Command Line Interface Reference, Modes C - D, StarOS Release 19

First Published: 2015-09-30
Last Modified: 2017-01-12

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.

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

© 2017 Cisco Systems, Inc. All rights reserved.
CHAPTER 1

Call Control Profile Configuration Mode  1

a-msisdn  7
access-restriction-data  8
accounting context   11
accounting mode      13
accounting stop-trigger  15
allocate-ptmsi-signature  16
apn-restriction  17
associate  19
attach access-type   22
attach allow  26
attach imei-query-type   28
attach restrict  30
authenticate activate  34
authenticate all-events  36
authenticate attach  38
authenticate context  40
authenticate detach  42
authenticate on-first-vector  43
authenticate rau  45
authenticate service-request  47
authenticate sms  49
authenticate tau  51
c
cc  53
check-zone-code  55
ciphering-algorithm-gprs  56
csfb  57
description  59
diameter-result-code-mapping 60
direct-tunnel 62
dns-ggsn 64
dns-mrme 65
dns-msc 67
dns-sgsn 69
dns-pgw 70
dns-sgw 71
egtp 72
eir-profile 74
encryption-algorithm-lte 75
encryption-algorithm-umts 76
end 78
epdg-s2b-gtpv2 79
equivalent-plmn 80
exit 82
gbr-bearing-preservation-timer 83
gmm Extended-T3312-timeout 84
gmm information-in-messages 86
gmm rau-accept 88
gmm retrieve-equipment-identity 90
gmm t3346 92
gs-service 94
gtp send 96
gtpp 99
gtpu fast-path 100
guti 102
gw-selection 104
hss 107
ignore-ul-data-status 109
idle-mode-signaling-reduction 110
integrity-algorithm-lte 112
integrity-algorithm-umts 113
lcs-mo 114
lcs-mt 115
lcs-ni 116
local-cause-code-mapping apn-mismatch 117
local-cause-code-mapping apn-not-subscribed 119
local-cause-code-mapping apn-not-supported-in-plmn-rat 120
local-cause-code-mapping auth-failure 122
local-cause-code-mapping congestion 124
local-cause-code-mapping ctxt-xfer-fail-mme 126
local-cause-code-mapping ctxt-xfer-fail-sgsn 128
local-cause-code-mapping gw-unreachable 130
local-cause-code-mapping hss-unavailable 132
local-cause-code-mapping map-cause-code 134
local-cause-code-mapping no-active-bearers 136
local-cause-code-mapping odb packet-services 138
local-cause-code-mapping odb roamer-to-vplmn 140
local-cause-code-mapping path-failure 142
local-cause-code-mapping peer-node-unknown 143
local-cause-code-mapping pgw-selection-failure 145
local-cause-code-mapping restricted-zone-code 147
local-cause-code-mapping sgw-selection-failure 149
local-cause-code-mapping vlr-down 151
local-cause-code-mapping vlr-unreachable 153
location-area-list 155
location-reporting 157
lte-zone-code 159
map 161
map-service 164
max-bearers-per-subscriber 165
max-pdns-per-subscriber 166
min-unused-auth-vectors 167
mobility-protocol 168
mps 169
msc-fallback-disable 171
network-feature-support-ie 173
network-initiated-pdp-activation 175
override-arp-with-ggsn-arp 179
paging-priority 180
pcscf-restoration 182
pdp-activate access-type 183
pdp-activate allow 185
pdp-activate restrict 187
pdn-type-override 189
peer-mme 191
peer-mse 193
peer-nri-length 194
plmn-protocol 196
prefer subscription-interface 198
ptmsi-reallocate 200
ptmsi-signature-reallocate 203
qos 205
rau-inter 208
rau-inter-plmn 212
rau-intra 216
re-authenticate 219
regional-subscription-restriction 220
release-access-bearer 223
reporting-action 225
reuse-authentication-triplets 226
rfsp-override 227
rfsp-override ue-settings 229
s1-reset 231
samog-gtpv1 232
samog-s2a-gtpv2 234
sctp-down 235
sgs-cause-code-mapping 236
sgsn-address 238
sgsn-core-nw-interface 241
sgsn-number 243
sgtp-service 245
sms-mo 246
sms-mt 248
CHAPTER 2

