Default: Disabled

use-all

Default: Disabled

This algorithm dictates that the system to communicate with all the DHCP servers configured on system.

Usage Guidelines

Use this command to determine how configured DHCP servers are utilized by the system.

Example

The following command configures the DHCP service to use the round-robin selection algorithm:

```
dhcp server selection-algorithm round-robin
```

end

Exits the 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.

lease-duration

Configures the minimum and maximum allowable lease times that are accepted in responses from DHCP servers.

Product GGSN

ASN-GW

HA

P-GW

SAEGW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > **context** *context_name* > **dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

lease-duration min *min_time* **max** *max_time*

min *min_time*

Specifies the minimum acceptable lease time (in seconds) as an integer from 600 trough 3600. Default: 600

max *max_time*

Specifies the maximum acceptable lease time (in seconds) as an integer from 10800 through 4294967295. Default: 86400

Usage Guidelines

To reduce the call setup time, the system requests IP addresses from the DHCP server in blocks rather than on a call-by-call basis. Each address received has a corresponding lease time, or time that it is valid. The values configured by command represent the minimum and maximum times that the system allows and negotiates for the lease(s).

If the DHCP server responds with values that are out of the range specified by the min and max values, the system accumulates warning statistics. Responses that fall below the minimum value are rejected by the system and the system contacts the DHCP server with the next highest priority. Responses that are greater than the maximum value are accepted.

When half of the lease time has expired, the system automatically requests a lease renewal from the DHCP server. This is configured using the **T1-threshold** command.

Example

The following command configures the minimum allowable lease time for the system to be *1000* and the maximum to be *36000*:

```
lease-duration min 1000 max 36000
```

lease-time

Configures the local DHCP Server lease time in seconds.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > **context** *context_name* > **dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

lease-time *time*
default lease-time

default

Returns the command to its default setting of 600.

time

Specifies the IP address lease time from the local DHCP server (in seconds) as an integer from 600 through 4294967295. Default: 600

Usage Guidelines

Use this command to configure the lease time of the IP address from the local DHCP server.

Example

The following command sets the lease time of the IP address from the local DHCP server to 20 minutes (1200 seconds):

```
lease-time 1200
```

max-retransmissions

Configures the maximum number of times that the system attempts to communicate with an unresponsive DHCP server before it is considered a failure.

Product

GGSN

ASN-GW

HA

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context *context_name* **> dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

max-retransmissions *max_number*

max_number

Specifies the maximum number of re-attempts the system tries when no response is received from a DHCP server. *max_number* is an integer from 1 through 20. Default: 5

Usage Guidelines

This command works in conjunction with the **dhcp detect-dead-server** parameter to set a limit to the number of communication failures that can occur with a configured DHCP server.

When the value specified by this parameter is met, a failure is logged. The **dhcp detect-dead-server** command specifies the number of consecutive failures that could occur before the server is marked as down.

In addition, the **retransmission-timeout** command controls the amount of time between re-tries.

Example

The following command configures the maximum number of times the system re-attempts communication with a DHCP server that is unresponsive to *5*:

```
max-retransmissions 5
```

retransmission-timeout

Configures the amount of time that must pass with no response before the system re-attempts to communicate with the DHCP server.

Product

GGSN

ASN-GW

HA

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context *context_name* **> dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

retransmission-timeout *time*

time

Specifies the time that the system waits (in milliseconds) before reattempting communication with the DHCP server. *time* is an integer from 100 through 20000. Default: 10000

Usage Guidelines

This command works in conjunction with the **max-retransmissions** command to establish a limit on the number of times that communication with a DHCP server is attempted before a failure is logged.

This parameter specifies the time between retries.

Example

The following command configures a retry timeout of *1000* milliseconds:

```
retransmission-timeout 1000
```

T1-threshold

Configures the DHCP T1 timer as a percentage of the allocated IP address lease.

Product

GGSN

ASN-GW

HA

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context *context_name* **> dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

T1-threshold *percentage*

percentage

Specifies the percentage of the allocated IP address lease time at which the DHCP call-line state is changed to "RENEWING". *percentage* is an integer from 40 through 66. Default: 50

Usage Guidelines

This command is used to identify the time at which a subscriber must renew their DHCP lease as a percentage of the overall lease time. (Refer to the **lease-duration** command in this chapter for information on configuring the IP address lease period.)

For example, if the lease-duration was configured to have a maximum value of 12000 seconds, and this command is configured to 40%, then the subscriber would enter the RENEWING state after 4800 seconds.

Example

The following command configures the T1 threshold to *40*%:

```
T1-threshold 40
```

T2-threshold

Configures the DHCP T2 timer as a percentage of the allocated IP address lease.

Product

GGSN

ASN-GW

HA

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context *context_name* **> dhcp-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax Description

T2-threshold *percentage*

percentage

Specifies the percentage of the allocated IP address lease time at which the DHCP call-line state is changed to "REBINDING". *percentage* is an integer from 67 through 99. Default: 88

Usage Guidelines

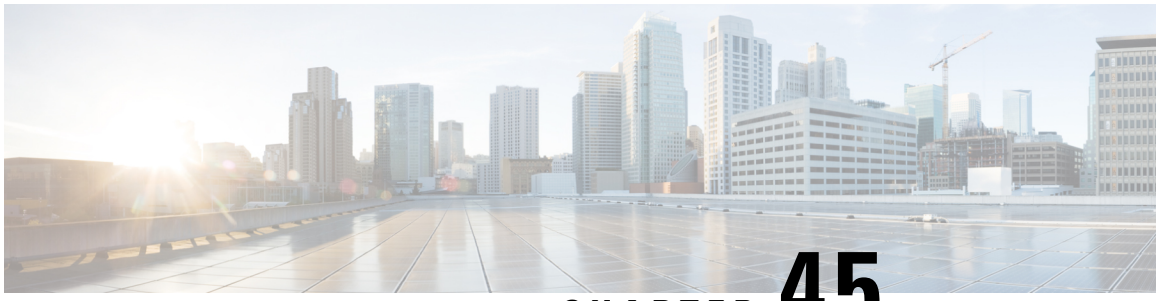
This command is used to identify the time at which a subscriber re-binds their DHCP leased IP address as a percentage of the overall lease time. (Refer to the **lease-duration** command in this chapter for information on configuring the IP address lease period.)

For example, if the lease-duration was configured to have a maximum value of 12000 seconds, and this command is configured to 70%, then the subscriber would enter the REBINDING state after 8400 seconds.

Example

The following command configures the T2 threshold to *70*%:

T2-threshold 70 *70*



CHAPTER 45

DHCPv6 Client Configuration Mode Commands

The Dynamic Host Configuration Protocol (DHCP) for Internet Protocol Version 6 (IPv6) Client Configuration Mode is used to create and manage DHCPv6 client parameters to support DHCPv6-based address assignment.

Command Modes

Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Client Configuration

configure > context *context_name* **> dhcpv6-service** *service_name* **> dhcpv6-client**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-client)#
```

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

- end, on page 1021
- exit, on page 1022
- max-retransmissions, on page 1022
- server-dead-time, on page 1023
- server-ipv6-address, on page 1024
- server-resurrect-time, on page 1025

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-retransmissions

Configures the maximum number of times that the system attempts to communicate with an unresponsive DHCPv6 server before it is considered a failure.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Client Configuration

configure > context *context_name* **> dhcpv6-service** *service_name* **> dhcpv6-client**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-client)#
```

Syntax Description

max-retransmissions *max_number*
default max-retransmissions

default

Returns the command to its default setting of 20.

max_number

Specifies the maximum number of re-attempts the system tries when no response is received from a DHCPv6 server. *max_number* is an integer from 1 through 20. Default: 20

Usage Guidelines

This command works in conjunction with the **detect-dead-server** DHCPv6 service command to set a limit to the number of communication failures that can occur with a configured DHCPv6 service.

When the value specified by this parameter is met, a failure is logged. The **detect-dead-server** DHCPv6 service parameter specifies the number of consecutive failures that could occur before the server is marked as down.

Example

The following command configures the maximum number of times the system re-attempts communication with a DHCPv6 server that is unresponsive to *5*:

max-retransmissions 5

server-dead-time

Configures the amount of time that the client attempts to communicate with an unresponsive DHCPv6 server. DHCPv6 server is considered to be dead if it doesn't respond after given tries from client.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Client Configuration

configure > context *context_name* **> dhcpv6-service** *service_name* **> dhcpv6-client**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-client)#
```

Syntax Description

server-dead-time *dead_time*
default server-dead-time

default

Returns the command to its default setting of 5.

dead_time

Specifies the maximum amount of time (in seconds) that the client attempts to communicate with an unresponsive DHCPv6 server.

dead_time must be an integer value from 1 through 1932100.

Default: 5

Usage Guidelines

Use this command to specify the maximum amount of time (in seconds) that the client attempts to communicate with an unresponsive DHCPv6 server.

This command works in conjunction with the **max-retransmissions** command to set a limit to the number of times that the system attempts to communicate with an unresponsive DHCPv6 server before it is considered a failure.

Example

The following command configures the client to continue trying to communicate with an unresponsive DHCPv6 server for no more than *10* seconds:

```
server-dead-time 10
```

server-ipv6-address

Configures DHCPv6 server(s) with which the DHCPv6 client is to communicate.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Client Configuration

configure > context *context_name* **> dhcpv6-service** *service_name* **> dhcpv6-client**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-client)#
```

Syntax Description

server-ipv6-address *ipv6_address* **[port** *port_number* **] [priority** *priority* **] [-noconfirm]**
no server-ipv6-address *ipv6_address*

no

Deletes a previously configured DHCPv6 server.

ipv6_address

Specifies the IP address of the DHCPv6 server expressed in IPv6 colon-separated-hexadecimal notation.

Default: FF02::1:2

port *port_number*

Specifies the port used for communicating with the DHCPv6 server.

port_number must be an integer from 1 through 65535. If unspecified, the default port is 547.

priority *priority*

Specifies the priority of the server if multiple servers are configured.

priority is an integer from 1 through 1000. 1 is the highest priority.

-noconfirm

Executes the command without prompting for further input from the user.

Usage Guidelines

Use this command to configure the DHCPv6 server(s) that the client is to communicate with. Multiple servers can be configured, each with their own priority.

Example

The following command configures a DHCPv6 server with an IP address of *1234:245:3456:4567:5678:6789:7890:8901*, a port of *300*, and a priority of *1*:

```
server-ipv6-address 1234:245:3456:4567:5678:6789:7890:8901 port 300
priority 1
```

server-resurrect-time

Configures the amount of time that a DHCPv6 client waits before considering a dead DHCPv6 server alive again.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Client Configuration

configure > context *context_name* **> dhcpv6-service** *service_name* **> dhcpv6-client**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-client)#
```

Syntax Description

server-resurrect-time *revive_time*
default server-resurrect-time

default

Returns the command to its default setting of 20.

revive_time

Specifies the maximum amount of time (in seconds) that a DHCPv6 client waits before considering a dead DHCPv6 server alive again.

*revive_time*must be an integer value from 1 through 1932100.

Default: 20

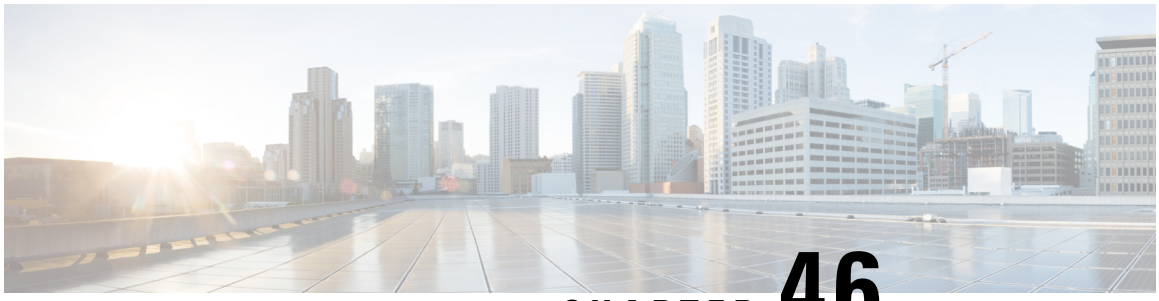
Usage Guidelines

Use this command to specify the amount of time that a DHCPv6 client waits before considering a dead DHCPv6 server alive again.

Example

The following command configures the client to wait *25* seconds before considering a dead DHCPv6 server alive again:

```
server-resurrect-time 25
```



CHAPTER 46

DHCPv6 Server Configuration Mode Commands

The Dynamic Host Configuration Protocol (DHCP) for Internet Protocol Version 6 (IPv6) Server Configuration Mode is used to create and manage DHCPv6 server parameters to support DHCPv6-based address assignment.

Command Modes

Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Server Configuration

configure > context *context_name* **> dhcpv6-service** *service_name* **> dhcpv6-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-server)#
```

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

- end, on page 1027
- exit, on page 1028
- ipv6, on page 1028
- preferred-lifetime, on page 1029
- prefix-delegation, on page 1029
- rebind-time, on page 1030
- renew-time, on page 1031
- valid-lifetime, on page 1032

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.

ipv6

Configures M/O flag for neighbor discovery protocol.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Server Configuration

configure > context *context_name* **> dhcpv6-service** *service_name* **> dhcpv6-server**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-dhcpv6-server)#`

Syntax Description

ipv6 nd { managed-config-flag | other-config-flag }

nd { managed-config-flag | other-config-flag }

Configure M/O flag for neighbor discovery protocol.

managed-config-flag: Configure M flag.

other-config-flag: Configure O flag.

Usage Guidelines

Use this command to specify the M/O flag for neighbor discovery protocol.

Example

The following command configures the M flag for neighbor discovery protocol:

ipv6 nd managed-config-flag

preferred-lifetime

Configures the preferred lifetime for prefixes assigned by the DHCPv6 service.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Server Configuration

configure > context *context_name* **> dhcpv6-service** *service_name* **> dhcpv6-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-server)#
```

Syntax Description

preferred-lifetime *pref_lifetime*
default preferred-lifetime

default

Returns the command to its default setting of 900.

pref_lifetime

Specifies the preferred lifetime (in seconds) for prefixes assigned by the DHCPv6 service.

pref_lifetime must be an integer value from 1 through 1932100.

Default: 900

Usage Guidelines

Use this command to specify the preferred lifetime for prefixes assigned by the DHCPv6 service.

Example

The following command configures the preferred lifetime for *1001* seconds:

preferred-lifetime 1001

prefix-delegation

Configures the lifetime parameters that can be used by a particular DHCPv6 service to allocate delegated prefixes.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Server Configuration

configure > context *context_name* **> dhcpv6-service** *service_name* **> dhcpv6-server**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-dhcpv6-server)#`

Syntax Description **prefix-delegation valid-lifetime** *valid_lifetime* **preferred-lifetime** *pref_lifetime*

valid-lifetime *valid_lifetime*

Specifies the valid lifetime (in seconds) for prefixes for which the delegated prefix is valid. After this is exhausted, delegated prefix is deemed invalid.

pref_lifetime must be an integer value from 1 through 1932100.

Default: 900

preferred-lifetime *pref_lifetime*

Specifies the preferred lifetime (in seconds) for which new connections can be established by these delegated prefixes. Once it is exhausted, no new connections can be made.

pref_lifetime must be an integer value from 1 through 1932100.

Default: 900

Usage Guidelines Use this command to specify the valid and preferred lifetime for prefixes assigned by the DHCPv6 service for prefix delegation.

Example

The following command configures the valid lifetime to *1500* seconds and preferred lifetime to *1200* seconds for prefix delegation:

```
prefix-delegation valid-lifetime 1500 preferred-lifetime 1200
```

rebind-time

Configures the rebind time for prefixes assigned by the DHCPv6 service.

Product GGSN

P-GW

SAEGW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Server Configuration

configure > context *context_name* **> dhcpv6-service** *service_name* **> dhcpv6-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-server)#
```

Syntax Description

rebind-time *rebind_time*
default rebind-time

default

Returns the command to its default setting of 900.

rebind_time

Specifies the rebind time (in seconds) for prefixes assigned by the DHCPv6 service.

rebind_time must be an integer value from 1 through 1932100.