Call-Home Configuration Mode 269
activate 271
alert-group 272
contact-email-addr 274
contract-id 275
customer-id 276
end 277
exit 278
mail-server 279
phone-number 280
profile 281
rate-limit 282
sender 283
site-id 285
street-address 286

CHAPTER 3

Call-Home Profile Configuration Mode 287
active 288
destination 289
end 291
exit 292
subscribe-to-alert-group 293
CHAPTER 4  CAMEL Service Configuration Mode Commands 297

associate-sccp-network 298
end 299
exit 300
tcap destination-address 301
timeout 302

CHAPTER 5  Card Configuration Mode Commands 305

aps 306
end 308
exit 309
framing 310
header-type 312
initial-e1-framing 313
link-aggregation 314
mode 316
redundancy 318
redundant with 321
service-type 322
shutdown 324

CHAPTER 6  CBS Service Configuration Mode Commands 325

bind 326
cbc-address-validation 327
cbc-server 328
end 330
exit 331
sabp timer 332
sabp-class2-aggregation 333
tcp-keepalive 334
tcp-mode 335

CHAPTER 7  CGW Service Configuration Mode Commands 337

associate 338
CHAPTER 8

Channelized Port Configuration Mode Commands 353

alarm-disable 355
alarm-soak-timer 357
clock-source 358
description 359
dlci 360
dlci 360
exit 363
frame-relay 364
hopath-sdfs 366
line-timing 367
loopback 368
hopath-sdfs 369
path 370
preferred slot 374
pwe3-cesopsn 375
shutdown 376
snmp trap link-status 377
threshold high-activity 378
threshold monitoring 380
threshold rx-utilization 382
threshold tx-utilization 384
toh-sdfs 386
vc-mapping 387
CHAPTER 9

Cipher Suite Configuration Mode Commands 389

   encryption 390
   end 391
   exit 392
   hmac 393
   key-exchange 394

CHAPTER 10

Class-Map Configuration Mode Commands 395

   end 396
   exit 397
   match any 398
   match dst-ip-address 399
   match dst-port-range 400
   match ip-tos 401
   match ipsec-spi 403
   match packet-size 404
   match protocol 405
   match src-ip-address 407
   match src-port-range 408

CHAPTER 11

Congestion Action Profile Configuration Mode Commands 409

   ddn 410
   drop 412
   end 414
   exclude-emergency-events 415
   exclude-voice-events 416
   exit 417
   none 418
   reject 420
   report-overload 423

CHAPTER 12

Connected Apps Configuration Mode Commands 425

   activate 426
   ca-certificate-name 427
CHAPTER 13
Content Filtering Policy Configuration Mode Commands 439

analyze 440
discarded-flow-content-id 445
end 446
exit 447
failure-action 448
timeout action 450

CHAPTER 14
Content Filtering Server Group Configuration Mode Commands 451

connection retry-timeout 452
deny-response code 453
dictionary 455
end 457
exit 458
failure-action 459
icap server 462
origin address 464
response-timeout 465
timeout action 466
url-extraction 467

CHAPTER 15
Context Configuration Mode Commands A-D 469

aaa accounting 472
aaa authentication 474
aaa constructed-nai 476

end 428
exit 429
ha-chassis-mode 430
ha-network-mode 431
rri-mode 432
sess-ip-address 434
sess-name 435
sess-passwd 436
sess-userid 437

aaa filter-id rulebase mapping  478
aaa group  479
aaa nai-policy  481
access-list undefined  483
administrator  484
apn  487
asn-qos-descriptor  489
asn-service-profile  491
asngw-service  493
asnpe-service  495
associate  497
bfd-protocol  499
bgp extended-asn-cap  500
bmsc-profile  501
busyout ip  503
busyout ipv6  505
cae-group  507
camel-service  508
cbs-service  510
cipher-suite  511
class-map  513
closedrp-rp handoff  515
config-administrator  516
content-filtering  519
credit-control-service  520
crypto dns-nameresolver  522
crypto group  523
crypto ipsec transform-set  525
crypto map  527
crypto template  529
css server  531
description  532
dhcp-client-profile  533
dhcp-server-profile  535
dhcp-service  537
dhcpv6-service  539
  