Default: 900

Usage Guidelines

Use this command to specify the rebind time for prefixes assigned by the DHCPv6 service.

Example

The following command configures the rebind time for *1001* seconds:

rebind-time 1001

renew-time

Configures the renewal time for prefixes assigned by the DHCPv6 service.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Server Configuration

configure > context *context_name* **> dhcpv6-service** *service_name* **> dhcpv6-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-server)#
```

Syntax Description

renew-time *renewal_time*
default renew-time

default

Returns the command to its default setting of 900.

renewal_time

Specifies the renewal time (in seconds) for prefixes assigned by the DHCPv6 service.

renewal_time must be an integer value from 1 through 1932100.

Default: 900

Usage Guidelines

Use this command to specify the renewal time for prefixes assigned by the DHCPv6 service.

Example

The following command configures the renewal time for *1001* seconds:

```
renew-time 1001
```

valid-lifetime

Configures the valid lifetime for prefixes assigned by the DHCPv6 service.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Server Configuration

configure > context *context_name* **> dhcpv6-service** *service_name* **> dhcpv6-server**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-server)#
```

Syntax Description

valid-lifetime *valid_lifetime*
default valid-lifetime

default

Returns the command to its default setting of 900.

valid_lifetime

Specifies the valid lifetime (in seconds) for prefixes assigned by the DHCPv6 service.

valid_lifetime must be an integer value from 1 through 1932100.

Default: 900

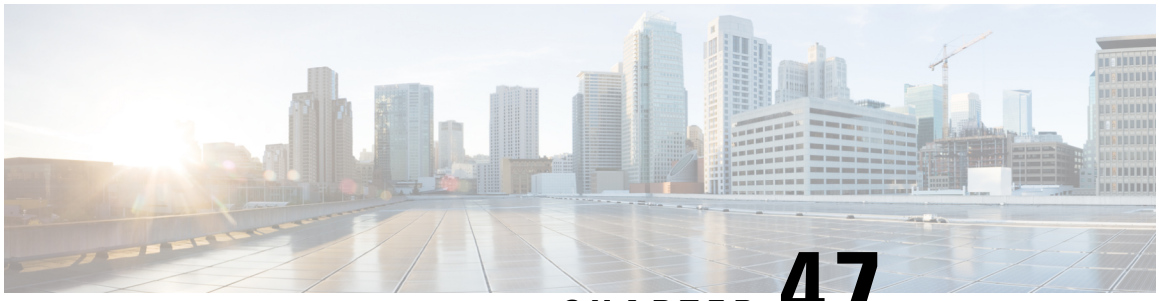
Usage Guidelines

Use this command to specify the valid lifetime for prefixes assigned by the DHCPv6 service.

Example

The following command configures the valid lifetime for *1001* seconds:

```
valid-lifetime 1001
```



CHAPTER 47

DHCPv6 Service Configuration Mode Commands

The Dynamic Host Configuration Protocol (DHCP) for Internet Protocol Version 6 (IPv6) Service Configuration Mode is used to create and manage DHCPv6 service instances for the current context.

Command Modes

Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration

configure > context *context_name* **> dhcpv6-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-service)#
```

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

- bind, on page 1035
- deadtime, on page 1036
- detect-dead-server, on page 1037
- dhcpv6-client, on page 1038
- dhcpv6-server, on page 1039
- end, on page 1040
- exit, on page 1040
- server, on page 1040

bind

Binds the DHCPv6 service to a logical IP interface facilitating the system's connection to the DHCPv6 server.

Product

GGSN

P-GW

SAEGW

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration

configure > context *context_name* **> dhcpv6-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-dhcpv6-service)#`

Syntax Description

`bind address` *`ipv6_address`* **`[ port`** *`port_number`* **`]`**
`no bind address`

no

Removes a previously configured binding.

address *ipv6_address*

Specifies the IP address of an interface in the current context through which the communication with the DHCPv6 server occurs. *ipv6_address* must be expressed in IPv6 colon-separated-hexadecimal notation.

port *port_number*

Specifies the listen port and is used to start the DHCPv6 server bound to it.

port_number must be an integer from 1 through 65535. If unspecified, the default port is 547.

Usage Guidelines

Use this command to associate or tie the DHCPv6 service to a specific logical IP address previously configured in the current context and bound to a port.

When this command is executed, the DHCPv6 service is started and begins the process of requesting addresses from the DHCPv6 server and storing them in cache memory for allocation to PDP contexts.

Only one interface can be bound to a service.

Example

The following command binds the DHCPv6 service to the interface with an IP address of *1234:245:3456:4567:5678:6789:7890:8901*:

`bind address 1234:245:3456:4567:5678:6789:7890:8901`

deadtime

Configures the amount of time that the system waits prior to re-communicating with a DHCPv6 server that was previously marked as down.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration

configure > context *context_name* **> dhcpv6-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-service)#
```

Syntax Description

deadtime *max_time*
default deadtime

default

Returns the command to its default setting of 120.

max_time

Specifies the maximum amount of time (in seconds) to wait before communicating with a DHCPv6 server that was previously unreachable.

max_time must be an integer value from 1 through 1932100.

Default: 120

Usage Guidelines

If the system is unable to communicate with a configured DHCPv6 server, after a pre-configured number of failures the system marks the server as being down.

This command specifies the amount of time that the system waits prior to attempting to communicate with the downed server.



Important If all DHCPv6 servers are down, the system will immediately treat all DHCPv6 servers as active, regardless of the **deadtime** that is specified.

Refer to the **detect-dead-server** and **max-retransmissions** commands for additional information on the process the system uses to mark a server as down.

Example

The following command configures the system to wait *600* seconds before attempting to re-communicate with a DHCPv6 server that was marked as down:

```
deadtime 600
```

detect-dead-server

Configures the number of consecutive communication failures that could occur before the system marks a DHCPv6 server as down.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration

configure > context *context_name* **> dhcpv6-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-service)#
```

Syntax Description

detect-dead-server consecutive-failures *max_number*
default detect-dead-server consecutive-failures

default

Returns the command to its default setting of 5.

consecutive-failures *max_number*

Specifies the number of failures that could occur before marking a DHCPv6 server as down.

max_number must be an integer from 1 through 1000.

Default: 5

Usage Guidelines

This command works in conjunction with the **max-retransmissions** DHCPv6 client command to set a limit to the number of communication failures that can occur with a configured DHCPv6 server.

The **max-retransmissions** DHCPv6 client parameter limits the number of attempts to communicate with a server. Once that limit is reached, the system treats it as a single failure. This parameter limits the number of consecutive failures that can occur before the system marks the server as down and communicate with the server of next highest priority.

If all of the configured servers are down, the system ignores the **detect-dead-server** configuration and attempts to communicate with the highest priority server again.

If the system receives a message from a DHCPv6 server that was previously marked as down, the system immediately treats it as being active.

Example

The following command configures the system to allow *8* consecutive communication failures with a DHCPv6 server before it marks it as down:

detect-dead-server consecutive-failures 8

dhcpv6-client

Enters the DHCPv6 Client Configuration Mode.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration

configure > context *context_name* **> dhcpv6-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-service)#
```

Syntax Description

dhcpv6-client

Usage Guidelines

Use this command to cause the system to enter the DHCPv6 Client Configuration Mode where parameters are configured for the DHCPv6 client.

Entering this command results in the following prompt:

```
[context_name]hostname(config-dhcpv6-client)#
```

DHCPv6 Client Configuration Mode commands are defined in the *DHCPv6 Client Configuration Mode Commands* chapter.

dhcpv6-server

Enters the DHCPv6 Server Configuration Mode.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration

configure > context *context_name* **> dhcpv6-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-service)#
```

Syntax Description

dhcpv6-server

Usage Guidelines

Use this command to cause the system to enter the DHCPv6 Server Configuration Mode where parameters are configured for the DHCPv6 server.

Entering this command results in the following prompt:

```
[context_name]hostname(config-dhcpv6-server)#
```

DHCPv6 Server Configuration Mode commands are defined in the *DHCPv6 Server Configuration Mode Commands* chapter.

Important Multiple DHCPv6 servers can be configured by entering the **dhcpv6-server** command multiple times. A maximum of 3 DHCPv6 servers can be configured.

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

Configures DHCPv6 servers with which the DHCPv6 service is to communicate and specifies the algorithm used to select DHCPv6 servers with which to communicate when multiple servers are configured.

Product GGSN

P-GW

SAEGW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration

configure > **context** *context_name* > **dhcpv6-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-service)#
```

Syntax Description

```
server { ipv6_address [ priority priority ] | selection-algorithm {
first-server | round-robin } }
default server selection-algorithm
no server ipv6_address
```

default

Uses the first-server algorithm.

no

Deletes a previously configured DHCPv6 server.

ipv6_address

Specifies the IP address of the DHCPv6 server expressed in IPv6 colon-separated-hexadecimal notation.

priority *priority*

Specifies the priority of the server if multiple servers are configured.

priority is an integer from 1 through 1000. 1 is the highest priority.

selection-algorithm { first-server | round-robin }

Specifies the algorithm used to select DHCPv6 servers with which to communicate when multiple servers are configured.

first-server: Uses the first-server algorithm. This algorithm dictates that the system select the DHCPv6 servers according to their priority, starting with the highest priority server. The system communicates with the server of the next highest priority only when the previous server is unreachable.

Default: Enabled

round-robin: Uses the round-robin algorithm. This algorithm dictates that the system communicates with the servers in a circular queue according to the server's configured priority, starting with the highest priority server. The next request is communicated with the next highest priority server, and so on until all of the servers have been used. At this point, the system starts from the highest priority server.

Default: Disabled

Usage Guidelines

Use this command to configure the DHCPv6 server(s) that the system is to communicate with. Multiple servers can be configured, each with their own priority. Up to 20 DHCPv6 servers can be configured.

In addition, use this command to determine how configured DHCPv6 servers are utilized by the system.

All DHCP messages are sent/received on UDP port 67.

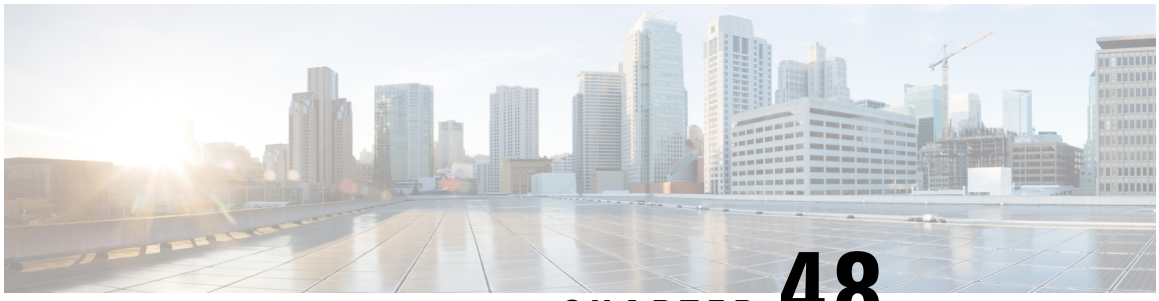


Important If a server is removed, all calls having an IP address allocated from the server will be released.

Example

The following command configures a DHCPv6 server with an IP address of *1234:245:3456:4567:5678:6789:7890:8901* and a priority of *1*:

```
server 1234:245:3456:4567:5678:6789:7890:8901 priority 1
```



CHAPTER 48

Diameter Endpoint Configuration Mode Commands

Diameter Endpoint Configuration Mode is accessed from the Context Configuration Mode. The base Diameter protocol operation is configured in this mode.

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

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

- app-level-retransmission, on page 1044
- associate, on page 1045
- cea-timeout, on page 1046
- connection retry-timeout, on page 1047
- connection timeout, on page 1048
- description, on page 1049
- destination-host-avp, on page 1049
- device-watchdog-request, on page 1051
- dpa-timeout, on page 1052
- dscp, on page 1052
- dynamic-peer-discovery, on page 1053
- dynamic-peer-failure-retry-count, on page 1054
- dynamic-peer-realm, on page 1055
- dynamic-route, on page 1056
- end, on page 1057
- exit, on page 1057
- load-balancing-algorithm, on page 1057
- max-outstanding, on page 1058
- origin address, on page 1059

- origin host, on page 1059
- origin realm, on page 1061
- osid-change , on page 1062
- peer, on page 1063
- peer-backoff-timer, on page 1066
- reconnect-timeout, on page 1067
- response-timeout, on page 1068
- rlf-template, on page 1069
- route-entry, on page 1071
- route-failure, on page 1072
- server-mode, on page 1074
- session-id include imsi, on page 1075
- use-proxy, on page 1076
- vsa-support, on page 1077
- watchdog-timeout, on page 1078

app-level-retransmission

This command enables/disables setting "T" bit and retaining the same End-to-End Identifier (E2E ID) for application-level retransmissions.

Product

eHRPD

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ default | no ] app-level-retransmission { retain-e2e | set-retransmission-bit }`

default

Configures this command with the default setting.

The default behavior is not to set the retransmission bit for a retried Diameter message.

retain-e2e

Sends the same End-to-End Identifier for a retried Diameter message.

set-retransmission-bit

Sets the retransmission bit for retried Diameter messages.

Usage Guidelines

Use this command to enable application-level transmission with "T" bit set.

'T' bit setting is done only for DIABASE protocol-based rerouting and not for application-based retransmissions. In order to identify such retransmissions, the server expects the T bit to be set at all levels (both DIABASE and application) of retransmission, which can be achieved with this CLI command.

In addition to using this CLI command for setting the T-bit in a retried message, it is also possible to retain the same End-to-End ID. With this feature turned on, the server can detect any duplicate/re-transmitted messages sent by Diameter clients or agents. Note that this feature is applicable to Gy and Rf messages as well.

Similar CLI command for setting T-bit is also present under Credit Control Group configuration mode, which when configured will take effect for Gy messages else endpoint configuration will be used.

Example

The following command specifies to set retransmission bit and retain e2e:

```
app-level-retransmission set-retransmission-bit retain-e2e
```

associate

This command associates/disassociates a Stream Control Transmission Protocol (SCTP) parameter template with the Diameter endpoint.

Product

ePDG

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
associate sctp-parameters-template template_name
no associate sctp-parameters-template
```

no

Disassociates an SCTP parameter template with the Diameter endpoint.

sctp-parameters-template *template_name*

Associates a previously created SCTP parameter template with the Diameter endpoint. *template_name* specifies the name for a pre-configured SCTP parameter template. For more information on SCTP parameter templates,

refer to the **sctp-param-template** command in the *Global Configuration Mode Commands* chapter in this guide.

Usage Guidelines

Use this command to associate a configured SCTP parameter template with the Diameter endpoint.

The SCTP parameter template allows for SCTP timer values to be configured for the interface using the Diameter endpoint configuration. For more information on SCTP parameters, refer to the *SCTP Parameter Template Configuration Mode Commands* chapter in this guide.



Important Only one SCTP parameter template can be associated with the Diameter endpoint configuration. The SCTP parameter template should be configured prior to issuing this command.



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*.

Only the following parameters from the template will be associated with the endpoint. When no SCTP parameter template is associated with the endpoint, the following default values are used:

sctp-cookie-life *60000* (default for the parameter template as well)

sctp-max-init-retx *5* (default for the parameter template as well)

sctp-max-path-retx *10* (default in the parameter template is 5)

sctp-rto-initial *3000* (default for the parameter template as well)

sctp-rto-max *60000* (default for the parameter template as well)

sctp-rto-min *1000* (default for the parameter template as well)

sctp-sack-period *200* (default for the parameter template as well)

timeout sctp-heart-beat *30* (default for the parameter template as well)

Example

The following command associates a pre-configured SCTP parameter template called *sctp1* to the Diameter endpoint:

```
associate sctp-parameters-template sctp1
```

cea-timeout

This command configures the Capabilities-Exchange-Answer (CEA) message timeout duration for Diameter sessions.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

cea-timeout *timeout*
default cea-timeout

default

Configures this command with the default setting.

Default: 30 seconds

timeout

Specifies the timeout duration (in seconds) to make the system wait for this duration for a CEA message. *timeout* must be an integer from 1 through 120.

Usage Guidelines

Use this command to configure the CEA timer, i.e., how long to wait for the Capabilities-Exchange-Answer message.

Example

The following command sets the Diameter CEA timeout to *16* seconds:

cea-timeout 16

connection retry-timeout

This command configures the Diameter Connection Retry Timeout parameter.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

connection retry-timeout *timeout*
default connection retry-timeout

default

Configures this command with the default setting.

Default: 30 seconds

timeout

Specifies the connection retry timeout duration in seconds. The timeout must be an integer from 1 through 3600.

Usage Guidelines

Use this command to configure the Diameter Connection Retry Timeout parameter.

Example

The following command sets the Diameter Connection Retry Timer to *120* seconds:

```
connection retry-timeout 120
```

connection timeout

This command configures the Diameter Connection Timeout parameter.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
connection timeout timeout
default connection timeout
```

default

Configures this command with the default setting.

Default: 30 seconds

timeout

Specifies the connection timeout duration (in seconds) as an integer from 1 through 30.

Usage Guidelines

Use this command to configure the Diameter Connection Timeout parameter.

Example

The following command sets the Diameter connection timeout to *16* seconds:

```
connection timeout 16
```

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.

destination-host-avp

This command controls encoding of the Destination-Host AVP in initial/retried requests.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > **context** *context_name* > **diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
destination-host-avp { always | initial-request [ redirected-request ] |
 retried-request [ redirected-request ] | session-binding [
redirected-request ] }
default destination-host-avp
```

default

Configures this command with the default setting. Default: session-binding

always

Includes the Destination-Host AVP in all types of request messages.

session-binding [redirected-request]

Includes the Destination-Host AVP when the Diameter session is bound with a host.

redirected-request: Includes the Destination-Host AVP in any redirected request message when the Diameter session is bound with a host.

initial-request

Includes the Destination-Host AVP in an initial request but not in a retried request.

redirected-request: Includes the Destination-Host AVP in any redirected request message.

retried-request

Includes the Destination-Host AVP in a retried request but not in an initial request.

redirected-request: Includes the Destination-Host AVP in any redirected request message.

Usage Guidelines

Use this command to control encoding of the Destination-Host AVP in initial/retried requests.

This command has been introduced in release 12.0, in earlier releases, the Destination-Host AVP is not sent in session-setup/initial request (first message sent on that interface for that subscriber. The message will vary with different interfaces. For example, CCR-Initial for Gy, ACR-start for Rf, and so on). Also, Destination-Host AVP was not sent in retried requests. For example, CCR-Update failed to be responded by server. The message was retransmitted to alternate server.

In both these scenarios, it is not known which server will respond to the initial/retried message, so the Destination-Realm is encoded but not the Destination-Host. Only after a response for this message is received from one of the hosts present in that realm, the session is considered to be BOUND with that server. Any message sent after this binding will have the Destination-Host AVP encoded.

If the application has selected one of the servers using application-level commands like the **peer-select** command for credit-control or the **diameter authentication** or **accounting server** command in a AAA group, encoding of this AVP in initial/retried request is configurable.

When an application receives the Result-Code 3006 -DIAMETER_REDIRECT_INDICATION from the AAA server, the Diameter request message is forwarded to the Redirect-Host specified in the server's response. The message gets routed properly in case the Diameter host is directly connected to the AAA server. If there is a DRA between P-GW/ePDG and AAA server, the message goes into a loop as DRA always routes the packet to the AAA server which had redirected the message. To avoid the unnecessary looping, a new configurable option **redirected-request**is added to the **destination-host-avp** CLI command. This new option allows encoding the Destination-Host AVP in any type of Diameter redirected messages.

In releases prior to 19, the Destination-Host AVP was encoded in the redirected message only if the original request included Destination-Host AVP. In release 19 and beyond, encoding of Destination-Host AVP in redirected message is based on the configuration of **redirected-request** in the **destination-host-avp** command. If the CLI command is enabled, Destination-Host AVP will be included in any type of Diameter redirected messages. As per the current implementation, it is not possible to send retried messages to a different host using the same peer. This behavior is applicable for normal retry and failure-handling scenarios.

Since any redirected request is considered as retried request, if the option "**retried-request**" is used, by default Update (Interims) or Terminate (Stop) redirected-request will be encoded with Destination-Host AVP without

the "**redirected-request**" option being configured. The reason to configure "**redirected-request**" as part of "**retried-request**" option is, in case of Initial-Retried request the Destination-Host AVP is not encoded if "**retried-request**" option alone is configured. To enable encoding Destination-Host AVP for Initial-Retried request, "**redirected-request**" is supported as an extension to "**retried-request**" as well.

Example

The following command specifies to include the Destination-Host AVP in initial request but not in retried request:

```
destination-host-avp initial-request
```

device-watchdog-request

This command manages the transport failure algorithm and configures the number of Device Watchdog Requests (DWRs) that will be sent before a connection is closed.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > **context** *context_name* > **diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

device-watchdog-request max-retries *retry_count*
default device-watchdog-request max-retries

default

Configures this command with the default setting. Default: 1

retry_count

Specifies the maximum number of DWRs, and it must be an integer from 1 through 10.

Usage Guidelines

Use this command to configure the number of DWRs to be sent before closing the connection from a Diameter endpoint.

Example

The following command sets the DWRs to *3*:

```
device-watchdog-request max-retries 3
```

dpa-timeout

This command configures the Disconnect-Peer-Answer (DPA) message timeout duration for Diameter sessions.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

dpa-timeout *timeout*
default dpa-timeout

default

Configures this command with the default setting.

Default: 30 seconds

timeout

Specifies the DPA message timeout duration (in seconds) as an integer from 1 through 60.

Usage Guidelines

Use this command to set the timer for DPA message timeout during Diameter connection session. This makes the system wait for this duration for DPA message.

Example

The following command sets the Diameter DPA timeout to *16* seconds:

dpa-timeout 16

dscp

This command sets the Differential Services Code Point (DSCP) value in the IP header of the Diameter messages sent from the Diameter endpoint.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

dscp { *value* | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }
default dscp

value

Specifies to configure a unique DSCP as an integer in the range of 0 through 63.

af*xx*

Specifies the use of an assured forwarding *xx* per hop behavior (PHB).

be

Specifies the use of best effort forwarding PHB. This is the default.

cs*x*

Specifies the use of class selector *x* per PHB.

ef

Specifies the use of expedited forwarding PHB.

Usage Guidelines

Use this command to set the DSCP in the IP header of the Diameter messages sent from the Diameter endpoint. In addition to the recommended PHBs the user may configure their own DSCP as an integer in the range of 0 through 63.

Example

The following command sets the DSCP to *be*:

dscp be

dynamic-peer-discovery

This command configures the system to dynamically locate peer Diameter servers by means of DNS.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
dynamic-peer-discovery [ protocol { sctp | tcp } ]
{ default | no } dynamic-peer-discovery
```

default

Configures this command with the default setting.

Default: disabled

no

Removes the configuration.

protocol { sctp | tcp }

Configures peer discovery to use a specific protocol. Default: TCP

sctp: Uses Streaming Control Transmission Protocol (SCTP) for peer discovery.

tcp: Uses Transmission Control Protocol (TCP) for peer discovery.

Usage Guidelines

Use this command to configure the system to dynamically locate peer Diameter servers by means of DNS.

Configure the **dynamic-peer-realm** command to locate Diameter servers using Naming Authority Pointer (NAPTR) queries. If the peer realm command is not configured, configuring this command will still allow applications to trigger an NAPTR query on their chosen realms.

The preferred transport protocol is TCP to resolve instances were multiple NAPTR responses with the same priority are received. The one using the TCP transport protocol will be chosen. If the transport protocol is configured through the CLI, then the configured protocol is given preference.

The IP address version will be the same as that of the origin host address configured for the endpoint. For IPv4 endpoints, A-type DNS queries will be sent to resolve Fully Qualified Domain Names (FQDNs). For IPv6 endpoints, AAAA-type queries are sent.

Example

The following command configures the system to dynamically locate peer Diameter servers using SCTP:

```
dynamic-peer-discovery protocol sctp
```

dynamic-peer-failure-retry-count

This command configures the number of times the system will attempt to connect to a dynamically discovered Diameter peer.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

dynamic-peer-failure-retry-count *no_of_retries*
default dynamic-peer-failure-retry-count

default

Configures this command with the default setting.

Default: 8

no_of_retries

Specifies the number of retry attempts to connect to a dynamically discovered Diameter peer. The value must be an integer from 0 through 255.

Usage Guidelines

Use this command to configure the number of times the system attempts to connect to a dynamically discovered Diameter peer.

After the specified number of attempts if the peer is still not open, the peer is moved into blacklist and other peers are tried. The blacklisted peer will be retried after a time period of one hour.

Example

The following command sets the retry attempts to *10*:

dynamic-peer-failure-retry-count 10

dynamic-peer-realm

This command configures the name of the realm where peer Diameter servers can be dynamically discovered.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > **context** *context_name* > **diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] dynamic-peer-realm *realm_name*

no

Removes the specified dynamic peer realm name from this endpoint configuration.

realm_name

Specifies the name of the peer realm where peer Diameter server are to be dynamically discovered. *realm_name* must be an existing realm, and must be an alphanumeric string of 1 through 127 characters.

Usage Guidelines

Use this command to locate Diameter servers using Naming Authority Pointer (NAPTR) queries.

Multiple realms can be configured. Even if the **dynamic-peer-discovery** command is not enabled, the realm configuration(s) will trigger dynamic peer discovery on all diabase instances.

Example

The following command configures a peer realm, used for dynamic peer discovery, with a name of *service-provider.com*:

```
dynamic-peer-realm service-provider.com
```

dynamic-route

This command configures the expiration time for dynamic routes created after a Diameter destination host is reached.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
dynamic-route expiry-timeout value
default dynamic-route expiry-timeout
```

default

Configures this command with the default setting. Default: 86400 seconds (1 day)

value

Specifies the time (in seconds) that a dynamic route to a Diameter host will expire. The value must be an integer from 1 through 86400000.

Usage Guidelines

Use this command to set expiration times for dynamic routes that are set up after a Diameter host has been reached.

Example

The following command sets the dynamic route expiration to *43200* seconds:

```
dynamic-route expiry-timeout 43200
```

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-algorithm

This command configures the behavior for load balancing Diameters peers in the event of a failure of an active server.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > **context** *context_name* > **diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **load-balancing-algorithm { highest-weight | lowest-weight-borrowing min-active-servers** *number* **}**
default load-balancing-algorithm

default

Configures this command with the default setting.

Default: **highest-weight**

highest-weight

Selects an idle server with the highest weight in failure scenarios. The highest-weight load balancing algorithm applies only to hosts with the same realm. In the case of multiple realms, load-balancing works based on a round-robin algorithm, and the weight value configured in the route entry gets ignored.

lowest-weight-borrowing min-active-servers *number*

Borrows an idle server with the lowest weight and adds it to the group of servers where load balancing is performed. *number* specifies the number of servers that must always be available as active for load balancing. *number* must be an integer from 2 through 4000.

Usage Guidelines

Use this command to configure the behavior for load balancing Diameter peers in the event of a failure of an active server.



Note In Gy, the Load-balancing is not supported if **diameter peer-select** command is configured under the credit control group, which selects a specific peer.

Example

The following command configures the load balancing behavior for Diameter peers to borrowing minimally active servers (lower weight) and maintaining an active server group of *30* servers:

```
load-balancing-algorithm lowest-weight-borrowing min-active-servers 30
```

max-outstanding

This command configures the maximum number of Diameter messages that any application can send to any one peer, while awaiting responses.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

max-outstanding *messages*
{ default | no } max-outstanding

no

Disables the maximum outstanding messages configuration.

default

Configures this command with the default setting.

Default: 256

messages

Specifies the maximum outstanding peer transmit window size setting. The input must be an integer from 1 through 4096.

Note that, in StarOS 14.1 and later releases, though the configuration allows up to 4K Diameter messages, it is restricted to queue up to 512 Diameter messages per peer to avoid any delay in the recovery of Diameter sessions.

Usage Guidelines

Use this command to set the unanswered Diameter messages that any application may send to any one peer, while awaiting responses. An application will not send any more Diameter messages to that peer until it has disposed of at least one of those queued messages. It disposes a message by either receiving a valid response or by discarding the message due to no response.

Example

The following command sets the Diameter maximum outstanding messages setting to *1024*:

```
max-outstanding 1024
```

origin address

This command has been deprecated. See the origin host, on page 1059 and origin realm, on page 1061 commands.

origin host

This command sets the origin host for the Diameter endpoint.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

origin host *host_name* **address** *ipv4_address | ipv6_address* **[port** *port_number* **] [accept-incoming-connections] [address** *ipv4_address_secondary |*

ipv6_address_secondary **]**
no origin host *host_name* **address** *ipv4_address* | *ipv6_address* **[port** *port_number* **]**

no

Removes the origin host configuration.

origin host *host_name*

Specifies the host name to bind the Diameter endpoint. *host_name* must be the local Diameter host name. The host name must be an alphanumeric string of 1 through 64 characters.

The host name must be an alphanumeric string of 1 through 255 characters.

address *ipv4_address | ipv6_address*

Specifies the IP address to bind the Diameter endpoint using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. This address must be one of the addresses of a chassis interface configured within the context in which Diameter is configured.

port *port_number*

Specifies the port number for the Diameter endpoint (on inbound connections). The port number must be an integer from 1 through 65535. Default: 3868



Important When multiple diamproxies are running in the chassis, it is highly recommended that port number is NOT specified.

Port number in the origin host should be configured only when the chassis is running in server mode, i.e. when **accept-incoming-connections** is configured.

In this case it will open a listening socket on the specified port. For configurations where chassis is operating as a client, port number should not be included. In this case, a random source port will be chosen for outgoing connections. This is applicable for both with or without multi-homing.



Important Currently if multi-homing is configured, then the specified port is used instead of randomly chosen port. This is done so that application knows which port is used by the kernel as it will have to use the same port while adding/removing IP address from the association. Nevertheless, configuring port number in origin host for client mode is not supported.

accept-incoming-connections

Accepts inbound connection requests for the specified host (enables server mode).



Important MME only: This keyword is not supported. The MME acts only in client mode; setting the S6a (HSS) endpoint to 'accept-incoming-connections' will prevent the initialization of the S6a connection to the HSS.

address *ipv4_address_secondary | ipv6_address_secondary*

Specifies the secondary bind address for the Diameter endpoint in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. This address must be one of the addresses of a chassis interface configured within the context in which Diameter is configured.

When a secondary IP address is dynamically added or removed from an SCTP association, the affected host notifies its peer of the change in configuration using the Address Configuration Change Chunk (ASCONF) chunk without terminating the SCTP connection.

Usage Guidelines

Use this command to set the bind address for the Diameter endpoint.

Diameter agent on the chassis listens to standard TCP port 3868 and also supports the acceptance of any incoming TCP connection from external server.

The command **origin host** *host-name* must be entered exactly once. Alternatively, the **origin host** *host-name* **address** *ipv4/ipv6_address* **[port** *port_number* **]** command may be entered one or more times.

The host names should be configured such that it is unique across all endpoints within the system. The host names and address values or address/port combinations should also be unique across all endpoints within the system.

The host names should be unique only within an endpoint.

This command allows the user to configure multiple endpoints with the same origin host name. That is, it allows multiple endpoints (specifically that are used under S6a, S13 and SLg) to share the same Origin Host/Origin Realm.



Important Please be noted it is not possible to associate/map origin-host across endpoints to a specific diamproxy instance or maintain a constant origin host–instance mapping. Origin hosts are a pool of host entries and will be assigned on need basis. Endpoint in itself is an independent encapsulated entity.

Example

The following command sets the origin host name to *test* and the IP address to *209.165.200.225*:

```
origin host test address 209.165.200.225
```

origin realm

This command configures the realm to use in conjunction with the origin host.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] origin realm *realm_name*

no

Removes the origin realm configuration.

realm_name

Specifies the realm to bind the Diameter endpoint. The *realm_name* must be an alphanumeric string of 1 through 127 characters. The realm is the Diameter identity. The originator's realm must be present in all Diameter messages. The origin realm can typically be a company or service name.

Usage Guidelines

Use this command to set the realm for the Diameter endpoint.

Diameter agent on the chassis listens to standard TCP port 3868 and also supports the acceptance of any incoming TCP connection from external server.

Example

The following command sets the origin realm to *companyx*:

```
origin realm companyx
```

osid-change

This command stores the Origin-State-Id AVP of a diameter peer node on the P-GW. This enables the P-GW to detect and clear sessions whenever there is a change in the Origin-State-Id of the diameter peer node. This command is introduced at the diameter endpoint level.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] osid-change action [clear-subscribers]

no

Disables the command.

action

Specifies the action to be taken.

clear subscribers

Clears subscribers connected to the peer.

Usage Guidelines

Use this command to store the Origin-State-Id AVP of a diameter peer node on the P-GW. This enables the P-GW to detect and clear sessions whenever there is a change in the Origin-State-Id of the diameter peer node. This command is introduced at the diameter endpoint level.

This command is disabled by default.

Example

The following command clears subscribers whose origin state IDs have changed.

:

```
diameter endpoint PGW-Gx use-proxy
    origin host PGW-Gx address 30.30.30.1 osid-change action
clear-subscribers no watchdog-timeout response-timeout 7
    connection timeout 5
    connection retry-timeout 2
    peer PGW-Gx-server realm PGW-Gx.com address 30.30.30.2 port 5333
#exit
```

peer

This command specifies a peer address for the Diameter endpoint.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

peer [*] *peer_name* **[*] [realm** *realm_name* **] [destination-host-name** *host_name* **] { address** *ipv4/ipv6_address* **[[load-ratio** *load_ratio_range* **] [port** *port_number* **] [connect-on-application-access] [send-dpr-before-disconnect disconnect-cause** *disconnect_cause* **] [sctp]] + | fqdn** *fqdn* **[[port** *port_number* **] [send-dpr-before-disconnect disconnect-cause** *disconnect_cause* **] [rlf-template** *rlf_template_name* **enable-snmp-traps]] }**
no peer *peer_name* **[realm** *realm_name* **]**

no

Removes the specified peer configuration.

[*] *peer_name* [*]

Specifies the peer's name as an alphanumeric string of 1 through 63 characters that allows punctuation characters.

The Diameter server endpoint can now be a wildcarded peer name (with * as a valid wildcard character). Client peers which satisfy the wild-carded pattern are treated as valid peers and the connection will be accepted. The wildcarded token indicates that the peer name is wildcarded and any '*' in the preceding string is treated as a wildcard.

realm *realm_name*

Specifies the realm of this peer as an alphanumeric string of 1 through 127 characters. The realm name can be a company or service name.

destination-host-name *host_name*

Specifies the destination host name as an alphanumeric string of 1 through 63 characters. Note that this is an optional keyword.

If a peer is selected by Diameter base protocol to forward an application request, then the host name specified through the "**destination-host-name**" option will be used to encode the Destination-Host AVP.

This keyword "**destination-host-name**" is made optional for backward compatibility. That means, if the destination-host-name is not specified in the CLI, the peer name itself is copied to the destination-host-name for backward compatibility.

In releases prior to 17.0, the endpoint configuration allows each SCTP association to be uniquely identified by a Diameter peer name. But there was a requirement where two SCTP associations are identified with the same peer name. This kind of reused peer-name was used by HSS peers which act as Active and Standby HSS nodes. The SCTP associations in HSS behave in a manner such that one association is always SCTP active (for the active HSS) while the other SCTP association with the standby HSS would be closed and would keep flapping. To avoid this scenario and address customer's requirement, in 17.0 and later releases, this optional keyword "**destination-host-name**" has been introduced in the **peer** CLI command to allow multiple unique peers (Diameter HSS servers) to be configured with the same host name.

With this enhancement, MME will be capable of provisioning multiple Diameter SCTP associations to reach the same HSS peer name. This configuration will also ensure that all the Diameter messages are exchanged properly with the configured destination host.

Internally the peers are identified with unique peer-name. But the Origin-host AVP provided by the server (in CER/CEA/App-msgs) is validated against both peer-name and destination-host-name provided in the CLI. Even if multiple peers are responding with same Origin-Host, this can be validated and accepted based on the CLI configuration.

address *ipv4/ipv6_address*

Specifies the Diameter peer IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. This address must be the IP address of the device with which the chassis is communicating.

load-ratio *load_ratio_range*

Specifies the Load Ratio for the peer. The Load Ratio can be configured in the range of 0 through 65535.

As a default behavior, the CLI command is not enabled for a peer and the default Load Ratio is 1, which will be used in load balancing only when at least one peer has non-default Load Ratio configured.

Not specifying the **load-ratio** *load_ratio_range* keyword from peer configuration will put the peer in default Load Ratio, and when all the peers have default Load Ratio, Diameter load balancing will be round robin.

The CLI takes effect when Diameter applications starts using an endpoint for sending messages.

fqdn *fqdn*

Specifies the Diameter peer FQDN as an alphanumeric string of 1 through 127 characters.

port *port_number*

Specifies the port number for this Diameter peer. The port number must be an integer from 1 through 65535.

connect-on-application-access

Activates peer on first application access.

send-dpr-before-disconnect

Sends Disconnect-Peer-Request (DPR).

disconnect-cause

Sends Disconnect-Peer-Request to the specified peer with the specified disconnect reason. The disconnect cause must be an integer from 0 through 2, for one of the following:

- REBOOTING(0)
- BUSY(1)
- DO_NOT_WANT_TO_TALK_TO_YOU(2)

rlf-template *rlf_template_name*

Specifies the RLF template to be associated with this Diameter peer.

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



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.



Important Peer level RLF template takes precedence over the endpoint level template.

enable-snmp-traps

Enables the Diameter RLF related SNMP Traps. Skipping this keyword will disable sending of RLF related traps.

By default, the Diameter RLF related traps (“over-threshold”, “over-limit” and “normal-state”) notifications will not be enabled.

This keyword is meaningful only with a valid RLF template. As such, the command has the following meaning:

- **rlf-template** *rlf_template_name*: Use the RLF template. Disable traps if previously configured.
- **rlf-template** *rlf_template_name* **enable-snmp-traps** : Use the RLF template and enable traps.
- Skip the whole RLF template block from the peer configuration line to detach the RLF from the peer along with the traps.

sctp

Uses Stream Control Transmission Protocol (SCTP) for this peer.

+

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

Usage Guidelines

Use this command to add a peer to the Diameter endpoint.

If the Diameter server side endpoint is catering to multiple peers, there has to be an entry for each peer in the peer list for that endpoint.

In cases where the client like GGSN does not use a diameter proxy, the peer list can be as large as the number of session managers on a GGSN. This might lead to a very complex configuration at the Diameter server endpoint.

To simplify the configurations, the Diameter server endpoint accepts a wildcarded peer name (with * as a valid wildcard character).

The client peers which satisfy the wild-carded pattern are treated as valid peers and the connection will be accepted. The new token 'wildcarded*' indicates that the peer name is wildcarded and any '*' in the preceding string should be treated as a wildcard.

For example, if the peer name is prefixed and suffixed with *ggsn* (* wildcard character) and an exact match is not found for the peer name portions peers like *0001-sessmgr.ggsn-gx*, *0002-sessmgr.ggsn-gx*, will be treated as valid peers at the Diameter server endpoint.

Example

The following command adds the peer named *test* with IP address *209.165.200.225* using port *126*:

```
peer test address 209.165.200.225 port 126
```

peer-backoff-timer

This command configures the time interval after which the Diameter peer will resume sending CCR-I messages to the PCRF server.

Product

GGSN

HA

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

peer-backoff-timer *timeout* **[send-app-level-term-req]**
{ default | no } peer-backoff-timer

default | no

Removes the configured peer backoff timer from Diameter endpoint configuration.

Default value of peer-backoff-timer is 7 seconds.

timeout

Specifies the peer backoff timeout duration in seconds, and must be an integer from 1 through 3600.

send-app-level-term-req

Sends termination request from application irrespective of whether or not the peer-backoff-timer is running.

Usage Guidelines

Use this command to configure a peer backoff timer which will be started when the server (primary or secondary PCRF) is busy. That is, the backoff-timer is started when the result code DIAMETER_TOO_BUSY (3004) is received from the PCRF. This PCRF is then marked as unavailable for the period configured by the backoff timer.

No CCR-I messages will be sent to the server until this timer expires. This timer will be per session manager level and will be applicable only to that instance.

Example

The following command sets the peer backoff timeout to *20* seconds:

```
peer-backoff-timer 20
```

reconnect-timeout

This command configures the time interval after which the Diameter peer will be reconnected automatically when DO_NOT_WANT_TO_TALK_TO_YOU disconnect cause is received.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

reconnect-timeout *timeout*
no reconnect-timeout

no

Disables auto reconnect of peer after receiving the disconnect cause "DO_NOT_WANT_TO_TALK_TO_YOU".

The default configuration is **no reconnect-timeout**. The connection to peer will not be retried until it is enabled by the administrator using the **diameter enable endpoint** command in the Exec mode.

timeout

Specifies the reconnect timeout duration in seconds, and the value must be an integer from 30 through 86400.

Usage Guidelines

Use this command to configure a timer which is started at the reception of the "DO_NOT_WANT_TO_TALK_TO_YOU" disconnect cause from the Diameter peer in Disconnect-Peer-Request message. After the timer expiry, the Diameter endpoint will automatically try to reconnect to the disconnected peer.

Currently in the system, the "DO_NOT_WANT_TO_TALK_TO_YOU " in the disconnect peer request is treated as an admin disable. Hence when the system gets into this state the connection will not be retried and the connection must be enabled by the administrator using the **diameter enable endpoint** command in the Exec mode.

Example

The following command sets the reconnect timeout to *100* seconds:

```
reconnect-timeout 100
```

response-timeout

This command configures the Response Timeout parameter. Response timeout specifies the maximum allowed response time for request messages sent from Diameter applications to Diameter server. On failure of reception of response for those request message within this specified time, this will be handled as failure by the corresponding applications and appropriate failure action will be initiated.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

response-timeout *timeout*
default response-timeout

default

Configures this command with the default setting.

Default: 60 seconds

timeout

Specifies the response timeout duration in seconds, and the value must be an integer from 1 through 300.

Usage Guidelines

Use this command to configure the Response Timeout parameter.

Example

The following command sets the response timeout to *100* seconds:

response-timeout 100

rlf-template

This command configures the RLF template to be used for the Diameter endpoint for throttling and rate control.

Important RLF template cannot be deleted if it is bound to any application (peers/endpoints).

Product

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > **context** *context_name* > **diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-diameter)#

Syntax Description

[no] rlf-template *rlf_template_name* **[enable-snmp-traps]**

no

Remove the specified RLF template from global configuration.

Important Do not use "**no rlf-template** *rlf_template_name*" in endpoint configuration mode. This CLI attempts to delete the specified RLF template. This CLI is part of global configuration, and not endpoint configuration.

rlf_template_name

The name of the RLF template to be used for Diameter endpoint configuration. *rlf_template_name* must be an alphanumeric string of 1 through 127 characters.

enable-snmp-traps

Enables the Diameter RLF related SNMP Traps. Skipping this keyword will disable sending of RLF related traps.

By default, the Diameter RLF related traps (“over-threshold”, “over-limit” and “normal-state”) notifications will not be enabled.

This keyword is meaningful only with a valid RLF template. As such, the command has the following meaning:

- **rlf-template** *rlf_template_name*: Use the RLF template. Disable traps if previously configured.
- **rlf-template** *rlf_template_name* **enable-snmp-traps** : Use the RLF template and enable traps.
- **no rlf-template** *rlf_template_name*: Detach the RLF from the endpoint along with traps.

Usage Guidelines

Use this command to configure the RLF Template to be used for the Diameter endpoint for throttling and rate control. This CLI command should be defined in the Diameter endpoint application to enable RLF module.

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.

Important This CLI command takes effect only if the RLF template is defined in the Global Configuration mode and the connection to the peer is open.

Currently in the deployment of the Diameter applications (Gx, Gy, etc.), many operators make use of "**max-outstanding** <*number*>" as a means of achieving some rate-limiting on the outgoing control traffic. With RLF in place, this is no longer required since RLF takes care of rate-limiting in all cases. If RLF is used and **max-outstanding** is also used, there might be undesirable results.

Important If RLF is being used with an "**diameter endpoint**", then set the **max-outstanding** value of the peer to be 255.

RLF provides only the framework to perform the rate limiting at the configured Transactions Per Second (TPS). The applications (like Diameter) should perform the configuration specific to each application.

For more information on this feature, refer to the *rlf-template* command in the *Global Configuration Mode Commands* chapter in this guide. For more information on RLF template configuration commands, refer to the *RLF Template Configuration Mode Commands* chapter in this guide.

Example

The following command configures an RLF template named *rlf_1* for Diameter endpoint:

```
rlf-template rlf_1
```

route-entry

This command creates an entry in the route table for Diameter peer.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
route-entry { [ host [ * ] host_name ] [ peer peer_id [ weight priority ] ] [
 realm [ * ] realm_name [ application credit-control peer peer_id ] [ weight
 value ] | peer peer_id [ weight value ] ] }
no route-entry { [ host [ * ] host_name ] [ peer peer_id ] [ realm [ * ]
realm_name { application credit-control peer peer_id | peer peer_id } ] }
```

no

Disables the specified route-entry table configuration.

host [*] *host_name*

Specifies the Diameter server's host name as an alphanumeric string of 1 through 63 characters. In 18.0 and later releases, the host name can additionally accept wildcard character (*). The support for wildcard entry is provided to allow routing of Diameter messages destined to any host @ any realm through the next-hop peer.

realm [*] *realm_name*

Specifies the realm name as an alphanumeric string of 1 through 127 characters. The realm may typically be a company or service name. In 18.0 and later releases, the realm name can additionally accept wildcard character (*). The support for wildcard entry is provided to allow routing of Diameter messages destined to any host @ any realm through the next-hop peer.

application credit-control

Specifies the credit control application — DCCA or RADIUS.

peer *peer_id*

Specifies the peer ID of the Diameter endpoint route as an alphanumeric string of 1 through 63 characters.

weight *priority*

Specifies the priority for a peer in the route table as an integer from 0 through 255. Default: 10

The peer with the highest weight is used. If multiple peers have the highest weight, selection is by round-robin mechanism.