  diameter accounting  541
  
  diameter authentication  544
  
  diameter authentication failure-handling  547
  
  diameter dictionary  549
  
  diameter endpoint  550
  
  diameter-hdd-module  552
  
  diameter sctp  554
  
  diameter origin  556
  
  dns-client  557
  
  domain  559

---

**CHAPTER 16**

*Context Configuration Mode Commands E-H*  561

  eap-profile  564
  
  edr-module active-charging-service  565
  
  egtp-service  567
  
  end  569
  
  epdg-service  570
  
  event-notif-endpoint  572
  
  exit  574
  
  external-inline-server  575
  
  fa-service  576
  
  firewall max-associations  578
  
  fng-service  579
  
  ggsn-service  580
  
  gprs-service  582
  
  gs-service  584
  
  gtpc overload-protection egress  586
  
  gtpc overload-protection ingress  588
  
  gtpp algorithm  590
  
  gtpp attribute  592
  
  gtpp charging-agent  603
  
  gtpp data-record-format-version  605
  
  gtpp data-request sequence-numbers  607
  
  gtpp dead-server suppress-cdrs  609
ikev1 keepalive dpd  674
ikev1 policy  676
ikev2-ikesa  678
ims-auth-service  680
ims-sh-service  682
inspector  684
interface  687
ip access-group  690
ip access-list  692
ip arp  694
ip as-path access-list  696
ip community-list  698
ip dns-proxy source-address  700
ip domain-lookup  701
ip domain-name  702
ip extcommunity-list  703
ip forward  705
ip guarantee  706
ip identification packet-size-threshold  707
ip igmp profile  708
ip localhost  709
ip name-servers  710
ip pool  712
ip prefix-list  726
ip prefix-list sequence-number  728
ip route  729
ip routing maximum-paths  732
ip routing overlap-pool  733
ip rri  734
ip rri-route  735
ip sri-route  737
ip vrf  739
ip vrf-list  741
ipms  742
ipne-service  744
ipsec replay 745
ipsec transform-set 746
ipsg-service 747
ipv6 access-group 749
ipv6 access-list 750
ipv6 dns-proxy 751
ipv6 neighbor 752
ipv6 pool 753
ipv6 prefix-list 758
ipv6 prefix-list sequence-number 760
ipv6 route 761
ipv6 route-access-list 764
ipv6 rri 766
ipv6 rri-route 767
ipv6 sri-route 769
isakmp disable-phase1-rekey 770
isakmp keepalive 771
isakmp policy 772
iups-service 773
l2tp peer-dead-time 775
lac-service 776
lawful-intercept 778
lawful-intercept dictionary 779
lma-service 780
lns-service 782
location-service 784
logging 786
mag-service 788
map-service 790
mipv6ha-service 792
mme-service 794
mobile-access-gateway 796
mobile-ip fa 797
mobile-ip ha assignment-table 799
mobile-ip ha newcall 801
mobile-ip ha reconnect  803
mpls bgp forwarding  804
mpls exp  805
mpls ip  806
mseg-service  807
multicast-proxy  808

CHAPTER 18

Context Configuration Mode Commands N-R  811
nw-reachability server  814
network-requested-pdp-context activate  816
network-requested-pdp-context gsn-map  818
network-requested-pdp-context hold-down-time  820
network-requested-pdp-context interval  821
network-requested-pdp-context sgsn-cache-time  822
operator  823
optimize pdsn inter-service-handoff  826
pcc-af-service  827
pcc-policy-service  829
pcc-service  831
pcc-sp-endpoint  833
pdg-service  835
pdif-service  836
pdsn-service  837
pdsnclsdnp-service  839
pgw-service  841
pilot-packet  843
policy  846
policy-group  847
policy-map  848
ppp  849
ppp magic-number  854
ppp statistics  855
proxy-dns intercept-list  857
radius accounting  859
radius accounting algorithm  862
radius accounting apn-to-be-included 864
radius accounting billing-version 865
radius accounting gtp trigger-policy 866
radius accounting ha policy 867
radius accounting interim volume 868
radius accounting ip remote-address 870
radius accounting keepalive 872
radius accounting rp 874
radius accounting server 877
radius algorithm 881
radius allow 882
radius attribute 884
radius authenticate null-username 887
radius authenticate apn-to-be-included 888
radius authenticator-validation 889
radius change-authorize-nas-ip 890
radius charging 893
radius charging accounting algorithm 895
radius charging accounting server 897
radius charging algorithm 899
radius charging server 900
radius deadtime 902
radius detect-dead-server 904
radius dictionary 906
radius group 908
radius ip vrf 909
radius keepalive 911
radius max-outstanding 913
radius max-retries 914
radius max-transmissions 915
radius mediation-device 917
radius probe-interval 918
radius probe-max-retries 919
radius probe-message 920
radius probe-timeout 921
radius server 922
radius strip-domain 925
radius timeout 926
radius trigger 927
remote-server-list 929
route-access-list extended 931
route-access-list named 933
route-access-list standard 935
route-map 937
router 939

CHAPTER 19

Context Configuration Mode Commands S-Z 941

s102-service 943
saegw-service 945
sbc-service 947
server 948
service-redundancy-protocol 950
session-event-module 951
sgsn-service 952
sgs-service 954
sgtp-service 956
sgw-service 958
sls-service 960
ssh 962
ssl 964
subscriber 965
threshold available-ip-pool-group 967
threshold ha-service init-rrq-rcvd-rate 969
threshold ip-pool-free 971
threshold ip-pool-hold 973
threshold ip-pool-release 975
threshold ip-pool-used 977
threshold monitoring 979
threshold pdsn-service init-rrq-rcvd-rate 981
twan-profile 983
udr-module active-charging-service 984
wsg-service 985

CHAPTER 20

Credit Control Configuration Mode Commands 987
apn-name-to-be-included 990
app-level-retransmission 991
associate 992
charging-rulebase-name 994
diameter dictionary 996
diameter disable-final-reporting-in-ccru 998
diameter dynamic-rules request-quota 1000
diameter enable-quota-retry 1001
diameter exclude-mscc-in-ccr-terminate 1002
diameter fui-redirected-flow 1003
diameter gsu-with-only-infinite-quota 1004
diameter hdd 1005
diameter ignore-returned-rulebase-id 1007
diameter ignore-service-id 1008
diameter mscc-final-unit-action terminate 1009
diameter mscc-per-ccr-update 1011
diameter msg-type 1013
diameter origin host 1016
diameter origin endpoint 1017
diameter peer-select 1018
diameter pending-timeout 1021
diameter reauth-blacklisted-content 1023
diameter redirect-url-token 1025
diameter redirect-validity-timer 1027
diameter result-code 1029
diameter send-ccri 1031
diameter service-context-id 1033
diameter session failover 1034
diameter update-dictionary-avps 1036
end 1038
event-based-session 1039
exit 1041
failure-handling 1042
gy-rf-trigger-type 1046
imsi-imeisv encode-format 1048
mode 1049
pending-traffic-treatment 1050
quota 1053
quota request-trigger 1054
quota time-threshold 1056
quota units-threshold 1057
quota volume-threshold 1059
radius usage-reporting-algorithm 1061
redirect-indicator-received 1062
redirect-require-user-agent 1064
servers-unreachable 1065
subscription-id service-type 1071
timestamp-rounding 1073
trigger type 1075
usage-reporting 1077

CHAPTER 21
Credit Control Service Configuration Mode Commands 1079
diameter dictionary 1080
diameter endpoint 1081
end 1082
exit 1083
failure-handling 1084
request timeout 1086

CHAPTER 22
Crypto Group Configuration Mode Commands 1087
end 1088
exit 1089
match address 1090
match ip pool 1092
switchover 1094
match 1154
natt 1156
ocsp 1157
payload 1159
peer 1161
remote-secret-list 1163
whitelist 1164

CHAPTER 27

Crypto Map IPSec IKEv1 Configuration Mode Commands 1165
end 1166
exit 1167
match address 1168
match crypto group 1170
match ip pool 1172
set 1174

CHAPTER 28

Crypto Map IKEv2-IPv4 Payload Configuration Mode Commands 1179
end 1180
exit 1181
ipsec 1182
lifetime 1183
rekey 1185

CHAPTER 29

Crypto Map IKEv2-IPv6 Configuration Mode Commands 1187
allow-cert-enc cert-hash-url 1189
authentication 1190
blacklist 1192
certificate list 1193
ca-crl list 1195
certificate 1197
control-dont-fragment 1199
dont-fragment 1201
exit 1202
ikev2-ikesa 1203
keepalive 1206
match 1208
ocsp 1210
payload 1212
peer 1214
remote-secret-list 1216
whitelist 1217