Usage Guidelines

Use this command to create a route table for Diameter application.

When a Diameter client starts to establish a session with a realm/application, the system searches the route table for the best match. If an entry has no host specified, the entry is considered to match the requested value. Similarly, if an entry has no realm or application specified, the entry is considered to match any such requested value. The best match algorithm is to prefer specific matches for whatever was requested, either realm/application or host/realm/application. If there are no such matches, then system looks for route table entries that have wildcards.

Wildcard (*) based Diameter realm routing is supported in 18.0 and later releases. With this feature turned ON, the customers can avoid configuring individual Diameter peers and/or realms for all possible Diameter servers in their network.

The wild card Diameter routes can be statically configured under a Diameter endpoint configuration using the CLI "**route-entry realm * peer** *peer_name*".

These route entries are treated as default route entries to be used to send a message when there is no matching host@realm based or realm based route entry available.

The wild card Diameter route is added along with other realm based route entries in diabase. The wild card route entry will be selected to route a message only if the message's destination realm does not match with any of the other static realm based routes.

For example,

route-entry realm abc.com peer *peer1*

route-entry realm def.com peer *peer2*

route-entry realm * peer peer-default

If the message's destination realm is *abc.com* then the message will be routed to *peer1*. If the message's destination realm is *def.com* then the message will be routed to *peer2*. If the destination realm is *xyz.com* then the message will be routed to "*peer-default*".

When multiple wild card route entries are configured with same weights, then the routes are selected in a round robin fashion. When multiple wild card route entries are configured with different weights, then the route with the highest weight will be selected.

In case when there are multiple wild card routes with higher and equal weights and some routes with lower weights, then only the higher weight routes will be selected in round robin-fashion. The lower weight route can be selected only when the higher weight routes are not valid because of the peers being not in good state.

Example

The following command creates a route entry with the host name *dcca_host1* and peer ID *dcca_peer* with priority weight of *10*:

```
route-entry host dcca_host1 peer dcca_peer weight 10
```

route-failure

This command controls what action is performed for the route table after failure or recovery after failure.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

route-failure { deadtime *seconds* **| recovery-threshold percent** *percentage* **| result-code** *result_code* **| threshold** *counter* **}**
default route-failure { deadtime | recovery-threshold | threshold }
no route-failure result-code *result_code*

no

Disables the route-failure configuration.

default

Configures the default setting for the specified parameter.

deadtime *seconds*

Specifies the time duration (in seconds) for which the system keeps the route in FAILED status. When this time expires, the system changes the status to AVAILABLE.

seconds must be an integer from 1 through 86400. Default: 60

recovery-threshold percent *percentage*

Specifies the percentage value at which the failure counter is reset when provisionally changing the status from FAILED to AVAILABLE.

For example, if a failure counter of 16 caused the status to change to FAILED. After the configured deadtime expires, the status changes to AVAILABLE. If this keyword is configured with 75 percent, the failure counter will be reset to 12 (75 percent of 16).

percentage must be an integer from 1 through 99. Default: 90

result-code *result_code*

Configures which answer messages are to be treated as failures, in addition to requests that time out. Up to 16 different result codes can be specified.

result_code must be an integer from 0 through 4294967295.

threshold *counter*

Configures the number of errors that causes the status to become FAILED. The counter value must be an integer from 0 through 4294967295. Default: 16

The error counter begins at zero, and whenever there is a good response it decrements (but not below zero) or increments (but not above this threshold).

Usage Guidelines

Use this command to control how failure/recovery is performed for the route table. After a session is established, it is possible for the session to encounter errors or Diameter redirection messages that cause the Diameter protocol to re-use the route table to switch to a different route.

Each Diameter client within the chassis maintains counters relating to the status of each of its connections to different hosts (when the destination is realm/application without a specific host, the host name is kept as "", i.e., blank).

Moreover, those counters are further divided according to which peer is used to reach each host. Each Diameter client maintains a status of each peer-to-host combination. Under normal good conditions the status will be AVAILABLE, while error conditions might cause the status to be FAILED.

Only combinations that are AVAILABLE will be used. If none are AVAILABLE, then system attempts the secondary peer if failover is configured and system can find an AVAILABLE combination there. If nothing is AVAILABLE, the system uses a FAILED combination.

Example

The following command configures the time duration for route failure to *90* seconds:

```
route-failure deadtime 90
```

server-mode

This command configures the Diameter endpoint to establish the system as the server side endpoint of the connection.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
server-mode [ demux-mode ]
```

demux-mode

Specifies that the Diameter proxy is to use the demux manager to identify the appropriate session manager. If this keyword is not enabled, the proxy will route the request directly to a session manager.

Usage Guidelines

Use this command to configure the Diameter endpoint to establish this system as the server side endpoint of the connection. When the Diameter proxy receives an incoming request, the proxy identifies the endpoint for the request. If the system is in client mode, the proxy extracts the instance ID of the session manager which serves as the session-ID of the request. If this command is enabled, the extraction of the instance ID is disabled.

Example

The following command sets the system as the server side of the Diameter endpoint and instructs the Diameter proxy to use the demux manager to identify the appropriate session manager where the request is to be routed:

```
server-mode demux-mode
```

session-id include imsi

This command associates/disassociates a Stream Control Transmission Protocol (SCTP) parameter template with the Diameter endpoint.

This command has been added under the diameter endpoint configuration mode to include IMSI in Diameter session-ID per Diameter endpoint at Gx, Gy, and Gz (Rf). Configuration changes will be applicable only to new Sessions at Gx, Gy and Rf. Configuration changes will not have any impact on existing sessions behavior at Gx, Gy, and Rf. For Gy, multiple Diameter sessions can be initiated per subscriber and the session ID format setting will bind to the subscriber. The setting will be taken to effect when the first Diameter session is established and following Gy sub sessions will keep using the session ID format used in first session.

Product

All

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
session-id include imsi
[no] session-id include imsi
```

no

Disables this feature, that is, IMSI is not included in the Diameter Session-ID, which is the default behavior.

include

Includes configured information in Diameter Session-ID.

imsi

Includes International Mobile Subscriber Identification (IMSI) in Diameter Session-ID.

session-id

Describes Diameter Session-ID format.

Usage Guidelines

Use this command to include IMSI in Diameter session-ID per Diameter endpoint at Gx, Gy, and Gz (Rf).

Example

The following command includes IMSI in Diameter session-ID per Diameter endpoint at Gx, Gy, and Gz (Rf):

```
session-id include imsi
```

use-proxy

This command enables/disables Diameter proxy for the Diameter endpoint. By default this command is disabled.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
use-proxy [ server-mode [ demux-mode ] ]
no use-proxy
```

no

Disables Diameter proxy for the current endpoint.

This command at endpoint level will equip an application to use Diameter proxy to route all its messages to an external peer.

server-mode

Specifies that the Diameter endpoint to establish the Diameter proxy as the server side endpoint of the connection.

demux-mode

Specifies that the Diameter endpoint to establish the Diameter proxy to use the Demux manager to identify the appropriate session manager. If this keyword is not enabled, the proxy will route the request directly to a session manager.

IPCF uses BindMux to identify the appropriate session manager.

Usage Guidelines

Use this command to establish a Diameter proxy to route all its messages to an external peer. The proxy acts as an application gateway for Diameter. It gets the configuration information at process startup and decides which Diameter peer has to be contacted for each application. It establishes the peer connection upon finding no peer connection already exists.

IPCF uses Bindmux as a Demux manager to help distribute new incoming sessions across available Sessmgrs on the system.

All the incoming Diameter requests/responses land on Diamproxy. Diamproxy checks if a Sessmgr is already serving this session based on parameters like session-id and peer-id of the request/response.

If no Sessmgr is allocated to the request and the Demux mode is ON, the DiamProxy forwards the new request to Demux/Bindmux for sessmgr allocation. Demux/Bindmux has updated information about the load on all the Sessmgrs and assigns the optimal Sessmgr to the Diameter session. Once a Sessmgr is allocated for the session, a mapping of session-id to Sessmgr is added at Diamproxy. All further requests for this session will be directly routed to Sessmgr.

Each proxy task will automatically select one of the host names configured with the **origin host** command. Multiple proxy tasks will not use the same host names, so there should be at least as many host names as proxy tasks. Otherwise, some proxy tasks will not be able to perform Diameter functionality. The chassis automatically selects which proxy tasks are used by which managers (i.e., ACSMgrs, Sessmgrs), without verifying whether the proxy task is able to perform Diameter functionality.

To be able to run this command, the Diameter proxy must be enabled. In the *Global Configuration Mode Commands* chapter, see the description of the **require diameter-proxy** command.

In 17.0 and later releases, when a PCEF is connected to OCS via multiple Diameter proxies, PCEF will choose the same Diameter proxy for the subsequent messages as long as it is available. Any subsequent messages (CCR-U/CCR-T) to the same host are sent via the same peer. Once the next-hop is chosen via round-robin method, the subsequent message for the session is sent to the same next-hop (peer).

In releases prior to 18.0, when the chassis is in standby state, all the Diameter proxies are stopped. In18.0 and later releases, all the Diameter proxies will be running even when the chassis is in standby mode. Any change in ICSR grouping mask will lead to stopping and restarting of all the diamproxies on the standby chassis.

Example

The following command enables Diameter proxy for the current endpoint:

```
use-proxy
```

The following command disables Diameter proxy for the current endpoint:

```
no use-proxy
```

vsa-support

This command allows DIABASE to use vendor IDs configured in the dictionary for negotiation of the Diameter peers' capabilities regardless of the supported vendor IDs received in Capabilities-Exchange-Answer (CEA) messages.

Product

GGSN

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
vsa-support { all-from-dictionary | negotiated-vendor-ids }
default vsa-support
```

default

Configures this command with the default setting.

Default: **negotiated-vendor-ids**

all-from-dictionary

Allows DIABASE to use the vendor IDs from the dictionary as indicated in the Capabilities-Exchange-Request (CER) messages from Diameter peers.

negotiated-vendor-ids

Allows DIABASE to use the supported vendor IDs satisfying capability negotiation.

Usage Guidelines

Use this command to set DIABASE to use the vendor IDs from the dictionary or use the vendor IDs satisfying the capabilities negotiation.

Example

The following command enables DIABASE to use the vendor IDs specified in the dictionary:

```
vsa-support all-from-dictionary
```

watchdog-timeout

This command configures the Watchdog Timeout parameter.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context *context_name* **> diameter endpoint** *endpoint_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
watchdog-timeout timeout
{ default | no } watchdog-timeout
```

no

Disables the watchdog timeout configuration.

default

Configures this command with the default setting.

Default: 30 seconds

timeout

Specifies the timeout duration (in seconds) as an integer from 6 through 30.

Usage Guidelines

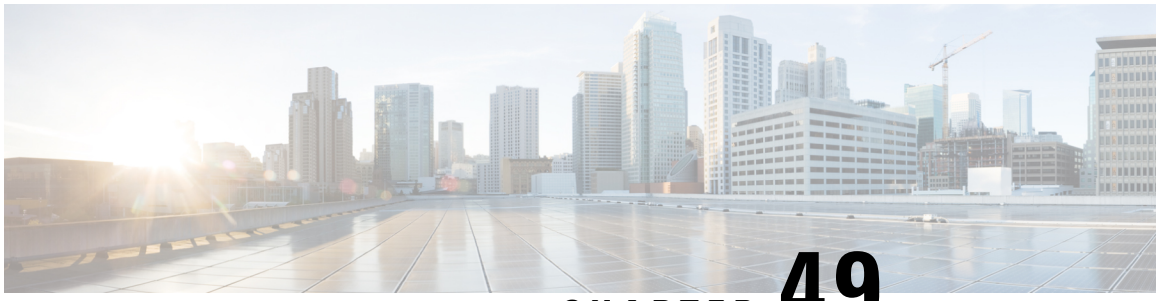
Use this command to configure the Watchdog Timeout parameter for the Diameter endpoint. If this timer expires before getting a response from the destination, other route to the same destination is tried, as long as the retry count setting has not exceeded (see the CLI command) and as long as the response timer has not expired (see the CLI command).

If the watchdog timer expires, the gateway sends the heartbeat message to Diameter endpoint. The timer is allowed to have the value up to a maximum of +2 or -2 seconds from the configured value.

Example

The following command sets the watchdog timeout setting to *15* seconds:

```
watchdog-timeout 15
```



CHAPTER 49

Diameter HDD Module Configuration Mode Commands

The HDD Module Configuration Mode allows you to configure Hard Disk Drive (HDD) module to store the failed CCR-T messages during OCS failure.

Important The commands in this configuration mode are license dependent. For more information, contact your Cisco account representative.

Command Modes Exec > Global Configuration > Context Configuration > Diameter HDD Module Configuration

configure > context *context_name* **> diameter-hdd-module**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-diameter-hdd)#`

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

- diameter-event, on page 1081
- end, on page 1086
- exit, on page 1086
- file, on page 1086

diameter-event

This command allows you to configure the HDD specific parameters.

Important This command is license dependent. For more information, contact your Cisco account representative.

Product HA

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter HDD Module Configuration

configure > context *context_name* **> diameter-hdd-module**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-diameter-hdd)#
```

Syntax Description

diameter-event { 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* **}] [via local-context] +] | use-harddisk }**
default diameter-event [purge | push-interval | push-trigger space-usage-percent | remove-file-after-transfer | transfer-mode [module-only | push via] | use-harddisk] +
no diameter-event [purge | remove-file-after-transfer | use-harddisk] +

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 Card (LC) is used for push
- **use-harddisk**: Disabled



Important The **use-harddisk** keyword is available only on the ASR 5000 and ASR 5500 chassis.

no

If previously configured, disables the specified configuration:

- **purge**: Disables purging of Diameter records.
- **remove-file-after-transfer**: Retains a copy of the Diameter file even after it has been pushed or pulled to another server.
- **use-harddisk**: Disables data storage on the ASR 5000 SMC hard disk or ASR 5500 hard disk array.



Important The **use-harddisk** keyword is available only on the ASR 5000 and ASR 5500 chassis.

purge { storage-limit *storage_limit* | time-limit *time_limit* } [max-files *max_records_to_purge*]

Specifies to purge/delete the Diameter 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 *push_interval*

Specifies the transfer interval (in seconds) to push Diameter files to an external file server.

push_interval must be an integer from 60 through 3600.

Default: 300

push-trigger space-usage-percent *trigger_percentage*

Specifies the record 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 record 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 Diameter 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* }] [via local-context] +]

Specifies the file transfer mode—how the Diameter files are transferred to an external file server.

- **pull**: Specifies that the external server is to pull the Diameter files.
- **push**: Specifies that the system is to push Diameter files to the configured external server.
- **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 HDD module. This enables to support individual record transfer-mode configuration for each module.
- **primary encrypted-url** *encrypted_url*: Specifies the primary URL location in encrypted format to which the system pushes the Diameter files.

  encrypted_url must be the location in an encrypted format, and must be an alphanumeric string of 1 through 1024 characters.
- **primary url** *url*: Specifies the primary URL location to which the system pushes the Diameter files.

  url must be the location, and must be an alphanumeric string of 1 through 1024 characters in the "*//user:password@host:[port]/directory*" format.
- **secondary encrypted-secondary-url** *encrypted_secondary_url*: Specifies the secondary URL location in encrypted format to which the system pushes the Diameter files when the primary location is unreachable or fails.

  encrypted_secondary_url must be the secondary location in an encrypted format, and must be an alphanumeric string of 1 through 1024 characters in the "*//user:password@host:[port]/directory*" format.
- **secondary secondary-url** *secondary_url*: Specifies the secondary location to which the system pushes the Diameter 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 "*//user:password@host:[port]/directory*" format.
- **via local-context**: Configuration to select LC/SPIO for transfer of Diameter records. The system pushes the Diameter files via SPIO in the local context.

use-harddisk



Important The **use-harddisk** keyword is available only on the ASR 5000 and ASR 5500 chassis.

ASR 5000: Specifies that on the ASR 5000 chassis the hard disk on the SMC be used to store Diameter files. On configuring to use the hard disk for Diameter record storage, Diameter files are transferred from packet processing cards to the hard disk on the SMC. Default: Disabled

ASR 5500: Specifies that on the ASR 5500 chassis the hard disk the FSC hard disk array be used to store Diameter files. On configuring to use the hard disk for Diameter record storage, Diameter files are transferred from DPCs to the hard disk array. Default: Disabled

+

Indicates that multiple keywords can be specified in a single command entry. When the "+" appears in the syntax, any of the keywords that appear prior to the "+" can be entered in any order.

Usage Guidelines

Use this command to configure how the Diameter records are moved and stored.

On the ASR 5000 or ASR 5500 chassis, you must run this command only from the local context. If you run this command in any other context it will fail and result in an error message.

If PUSH transfer mode is configured, the external server URL to which the Diameter 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 the external server 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 the "diameter" directory created within it.

When changing the transfer mode from push to pull, after changing, enable PULL on the external server. 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 **use-harddisk** command is available only on the ASR 5000 and ASR 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 **use-harddisk** command is configured to store EDR/UDR/EVENT/DIAMETER files. 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 all the 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 **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.

Limitations:

- When an ICSR event occurs unexpectedly before the CCR-T message is written, the CCR-T will not written to the HDD and hence the usage will be lost.

- It is expected that the customers requiring this feature should monitor the HDD and periodically pull and delete the files so that the subsequent records can be buffered.

Example

The following command retains a copy of the Diameter file after it has been transferred to the storage location:

```
no diameter-event remove-file-after-transfer
```

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 the file creation properties for Diameter records.



Important This command is license dependent. For more information, contact your Cisco account representative.

Product HA

P-GW

Privilege Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Diameter HDD Module Configuration

configure > context *context_name* **> diameter-hdd-module**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-diameter-hdd)#
```

Syntax Description

file [compression { gzip | none }] [current-prefix *string* **] [delete-timeout** *seconds* **] [directory** *directory_name* **] [exclude-checksum-record] [field-separator { hyphen | omit | underscore }] [name** *file_name* **] [reset-indicator] [rotation [num-records** *number* **| tariff-time minute** *minute_value* **hour** *hour_value* **| 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] [name] [reset-indicator] [rotation { num-records | tariff-time | time | volume }] [sequence-number] [storage-limit] [time-stamp] [trailing-text] [trap-on-file-delete] +

default

Configures the default setting for the specified keyword(s).

compression { gzip | none }

Specifies compression of Diameter files.

- **gzip**: Enables GNU zip compression of the Diameter 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 Diameter file that is currently being used to store Diameter 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 Diameter 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 Diameter files.

directory_name must be an alphanumeric string of 1 through 191 characters.

Default: **/records/diameter**

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 Diameter file.

Default: Disabled (inserts checksum record into the Diameter file)

field-separator [hyphen | omit | underscore]

Specifies the field inclusion/exclusion type of separators between two fields of Diameter 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. This is the default field separator.

name *file_name*

Specifies a string to be used as the base file name for Diameter files.

Default: **diameter**

file_name must be an alphanumeric string of 1 through 31 characters.

reset-indicator

Specifies inclusion of the reset indicator counter value, from 0 through 255, in the Diameter file name, and is incremented (by one) whenever any of the following conditions occur:

- An ACSMgr/SessMgr process fails.
- A peer chassis has taken over in compliance with the Interchassis Session Recovery feature.
- The sequence number has rolled over to zero.

rotation { num-records *number* | tariff-time minute *minute_value* hour *hour_value* | time *seconds* | volume *bytes* }

Specifies when to close a Diameter file and create a new one.

- **num-records** *number*: Specifies the number of records that should be added to the file. When the number of records in the file reaches the specified value, the file is complete.

  number must be an integer from 100 through 10240.

  Default: 1024

- **time** *seconds*: Specifies the period of time (in seconds) to wait before closing the Diameter file and creating a new one.

seconds must be an integer from 30 through 86400.

Default: 3600

- **tariff-time minute** *minute_value* **hour** *hour_value*: Specifies the time of day (hour and minute) at which the files are rotated once per day.

  minute_value is an integer value from "0" up to "59".

  hour_value is an integer value from "0" up to "23".



Important The options **time** and **tariff-time** are mutually exclusive and only any one of them can be configured. Other file rotation options can be used with either of them.

- **volume** *bytes*: Specifies the maximum size (in bytes) of the Diameter file before closing it and creating a new one.

  bytes must be an integer from 51200 through 62914560.

  Default: 102400

  Note that a higher setting may improve the compression ratio when the compression keyword is set to gzip.

sequence-number { length *length* | omit | padded | padded-six-length | unpadded }

Specifies including/excluding 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.

- **omit**: Excludes the sequence number from the file name.
- **padded**: Includes the padded sequence number with preceding zeros in the file name. This is the default setting.
- **padded-six-length**: Includes the padded sequence number with six preceding zeros in the file name.
- **unpadded**: Includes the unpadded sequence number in the file name.

storage-limit *limit*

Specifies deleting files when the specified amount of space (in bytes) is used up for Diameter file storage RAM on packet processing cards.

limit must be an integer from 10485760 through 536870912. Default: 33554432



Important The total storage limit is 536870912 bytes (512 MB). This limit is for all the record (EDR/UDR/EVENT/Diameter) files.

time-stamp { expanded-format | rotated-format | unix-format }

Specifies the timestamp of when the file was created to be included in the file name.

- **expanded-format**: Specifies the UTC MMDDYYYYHHMMSS format. This is the default setting.
- **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.

string must be an alphanumeric string of 1 through 30 characters.

Deafult: Disabled

trap-on-file-delete

Instructs the system to send an SNMP notification (starCDRFileRemoved) when the Diameter file is deleted due to lack of space.

Default: Disabled

xor-final-record

Specifies inserting an XOR checksum (in place of the CRC checksum) into the Diameter file header if the **exclude-checksum-record** is left at its default setting.

Default: Disabled

+

Indicates that multiple keywords can be specified in a single command entry. When the "+" appears in the syntax, any of the keywords that appear prior to the "+" can be entered in any order.

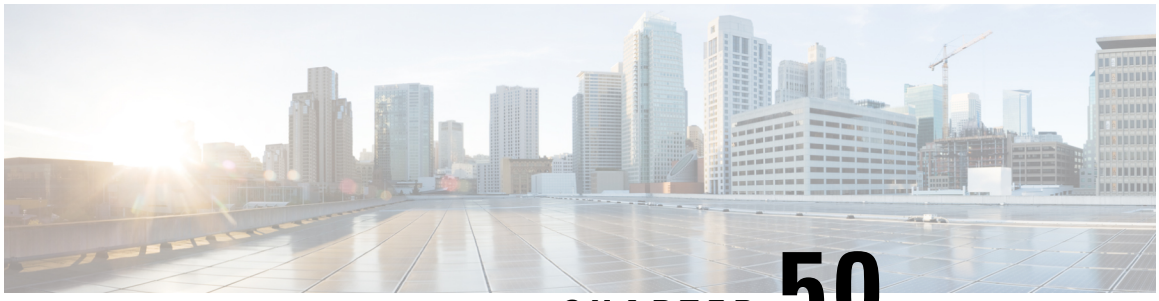
Usage Guidelines

Use this command to configure file characteristics for Diameter records.

Example

The following command sets the prefix of the current active Diameter file to *Current*:

```
file current-prefix Current
```



CHAPTER 50

Diameter Failure Handling Template Configuration Mode Commands

Command Modes

Diameter Failure Handling Template Configuration Mode is accessed from the Global Configuration Mode. This mode allows an operator to configure failure handling template that can be associated to different Diameter services.

Exec > Global Configuration > Failure Handling Template Configuration

configure > failure-handling-template *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fh-template)#
```

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

- end, on page 1091
- exit, on page 1092
- msg-type, on page 1092

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-type

This command specifies the failure handling behavior in the event of a communication failure with the prepaid server.

Product

GGSN

HA

HSGW

IPSG

PDSN

P-GW

S-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Failure Handling Template Configuration

configure > failure-handling-template *template_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-fh-template)#`

Syntax Description

msg-type { any | authentication info request | authorization-request | check-identity-request | credit-control-initial | credit-control-terminate | credit-control-update | eap-request | eap-termination-request | notify-request | profile-update-request | purge-ue-request | update-location-request | user-data-request } failure-type { any | diabase-error | diameter result-code { any-error | *result-code* **[** *to end-result-code* **] } | diameter exp-result-code { any-error |** *result-code* **[** *to end-result-code* **] } | resp-timeout | tx-expiry } action { continue [discard-traffic | local-fallback [without-retry] | retry-server-on-event | send-ccrt-on-call-termination | without-retry] | retry-and-terminate**

```
 [ max-transmissions | without-term-req ] | terminate [ without-term-req
 ] }
no msg-type { any | authentication info request | authorization-request
| check-identity-request | credit-control-initial |
credit-control-terminate | credit-control-update | eap-request |
eap-termination-request | notify-request | profile-update-request |
purge-ue-request | update-location-request | user-data-request }
failure-type { any | diabase-error | diameter result-code { any-error |
result-code [ to end-result-code ] } | diameter exp-result-code { any-error |
result-code [ to end-result-code ] } | resp-timeout | tx-expiry }
```

no

Removes the configuration associated with the failure handling template.

{ any | authentication info request | authorization-request | check-identity-request | credit-control-initial | credit-control-terminate | credit-control-update | eap-request | eap-termination-request | notify-request | profile-update-request | purge-ue-request | update-location-request | user-data-request }

Defines the failure handling behavior based on the failures in the following request messages:

- Any request
- Authentication-Information Request through S6a or S13 Diameter interface
- Authorization Request through PDIF-EAP, STa, S6b, or Wm interface
- Check-Identity-Information-Request through S6a or S13 interface
- Credit-Control-Initial-Request (CCR-I) through Gx, Gy or Ty interface
- Credit-Control-Terminate-Request (CCR-T) through Gx, Gy or Ty interface
- Credit-Control-Update-Request (CCR-U) through Gx, Gy or Ty interface
- EAP request through Cx, PDIF-EAP, STa, S6b, or Wm interface
- EAP Termination request through Cx, PDIF-EAP, STa, S6b, or Wm interface
- Notify-Request through S6a or S13 interface
- Profile-Update-Request through Sh interface
- Purge-UE-Request through S6a or S13 interface
- Update-Location-Request through S6a or S13 interface
- User-Data-Request through Sh interface

failure-type { any | diabase-error | diameter result-code { any-error | *result-code* [*to end-result-code*] } | diameter exp-result-code { any-error | *result-code* [*to end-result-code*] } | resp-timeout | tx-expiry }

Defines the failure handling behavior based on the different types of failure, for example, Diabase error or any error due to expiry of response timeout or Tx timer, etc.

result-code [to end-result-code]: result-code specifies the result code number, must be an integer from 3000 through 9999. end-result-code specifies the upper limit of a range of result codes. end-result-code must be greater than result-code.

action { continue [discard-traffic | local-fallback[without-retry] | retry-server-on-event | send-ccrt-on-call-termination | without-retry] | retry-and-terminate [max-transmissions *number-of-retries* | without-term-req] | terminate [without-term-req] }

Configures the action to be taken in the event of a communication failure with the server from one of the following:

- **continue** – In the event of a failure the user session continues. DCCA/Diameter will make periodic request and/or connection retry attempts and/or will attempt to communicate with a secondary peer depending on the peer configuration and session-binding setting.
  - **discard-traffic** – Continue the session but blocks/discards the data traffic.

    Use this command to specify the behavior in the event of a communication failure with the prepaid server. If there are different failure handling configurations present within the template for the same message type, the action is applied as per the latest error encountered.

    If previously configured, use the **no msg-type { credit-control-initial | credit-control-terminate | credit-control-update } failure-type any action continue discard-traffic** CLI command to remove the configuration associated with the failure handling template.

    The **discard-traffic** keyword takes effect when "continue" action is configured and Gy failure happens.

    This CLI option is disabled by default.
  - **local-fallback** – Continue the session with the PCC rules defined in the local policy.
    - **without-retry** – Continue the session without retrying the secondary PCRF server. By default, the message will be retried to secondary PCRF before falling back to the local policy.