CHAPTER 30  
Crypto Map IKEv2-IPv6 Payload Configuration Mode Commands 1219
  end 1220
  exit 1221
  ipsec 1222
  lifetime 1224
  rekey 1226

CHAPTER 31  
Crypto Template Configuration Mode Commands 1229
  allow-cert-enc cert-hash-url 1231
  allow-custom-fqdn-idr 1232
  authentication 1233
  blacklist 1235
  ca-certificate list 1236
  ca-crl list 1237
  certificate 1238
  configuration-payload 1239
  control-dont-fragment 1240
  dns-handling 1241
  dos cookie-challenge notify-payload 1243
  end 1245
  exit 1246
  identity local 1247
  ikev2-ikesa 1248
  ip 1251
  ipv6 1253
  keepalive 1254
  max-childsa 1255
  nai 1256
natt 1258
notify-payload 1259
ocsp 1261
payload 1263
peer network 1265
remote-secret-list 1266
timeout 1267
whitelist 1268

CHAPTER 32

Crypto Template IKEv2-Dynamic Payload Configuration Mode Commands 1269
end 1271
exit 1272
ignore-rekeying-requests 1273
ip-address-allocation 1274
ipsec transform-set 1276
lifetime 1277
maximum-child-sa 1278
rekey 1279
tsi 1280
tsr 1281

CHAPTER 33

Crypto IPSec Transform Set Configuration Mode Commands 1283
end 1284
exit 1285
mode 1286

CHAPTER 34

CSCF ATCF-ATGW Policy Configuration Mode Commands 1287
criteria 1288
end 1290
exit 1291
ps-cs-alerting 1292

CHAPTER 35

CSCF Access Profile Configuration Mode Commands 1293
access-security-type 1294
authentication 1295
CHAPTER 36
CSCF ACL Configuration Mode Commands 1305
after 1306
before 1307
deny 1308
derect 1309
redirect 1310

CHAPTER 37
CSCF AoR Policy Rules Configuration Mode Commands 1321
after 1322
aor 1323
before 1324
end 1325
exit 1326

CHAPTER 38
CSCF ATCF-ATGW Configuration Mode Commands 1327
call-linger-timer 1328
des 1329
exit 1330
mgmt-uri 1331
polocy name 1332
stm-sr 1333
trusted scc-as 1334

CHAPTER 39
CSCF Charging Configuration Mode Commands 1335
des 1336
exclude 1337
CHAPTER 40 CSCF Crypto Template Configuration Mode Commands 1341
end 1342
exit 1343
ipsec 1344

CHAPTER 41 CSCF Diameter Selection Configuration Mode Commands 1345
aaa-group 1346
end 1349
exit 1350

CHAPTER 42 CSCF EATF Configuration Mode Commands 1351
e-stn-sr 1352
end 1353
exit 1354

CHAPTER 43 CSCF Emergency-CSCF Configuration Mode Commands 1355
eatf 1356
end 1357
exit 1358
plani 1359
privacy 1361
psap-file 1362

CHAPTER 44 CSCF Enforce Codec Policy Configuration Mode Commands 1363
dynamic-codec 1364
end 1366
exit 1367
static-codec 1368

CHAPTER 45 CSCF IFC SPT Group Mode Commands 1371
end 1372
exit 1373
spt-condition 1374
exit 1413
hunting-method 1414
server 1415

CHAPTER 52
CSCF Peer Servers Group Configuration Mode Commands 1417
end 1418
exit 1419
peer-servers 1420

CHAPTER 53
CSCF Peer Server Monitoring Configuration Mode Commands 1423
dummy-as 1424
end 1425
exit 1426
ims-capable 1427
lro-selection-profile 1428
mode 1429
monitor-status 1430
nw-session-template 1432
registration 1433
tps-rate 1434

CHAPTER 54
CSCF Policy Configuration Mode Commands 1435
aor-policy-rules 1436
end 1437
exit 1438
service-policy-rules 1439

CHAPTER 55
CSCF Policy Rules Configuration Mode Commands 1441
allow-noauth 1443
allow-unsecure 1444
authorization 1445
end 1447
enforce-codec-policy 1448
exit 1449
max-cscf-concurrent-sessions 1450
policy 1452
qos 1454
signalling-bearer-loss 1456
video-sessions 1457

CHAPTER 56
CSCF Prefix Table Configuration Mode Commands 1459
end 1460
exit 1461
number 1462

CHAPTER 57
CSCF Proxy-CSCF Configuration Mode Commands 1465
allow rfc3261-ua-interworking 1467
atcf-atgw 1468
core-reg-expiry-time 1469
diameter 1470
emergency 1474
emergency-call-mode 1476
end 1477
exit 1478
interrogating-cscf-role 1479
message-max-size 1480
network-id 1481
perf-policy-control 1482
peer-sbc 1483
plmn-id 1485
reg-preloaded-route 1486
reg-service-route 1487
reliable-prov-resp 1488
restoration-procedure 1489
security-parameters 1490
sigcomp 1491
sip-header 1492
sip-param 1494
store-session-path 1496
C H A P T E R  5 8

CSCF Routes Configuration Mode Commands  1497

  after  1498
  before  1499
  end  1500
  exit  1501
  route  1502

C H A P T E R  5 9

CSCF Service Configuration Mode Commands  1513

  RetryAfter-header-value  1516
  access-service  1517
  access-type  1519
  allow-dereg  1522
  bind  1523
  caller-preference  1526
  charging  1527
  cnsa-media-profile  1528
  core-service  1530
  custom cdf-selection  1531
  custom reason-header-cause  1532
  custom reg-binding  1534
  custom response  1535
  custom volte  1538
  default-aor-domain  1539
  emergency-cscf  1540
  end  1541
  exit  1542
  history-info  1543
  interface statistics sip  1544
  interrogating-cscf  1545
  ipv4-ipv6-interworking  1546
  keepalive  1547
  lawful-intercept  1549
  li-packet-cable  1550
  max-reqmsg-size  1551
max-sipmsg-size 1552
media-bridging 1553
monitoring 1554
multiple-reg same-private-id 1555
nat-policy 1556
nat-pool 1558
policy 1560
policy-name 1563
proxy-cscf 1564
proxy-serving-cscf 1565
recurse-on-redirect-resp 1566
reject-on-cnsa-failure 1567
release-call-on-media-loss 1568
rfc3261-proxy 1569
server-header 1570
server-name 1572
serving-cscf 1573
serving-cscf-list 1574
session-timer 1576
strict-check configured-aor-domain 1578
strict-outbound 1579
subscriber-policy-override 1580
subscription 1581
support-content-type any 1583
tcp-proxy 1584
threshold 1585
timeout 1587
transport-switching 1590
trusted-domain-entity 1591

CHAPTER 60

CSCF Security Configuration Mode Commands 1593

auth-failure-weight 1594
bad-request-weight 1596
dos-prevention 1598
end 1599
CHAPTER 61

CSCF Serving-CSCF Configuration Mode Commands 1611

3gpp 1613
allow rfc3261-ua-interworking 1615
as-call invite-request-uri update 1616
authentication 1617
bgcf-proxy 1620
diversion-info 1622
end 1623
exit 1624
forking 1625
interrogating-cscf-role 1627
lir-failure 1628
local-call-features 1629
network-id 1630
npdb-client 1631
policy 1633
registration lifetime 1634
reliable-prov-resp 1636
server-name 1637
sfc 1638
sip-header insert 1639
sip-request 1640
tas 1642
tas-service 1643
user-authorization 1644

CHAPTER 62

CSCF Session Template Configuration Mode Commands 1645

end 1646
CHAPTER 63  CSCF Signalling Compression Configuration Mode Commands  1655

  compression-mode  1656
  decompression-memory-size  1658
  end  1659
  exit  1660
  state-memory-size  1661

CHAPTER 64  CSCF SIP Proxy Configuration Mode Commands  1663

  as-call  1664
  authentication  1665
  diversion-info  1667
  emergency  1668
  end  1670
  exit  1671
  registration  1672
  reliable-prov-resp  1674
  sifc  1675
  sigcomp  1676
  tas  1677
  tas-service  1678

CHAPTER 65  CSCF Subdomain-route List Configuration Mode Commands  1679

  after  1680
  before  1681
  end  1682
  exit  1683
  route  1684
CHAPTER 72  DHCP Server Profile Configuration Mode Commands  1733
  dhcpv6-server-preference  1734
  disable  1735
  enable  1736
  end  1738
  exit  1739
  process  1740