      The **without-retry** keyword is introduced to support Overload Control on Diameter interfaces such as Gx, S6b and SWm and also to prevent network overload and outages. For more information on Diameter Overload Control feature, refer to the *AAA Interface Administration and Reference* guide.
  - **retry-server-on-event** – Reconnects to PCRF server on update and termination requests or re-authorization from server, for failure-handling CONTINUE sessions.



Important This option is valid only for credit-control-update request though it is allowed to configure for all the requests.

  - **send-ccrt-on-call-termination** – Sends CCR-T to PCRF on call termination for failure-handling CONTINUE.



Important This option is valid only for credit-control-update request though it is allowed to configure for all the requests.

- **without-retry** – Continue the session without retrying the secondary PCRF.

- **retry-and-terminate** – In the event of a failure the user session continues for the duration of one retry attempt with the server. If this retry attempt also fails, the session is terminated.
  - **max-transmissions** *number-of-retries*: Specifies the maximum number of retries to the server. The maximum server retries that can be configured is 5 and the default value for retries is 1. When max-retries are exhausted, session termination happens.

    CCR-U is retried for a maximum of number of retries configured in the failure handling template when experimental result code (4198 - DIAMETER_PENDING_TRANSACTION) is received from PCRF in CCA-U.



Important In releases prior to 17, CCR-U is retried for a maximum of number of times configured in the failure handling template when experimental result code with a proprietary value "4198 - DIAMETER_PENDING_TRANSACTION" is received from PCRF in CCA-U. In release 17 and later, support is added for Negotiation of Pending Transactions (PT) in initial session establishment, and the standards-defined experimental result code (4144) is used in CCA/RAA to advertise the support of the PT feature.

  - **without-term-req** – Terminate the session without sending the termination request (CCR-T).

- **terminate** – In the event of a failure the user session is terminated.
  - **without-term-req** – Terminate the session without sending the termination request (CCR-T).

Usage Guidelines

Use this command to specify the behavior in the event of a communication failure with the prepaid server. If there are different failure handling configurations present within the template for the same message type, the action is applied as per the latest error encountered.

Lookup is done first to identify if there is an exact match for **message-type** and **failure-type**. If not present, lookup is done for 'any' match for message and failure type.

That is, when there are multiple matches, it is preferred to find a match to a specifically configured value over a match to something configured with **any** or **any-error**. If there are multiple best matches, the one with a specifically configured **msg-type** over a match to **msg-type any** is preferred.

There are two levels of possible communication failure:

- The TCP connection failed
- DIAMETER routing failed to deliver a request or failed to receive a response.

The specified behavior is used for sessions when no behavior is specified by the server, such as by the CC-Failure-Handling AVP in DIAMETER messages. This command may be entered once for each type of message.

The following are the default action for Diameter result codes:

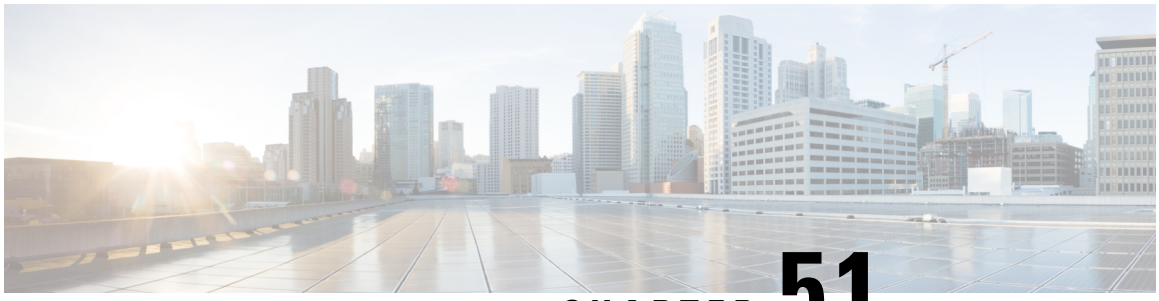
- For all protocol error codes 3000 to 3999, the default action is **terminate**. For all transient error codes 4000, 4001, 4004 to 4180, and 4182 to 4999, the default action is **continue**.
- For transient error codes 4002, 4003, and 4181, the default action is retry-and-**terminate**.

- For error code 4001, the default action is **terminate**.
- For permanent error codes 5000 to 5999, the default action is **terminate**.

Example

The following command configures to terminate the session when the Diameter application encounters a failure due to Diabase error in the Credit-Control Initial Request (CCR-I) message:

```
msg-type credit-control-initial failure-type diabase-error action terminate
```



CHAPTER 51

Diameter Host Select Configuration Mode Commands

Diameter Host Select Configuration Mode is accessed from the Global Configuration Mode. This mode allows an operator to configure Diameter host tables of peer servers that can be shared by different services.

Command Modes

Exec > Global Configuration > Diameter Host Select Configuration

configure > diameter-host-template *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-host-template)#
```

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

- end, on page 1097
- exit, on page 1098
- host-select row-precedence, on page 1098
- host-select table, on page 1101

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.

host-select row-precedence

This command configures individual rows of peer servers within the Diameter host table.

Product

GGSN

HA

HSGW

IPSG

PDSN

P-GW

SCM

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Diameter Host Select Configuration

configure > diameter-host-template *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-host-template)#
```

Syntax Description

In StarOS 14.1 and earlier releases:

host-select row-precedence *precedence* **table { 1 | 2 } host** *host_name* **[realm** *realm_id* **] [secondary host** *sec_host_name* **realm** *sec_realm_id* **]] [-noconfirm]**

host-select row-precedence *precedence* **table prefix-table { 1 | 2 } msisdn-prefix-from** *msisdn_prefix_from* **msisdn-prefix-to** *msisdn_prefix_to* **host** *host_name* **[realm** *realm_id* **] [secondary host** *sec_host_name* **realm** *sec_realm_id* **] [-noconfirm]**

no host-select row-precedence *precedence* **table { 1 | 2 | prefix-table { 1 | 2 } } [-noconfirm]**

In StarOS 15.0 and later releases:

host-select row-precedence *precedence* **table { 1 | 2 } host** *host_name* **[realm** *realm_id* **] [secondary host** *sec_host_name* **realm** *sec_realm_id* **]] [-noconfirm]**
host-select row-precedence *precedence* **table { { range-table { 1 | 2 } { imsi-based { [prefix | suffix]** *imsi-value* **[to** *imsi-value* **] } | msisdn-based { [prefix | suffix]** *msisdn-value* **[to** *msisdn-value* **] } } host** *host_name* **[realm** *realm_id* **] [secondary host** *sec_host_name* **realm** *sec_realm_id* **] algorithm { active-standby | round-robin }] } } [-noconfirm]**
no host-select row-precedence *precedence* **table { 1 | 2 | range-table { 1 | 2 } } [-noconfirm]**

no

Removes the specified row from the primary or secondary table or primary/secondary MSISDN prefix table for 14.0 and earlier releases, or IMSI/MSISDN range table for 15.0 and later releases.

row-precedence *precedence*

Specifies the row in the table as an integer from 1 through 128. Note that the row precedence number in IMSI/MSISDN configuration must be unique.

Important In StarOS release 14.0 and later, *precedence* may be an integer from 1 through 256 for SCM.

table { 1 | 2 }

Specifies the Diameter host table that will be edited.

- **1**: Specifies the primary table
- **2**: Specifies the secondary table

table prefix-table { 1 | 2 } msisdn-prefix-from *msisdn_prefix_from* msisdn-prefix-to *msisdn_prefix_to* host *host_name* [realm *realm_id*] [secondary host *sec_host_name* realm *sec_realm_id*]

Important This command syntax is applicable to StarOS release 14.1 and earlier.

prefix-table { 1 | 2 }: Specifies a primary or secondary table containing ranges of MSISDN prefixes.

msisdn-prefix-from *msisdn_prefix_from* **msisdn-prefix-to** *msisdn_prefix_to*: Specifies the starting and ending Mobile Station International Subscriber Directory Number (MSISDN) prefixes for a row in the prefix-table.

host *host_name*: Identifies the primary Diameter peer server to be added to this row by its host name. *host_name* can be entered as an IP address or a DNS hostname (1 through 128 alphanumeric characters).

secondary host *host_name*: Identifies the secondary Diameter peer server to be added to this row by its host name. *host_name* can be entered as an IP address or a DNS hostname (1 through 128 alphanumeric characters).

realm *realm_id*: Specifies an optional realm ID as an alphanumeric string of 1 through 128 characters.

msisdn-prefix-from *msisdn_prefix_from* msisdn-prefix-to *msisdn_prefix_to*

Specifies the starting and ending Mobile Station International Subscriber Directory Number (MSISDN) prefixes for a row in the prefix-table.

host *host_name*

Identifies the primary Diameter peer server to be added to this row by its host name.

host_name can be entered as an IP address or a DNS hostname (1 through 128 alphanumeric characters).

secondary host *host_name*

Identifies the secondary Diameter peer server to be added to this row by its host name.

host_name can be entered as an IP address or a DNS hostname (1 through 128 alphanumeric characters).

[realm *realm_id*]

Specifies an optional realm ID as an alphanumeric string of 1 through 128 characters.

table { { range-table { 1 | 2 }{ imsi-based { [prefix | suffix] *imsi-value* [to *imsi-value*] } | msisdn-based { [prefix | suffix] *msisdn-value* [to *msisdn-value*] } } host *host_name* [realm *realm_id*] [secondary host *sec_host_name* realm *sec_realm_id*] algorithm { active-standby | round-robin }] } }

Important This command syntax is applicable to StarOS release 15.0 and later.

range-table { 1 | 2 }: Specifies a primary or secondary table containing ranges of IMSI or MSISDN prefix/suffix.

imsi-based { [prefix | suffix] *imsi-value* **[to** *imsi-value* **] }**: Specifies to use the prefix/suffix/range values of IMSI of the subscriber for Diameter peer selection.

msisdn-based { [prefix | suffix] *msisdn-value* **[to** *msisdn-value* **] }**: Specifies to use the prefix/suffix/range values of MSISDN of the subscriber for Diameter peer selection.

host *host_name*: Identifies the primary Diameter peer server to be added to this row by its host name. *host_name* can be entered as an IP address or a DNS hostname (1 through 128 alphanumeric characters).

secondary host *host_name*: Identifies the secondary Diameter peer server to be added to this row by its host name. *host_name* can be entered as an IP address or a DNS hostname (1 through 128 alphanumeric characters).

realm *realm_id*: Specifies an optional realm ID as an alphanumeric string of 1 through 128 characters.

algorithm { active-standby | round-robin }: Specifies to select the algorithm to pick the primary and the secondary hosts either in an active standby mode or in round robin fashion.

[-noconfirm]

Executes the command without prompting for further input from the user.

Usage Guidelines

Use this command to add or modify individual rows in Diameter host server tables. Each table may contain up to 256 rows.

In Releases 15.0 and later, the existing CLI command "**host-select row-precedence**" in the Diameter Host Template Configuration mode is modified to enable the selection of Diameter peer based on the configured prefix/suffix/range values of IMSI or MSISDN of subscriber. This configuration change allows the overlapping range of IMSI or MSISDN values.

PCRF peer selection is based on the first match of prefix/suffix/range on row precedence priorities. If the subscriber's IMSI/MSISDN does not match with any configured IMSI/MSISDN range, then IMS Authorization application selects the default peer.



Important The length of IMSI or MSISDN range is the same in any IMSI or MSISDN host template configuration list.

Once a row is selected the failure handling for the subscriber is done based on this configuration. With this feature being turned on, the primary and the secondary hosts configured can be picked up in an active standby mode or in round robin fashion.

Example

The following command adds a row to a Diameter peer server table with the following parameters:

- row (precedence) = 1
- table = 1 (primary)
- Diameter peer server hostname = minid
- realm = namerica

```
host-select row-precedence 1 table 1 host minid realm namerica
```

host-select table

This command configures a table of peer servers associated with the Diameter host template.

Product

GGSN

HA

HSGW

IPSG

PDSN

P-GW

SCM

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Diameter Host Select Configuration

configure > diameter-host-template *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-host-template)#
```

Syntax Description

In StarOS 14.1 and earlier releases:

```
host-select table { 1 | 2 | prefix-table { 1 | 2 } } algorithm {
ip-address-modulus [ prefer-ipv4 | prefer-ipv6 ] | msisdn-modulus |
round-robin }
no host-select table
```

In StarOS 15.0 and later releases:

```
host-select table { 1 | 2 | range-table { 1 | 2 } } algorithm {
ip-address-modulus [ prefer-ipv4 | prefer-ipv6 ] | msisdn-modulus |
round-robin }
no host-select table
```

no

Removes the table associated with the Diameter host template.

table { 1 | 2 | prefix-table { 1 | 2 } }

Important This command syntax is applicable to StarOS release 14.1 and earlier.

Specifies the Diameter host table that will be edited.

- **1**: Specifies the primary table
- **2**: Specifies the secondary table
- **prefix-table { 1 | 2 }**: Specifies a primary or secondary table containing ranges of MSISDN prefixes.

This keyword option enables activating the configured table.

table { 1 | 2 | range-table { 1 | 2 } }

Important This command syntax is applicable to StarOS release 15.0 and later.

Specifies the Diameter host table that will be edited.

- **1**: Specifies the primary table
- **2**: Specifies the secondary table

- **range-table { 1 | 2 }**: Specifies a primary or secondary table containing ranges of IMSI or MSISDN prefix/suffix.

This keyword option enables activating the configured table.

algorithm { ip-address-modulus [prefer-ipv4 | prefer-ipv6] | msisdn-modulus | round-robin }

Specifies the algorithm to be used when selecting a row in this table.

- **ip-address-modulus**: Use an IP address (in binary) to select a row.
  - **prefer-ipv4**: If both IPv4 and IPv6 addresses are available, use the IPv4 address.
  - **prefer-ipv6**: If both IPv4 and IPv6 addresses are available, use the IPv6 address.
- **msisdn-modulus**: Use an MSISDN (without leading "+") to select a row.
- **round-robin**: Select a row in round-robin manner for each new session.



Important The Round Robin algorithm is effective only over a large number of selections, and not at a granular level.

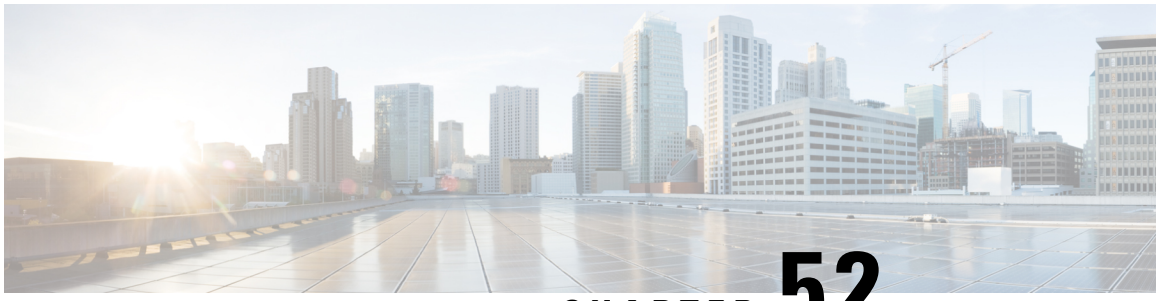
Usage Guidelines

Use this command to add or modify a Diameter host server table associated with a Diameter host template.

Example

The following command adds a primary table that uses the *ip-address-modulus* algorithm for selecting a row:

```
host-select table 1 algorithm ip-address-modulus
```



CHAPTER 52

DNS Client Configuration Mode Commands

The DNS Client Configuration Mode is used to manage the system's DNS interface and caching parameters.

Command Modes

Exec > Global Configuration > Context Configuration > DNS Client Configuration

configure > context *context_name* **> dns-client** *client_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dns-client)#
```

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

- bind, on page 1105
- cache algorithm, on page 1106
- cache size, on page 1107
- cache ttl, on page 1108
- case-sensitive, on page 1109
- description, on page 1110
- end, on page 1110
- exit, on page 1110
- randomize-answers, on page 1111
- resolver, on page 1111
- round-robin answers, on page 1112

bind

Binds the DNS client to a pre-configured logical IP interface.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DNS Client Configuration

configure > **context** *context_name* > **dns-client** *client_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dns-client)#
```

Syntax Description

```
bind { address ip_address [ port number ] | query-over-gtp }
no bind address
```

no

Removes the binding of the client to a specified interface.

bind address *ip_address*

Specifies the IP address of the interface to which the DNS client is being bound in IPv4 dotted-decimal notation.

bind port *number*

Specifies the UDP port number of the interface to which the DNS client is being bound as an integer from 1 to 65535. Default: 6011

bind query-over-gtp

Specifies that DNS client query is to be performed over GTP.

Usage Guidelines

Use this command to associate the client with a specific logical IP address.

Example

The following command binds the DNS client to a logical interface with an IP address of *10.2.3.4* and a port number of *6000*:

```
bind address 10.2.3.4 port 6000
```

cache algorithm

Configures the method of use for the DNS VPN and session cache.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DNS Client Configuration

configure > **context** *context_name* > **dns-client** *client_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dns-client)#
```

Syntax Description

```
cache algorithm { central | local } { FIFO | LRU | LFU }
default cache algorithm { central | local }
```

default

Sets the DNS VPN and session cache method to default setting.

central | local

central: Specifies the central proclet (VPN manager)

local: Specifies the local proclet (session manager)

FIFO | LRU | LFU

FIFO: First in first out. This is the default setting for the central proclet.

LRU: Least recently used. This is the default value for the local proclet.

LFU: Least frequently used.

Usage Guidelines

Use this command to configure the method by which entries are added and removed from the DNS cache.

Example

The following command configures the cache algorithm for the central proclet to least frequently used (LFU):

```
cache algorithm central lfu
```

cache size

Configures the maximum number of entries allowed in the DNS cache.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DNS Client Configuration

configure > context *context_name* **> dns-client** *client_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dns-client)#
```

Syntax Description

```
cache size { central | local } max_size
default cache size { central | local }
```

default

Sets the maximum number of entries allowed in the DNS cache to default setting.

{ central | local } *max_size*

central *max_size*: Specifies the maximum number of entries allowed in the central proclet cache as an integer from 100 through 65535. Default: 50000.

local *max_size*: Specifies the maximum number of entries allowed in the local proclet cache as an integer from 100 through 65535. Default: 1000.

Usage Guidelines

Use this command to configure the maximum number of entries allowed in the DNS cache.

Example

The following command configures the cache size of the central proclet to *20000*:

```
cache size central 20000
```

cache ttl

Configures the DNS cache time to live (TTL) for positive and negative responses.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DNS Client Configuration

configure > context *context_name* **> dns-client** *client_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dns-client)#
```

Syntax Description

```
cache ttl { negative | positive } seconds
default cache ttl { negative | positive }
no cache [ ttl { negative | positive } ]
```

no

Disables any or all configured DNS cache parameters.

default

Sets the DNS cache time to live for positive and negative responses to the default setting.

{ negative | positive } *seconds*

negative *seconds*: Specifies the time to live for negative responses as an integer from 60 through 86400. Default: 60.

Note The DNS client is always reinitialized when the **ip name-servers** CLI configuration is changed for a context. As a result, the **cache ttl negative** value is reset to the default value if **no cache ttl negative** CLI is configured for the DNS client in the context. Therefore, check and reconfigure the **no cache ttl negative** CLI after the **ip name-servers** CLI configuration is changed on the node.

positive *seconds*: Specifies the time to live for positive responses. as an integer from 60 through 86400. Default: 86400 (1 day).

Usage Guidelines Use this command to adjust the DNS cache time to live.

Example

The following commands set the TTL DNS cache to *90* seconds for negative responses and *43200* seconds for positive responses:

```
cache ttl negative 90
cache ttl positive 43200
```

case-sensitive

Configures the case sensitivity requirement for responses to DNS requests.

Product All

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > DNS Client Configuration

configure > context *context_name* **> dns-client** *client_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dns-client)#
```

Syntax Description **`[ default | no ] case-sensitive response`**

default

Returns the command to its default setting of disabled.

no

Disables the requirement for case sensitivity in DNS responses.

case-sensitive response

Enables the requirement for case sensitivity in DNS responses.

Usage Guidelines Use this command to require case sensitivity (identical case usage between request and response) on all responses to DNS request messages.

description

Allows you to enter descriptive text for this configuration.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

description *text*
no description

no

Clears the description for this configuration.

text

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

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

Usage Guidelines

The description should provide useful information about this configuration.

end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

end

Usage Guidelines

Use this command to return to the Exec mode.

exit

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

exit

Usage Guidelines

Use this command to return to the parent configuration mode.

randomize-answers

Configures the DNS client to return DNS answers in random fashion if multiple results are available for a DNS query.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DNS Client Configuration

configure > context *context_name* **> dns-client** *client_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-dns-client)#`

Syntax Description

`[no | default] randomize-answers`

no

Removes the configured random method for DNS answers.

default

Disables the random method for DNS answers.

randomize-answers

Enables the random method for DNS answers.

Usage Guidelines

Use this command to configure the DNS client to return the DNS results in a random fashion if multiple results are available for a DNS query.

Only one valid option can be used for distribution of DNS answers: default, round-robin, or randomized.

Example

The following command configures the DNS client to use randomize the DNS query answers if multiple results are available for a DNS query:

`randomize-answers`

resolver

Configures the number of DNS query retries and the retransmission interval once the response timer expires.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DNS Client Configuration

configure > context *context_name* **> dns-client** *client_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dns-client)#
```

Syntax Description

resolver { number-of-retries *retries* **| retransmission-interval** *time* **}**
default resolver { number-of-retries | retransmission-interval }

default

Resets the specified resolver configuration to the default.

number-of-retries *retries*

Configures the number of DNS query retries on DNS response timeout as an integer from 0 through 4. Default: 2.

retransmission-interval *time*

Configures the initial retransmission interval (in seconds) for retransmission after the DNS response timeout as an integer from 2 to 5. Default is 3 seconds. The retransmission interval doubles after each retry when only one server is configured. In case both primary and secondary servers are configured, the retransmission time is doubled for the last retry.

Usage Guidelines

Set the DNS retransmission retries or the retransmission interval. Issue the command twice to configure both parameters, one-at-a-time.

Example

The following command sets the DNS resolver retries to *4*:

```
resolver number-of-retries 4
```

round-robin answers

Configures the DNS client to return the DNS results in round-robin fashion if multiple results are available for a DNS query.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > DNS Client Configuration

configure > context *context_name* **> dns-client** *client_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dns-client)#
```

Syntax Description

```
[ no | default ] round-robin-answers
```

no

Removes the configured round robin method for DNS answer.

default

Disables the round robin method for DNS answer.

round-robin-answers

Enables the round robin method for DNS answer.

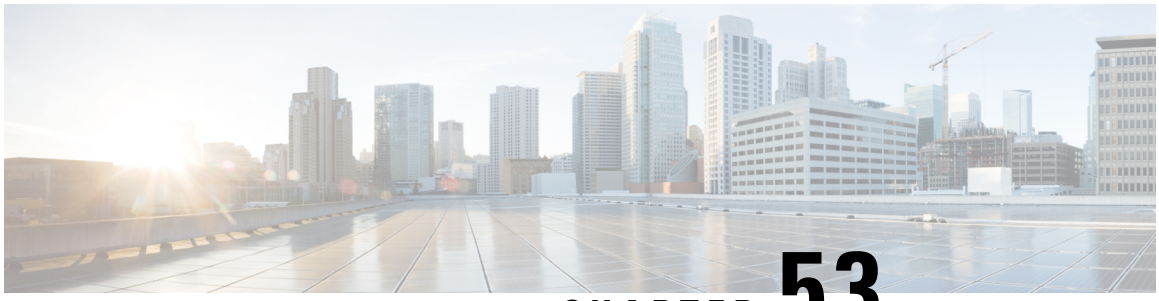
Usage Guidelines

Use this command to configure the DNS client to return the DNS results in round-robin fashion if multiple results are available for a DNS query.

Example

The following command configures the DNS client to use round robin method for DNS query answers:

```
round-robin-answers
```



CHAPTER 53

DSCP Template Configuration Mode Commands

Command Modes

The DSCP Template Configuration Mode provides the commands to configure DSCP marking for control packets and data packets for Gb over IP. Any number of DSCP templates can be generated in the SGSN Global configuration mode and then a template can be associated with one or more GPRS Services via the commands in the GPRS Service configuration mode.

Exec > Global Configuration > SGSN Global Configuration > DSCP Template Configuration

configure > context *context_name* **> sgsn-global > dscp-template** *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dscp-template-template_name)#
```

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

- control-packet, on page 1115
- end, on page 1117
- exit, on page 1117
- data-packet, on page 1118

control-packet

Configures the diffserv code point marking (DSCP) value for 3GPP quality of service (QoS) class downlink control packets.

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

HNB-GW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration > DSCP Template Configuration

configure > context *context_name* **> sgsn-global > dscp-template** *template_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dscp-template-template_name)#
```

Syntax Description

```
control-packet qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31
 | af32 | af33 | af41 | af42 | af43 | be | cs1 | cs2 | cs3 | cs4 | cs5 |
 cs6 | cs7 | ef }
 default control-packet
```

default

Resets the quality of service (QoS) DSCP setting to the 'BE' (best effort) default value.

DSCP marking option

Select one of the following downlink DSCP options for the control packets:

• **af11:** Assured Forwarding 11 per-hop-behavior (PHB)	• **be:** Best Effort for Forwarding
• **af12:** Assured Forwarding 12 PHB	• **cs1:** Class Selector 1 PHB
• **af13:** Assured Forwarding 13 PHB	• **cs2:** Class Selector 2 PHB
• **af21:** Assured Forwarding 21 PHB	• **cs3:** Class Selector 3 PHB
• **af22:** Assured Forwarding 22 PHB	• **cs4:** Class Selector 4 PHB
• **af23:** Assured Forwarding 23 PHB	• **cs5:** Class Selector 5 PHB
• **af31:** Assured Forwarding 31 PHB	• **cs6:** Class Selector 6 PHB
• **af32:** Assured Forwarding 32 PHB	• **cs7:** Class Selector 7 PHB
• **af33:** Assured Forwarding 33 PHB	• **ef:** Expedited forwarding PHB
• **af41:** Assured Forwarding 41 PHB	
• **af42:** Assured Forwarding 42 PHB	
• **af43:** Assured Forwarding 43 PHB	

Usage Guidelines

This command configures the QoS DSCP marking type for downlink control packets.

Related commands for SGSN:

- To create/delete a DSCP template, use the **dscp-template** in the SGSN Global configuration mode (see the *SGSN Global Configuration Mode Commands* section).
- To associated a specpific DSCP template with a specific GPRS service configuration, use the **associate-dscp-template downlink** documented in the *GPRS Service Configuration Mode Commands* section.
- To check values configured for DSCP templates, use the **show sgsn-mode** command documented in the *Exec Mode Commands* section.

Related commands for HNB-GW:

- To create/delete a DSCP template, use the **dscp-template** in the *SGSN Global Configuration Mode*.
- To associated a specpific DSCP template with a system for a PSP instance in SS7 routing domain, use **associate-dscp-template downlink** documented in the *SGSN PSP Configuration Mode Commands* section.

Example

Use a command similar to the following to set expedited forward per-hop behavior for the downlink control packets:

```
control-packet qos-dscp ef
```

Use the following command to reset the default best effort per-hop behavior:

```
default control-packet
```

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.

data-packet

Configures the diffserv code point marking (DSCP) value for 3GPP quality of service (QoS) class downlink data packets.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > SGSN Global Configuration > DSCP Template Configuration

configure > **context** *context_name* > **sgsn-global** > **dscp-template** *template_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-dscp-template-`*`template_name`*`)#`

Syntax Description

```
control-packet { background | conversationa | interactive { priority1 |
priority2 | priority3 } | streaming } qos-dscp { af11 | af12 | af13 |
af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs1
| cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }
default data-packet { background | conversationa | interactive { priority1
 | priority2 | priority3 } | streaming }
```

default

Resets the quality of service (QoS) DSCP setting to the **be** (best effort) default value.

background | conversationa | interactive | streaming

Select the QoS traffic class of service for the downlink data packets.

priority1 | priority2 | priority3

Select the traffic handling priority to be applied to the specified traffic class.

DSCP option

Select one of the following DSCP settings for the selected traffic class. Default is best effort (**be**) for all traffic classes settings.

• **af11:** Assured Forwarding 11 per-hop-behavior (PHB)	• **be:** Best Effort for Forwarding
• **af12:** Assured Forwarding 12 PHB	• **cs1:** Class Selector 1 PHB
• **af13:** Assured Forwarding 13 PHB	• **cs2:** Class Selector 2 PHB
• **af21:** Assured Forwarding 21 PHB	• **cs3:** Class Selector 3 PHB
• **af22:** Assured Forwarding 22 PHB	• **cs4:** Class Selector 4 PHB

• **af23:** Assured Forwarding 23 PHB	• **cs5:** Class Selector 5 PHB
• **af31:** Assured Forwarding 31 PHB	• **cs6:** Class Selector 6 PHB
• **af32:** Assured Forwarding 32 PHB	• **cs7:** Class Selector 7 PHB
• **af33:** Assured Forwarding 33 PHB	• **ef:** Expedited forwarding PHB
• **af41:** Assured Forwarding 41 PHB	
• **af42:** Assured Forwarding 42 PHB	
• **af43:** Assured Forwarding 43 PHB	

Usage Guidelines

This command configures the QoS DSCP marking type for downlink data packets. DSCP levels indicate how packets are to be handled

Related commands:

- To create/delete a DSCP template, use the **dscp-template** in the SGSN Global configuration mode (see the *SGSN Global Configuration Mode Commands* section).
- To associated a specpific DSCP template with a specific GPRS service configuration, use the **associate-dscp-template downlink** documented in the *GPRS Service Configuration Mode Commands* section.
- To check values configured for DSCP templates, use the **show sgsn-mode** command documented in the *Exec Mode Commands* section.

Example

Use a command similar to the following to set expedited forward per-hop behavior for the downlink control packets:

```
control-packet qos-dscp ef
```

Use the following command to reset the default best effort per-hop behavior:

```
default control-packet
```