CHAPTER 73  DHCP Service Configuration Mode Commands  1743
  allow  1745
  bind  1747
  default  1750
  dhcp chaddr-validate  1752
  dhcp client-identifier  1754
  dhcp deadtime  1756
  dhcp detect-dead-server  1758
  dhcp ip vrf  1760
  dhcp server  1762
  dhcp server selection-algorithm  1764
  end  1766
  exit  1767
  lease-duration  1768
  lease-time  1770
  max-retransmissions  1771
  retransmission-timeout  1772
  T1-threshold  1773
  T2-threshold  1774

CHAPTER 74  DHCPv6 Client Configuration Mode Commands  1775
  end  1776
  exit  1777
max-retransmissions 1778
server-dead-time 1780
server-ipv6-address 1782
server-resurrect-time 1784

CHAPTER 75

DHCPv6 Server Configuration Mode Commands 1785
end 1786
exit 1787
ipv6 1788
preferred-lifetime 1789
prefix-delegation 1790
rebind-time 1791
renew-time 1792
valid-lifetime 1793

CHAPTER 76

DHCPv6 Service Configuration Mode Commands 1795
bind 1796
deadtime 1798
detect-dead-server 1800
dhcpv6-client 1802
dhcpv6-server 1803
deref 1804
exit 1805
server 1806

CHAPTER 77

Diameter Endpoint Configuration Mode Commands 1809
app-level-retransmission 1811
associate 1813
cea-timeout 1815
connection retry-timeout 1816
connection timeout 1817
description 1818
destination-host-avp 1819
device-watchdog-request 1821
dpa-timeout 1822
CHAPTER 78  Diameter HDD Module Configuration Mode Commands  1861

diameter-event  1862
end  1867
exit  1868
file  1869

CHAPTER 79  Diameter Failure Handling Template Configuration Mode Commands  1873

end  1874
exit  1875
msg-type  1876
CHAPTER 80  Diameter Host Select Configuration Mode Commands  1881
  end  1882
  exit  1883
  host-select row-precedence  1884
  host-select table  1887

CHAPTER 81  DNS Client Configuration Mode Commands  1889
  bind  1890
  cache algorithm  1892
  cache size  1893
  cache ttl  1894
  case-sensitive  1896
  description  1897
  end  1898
  exit  1899
  resolver  1900
  round-robin answers  1901

CHAPTER 82  DSCP Template Configuration Mode Commands  1903
  control-packet  1904
  end  1907
  exit  1908
  data-packet  1909
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.

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).

**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) #
```

**Important**

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

- a-msisd, page 7
- access-restriction-data, page 8
- accounting context, page 11
- accounting mode, page 13
- accounting stop-trigger, page 15
- allocate-ptmsi-signature, page 16
- apn-restriction, page 17
- associate, page 19
• attach access-type, page 22
• attach allow, page 26
• attach imei-query-type, page 28
• attach restrict, page 30
• authenticate activate, page 34
• authenticate all-events, page 36
• authenticate attach, page 38
• authenticate context, page 40
• authenticate detach, page 42
• authenticate on-first-vector, page 43
• authenticate rau, page 45
• authenticate service-request, page 47
• authenticate sms, page 49
• authenticate tau, page 51
• cc, page 53
• check-zone-code, page 55
• ciphering-algorithm-gprs, page 56
• csfb, page 57
• description, page 59
• diameter-result-code-mapping, page 60
• direct-tunnel, page 62
• dns-ggsn, page 64
• dns-mrme, page 65
• dns-msc, page 67
• dns-sgsn, page 69
• dns-pgw, page 70
• dns-sgw, page 71
• egtp, page 72
• eir-profile, page 74
• encryption-algorithm-lte, page 75
• encryption-algorithm-umts, page 76
• end, page 78
• epdg-s2b-gtpv2, page 79
• equivalent-plmn, page 80
• exit, page 82
• gbr-bearer-preservation-timer, page 83
• gmm Extended-T3312-timeout, page 84
• gmm information-in-messages, page 86
• gmm rau-accept, page 88
• gmm retrieve-equipment-identity, page 90
• gmm t3346, page 92
• gs-service, page 94
• gtp send, page 96
• gtpp, page 99
• gtpu fast-path, page 100
• guti, page 102
• gw-selection, page 104
• hss, page 107
• ignore-ul-data-status, page 109
• idle-mode-signaling-reduction, page 110
• integrity-algorithm-lte, page 112
• integrity-algorithm-umts, page 113
• lcs-mo, page 114
• lcs-mt, page 115
• lcs-ni, page 116
• local-cause-code-mapping apn-mismatch, page 117
• local-cause-code-mapping apn-not-subscribed, page 119
• local-cause-code-mapping apn-not-supported-in-plmn-rat, page 120
• local-cause-code-mapping auth-failure, page 122
• local-cause-code-mapping congestion, page 124
• local-cause-code-mapping ctxt-xfer-fail-mme, page 126
• local-cause-code-mapping ctxt-xfer-fail-sgsn, page 128
• local-cause-code-mapping gw-unreachable, page 130
• local-cause-code-mapping hss-unavailable, page 132
• local-cause-code-mapping map-cause-code, page 134
• local-cause-code-mapping no-active-bearers, page 136
• local-cause-code-mapping odb packet-services, page 138
• local-cause-code-mapping odb roamer-to-vplmn, page 140
• local-cause-code-mapping path-failure, page 142
• local-cause-code-mapping peer-node-unknown, page 143
• local-cause-code-mapping pgw-selection-failure, page 145
• local-cause-code-mapping restricted-zone-code, page 147
• local-cause-code-mapping sgw-selection-failure, page 149
• local-cause-code-mapping vlr-down, page 151
• local-cause-code-mapping vlr-unreachable, page 153
• location-area-list, page 155
• location-reporting, page 157
• lte-zone-code, page 159
• map, page 161
• map-service, page 164
• max-bearers-per-subscriber, page 165
• max-pdns-per-subscriber, page 166
• min-unused-auth-vectors, page 167
• mobility-protocol, page 168
• mps, page 169
• msc-fallback-disable, page 171
• network-feature-support-ie, page 173
• network-initiated-pdp-activation, page 175
• override-arp-with-ggsn-arp, page 179
• paging-priority, page 180
• pcscf-restoration, page 182
• pdp-activate access-type, page 183
• pdp-activate allow, page 185
• pdp-activate restrict, page 187
• pdn-type-override, page 189
• peer-mme, page 191
• peer-msc, page 193
• peer-nri-length, page 194
• plmn-protocol, page 196
- prefer subscription-interface, page 198
- ptmsi-reallocate, page 200
- ptmsi-signature-reallocate, page 203
- qos, page 205
- rau-inter, page 208
- rau-inter-plmn, page 212
- rau-intra, page 216
- re-authenticate, page 219
- regional-subscription-restriction, page 220
- release-access-bearer, page 223
- reporting-action, page 225
- reuse-authentication-triplets, page 226
- rfsp-override, page 227
- rfsp-override ue-settings, page 229
- s1-reset, page 231
- samog-gtpv1, page 232
- samog-s2a-gtpv2, page 234
- sctp-down, page 235
- sgs-cause-code-mapping, page 236
- sgsn-address, page 238
- sgsn-core-nw-interface, page 241
- sgsn-number, page 243
- sgtp-service, page 245
- sms-mo, page 246
- sms-mt, page 248
- srns-inter, page 250
- srns-intra, page 252
- srvcc exclude-stnsr-nanpi, page 254
- subscriber multi-device, page 255
- subscriber-control-inactivity, page 256
- super-charger, page 258
- tau, page 259
- tcp-maximum-segment-size, page 261
• timeout, page 262
• treat-as-hplmn, page 264
• vplmn-address, page 265
• zone-code, page 267
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 MSISDN (A-MSISDN) is available in the subscription data, the HSS sends the provisioned Additional-MSISDN together with the MSISDN, in 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.

Examples
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.

**Examples**

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

\texttt{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.

**Examples**

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**
```plaintext
accounting mode { gtp | none | radius-diameter }
remove accounting mode
```

- **remove**
  Removes the accounting mode.

- **gtp**
  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*.
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.

**Examples**
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.

**Examples**
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.

**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.

**Examples**

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 { accounting-policy policy_name | ho-restrict-list list_name | hss-peer-service service_name | s13-interface | s6a-interface | s13-prime-interface | s6d-interface | tai-mgmt-db tai-db_name }

remove associate { accounting-policy | ho-restrict-list | hss-peer-service | s13-interface | s6a-interface | s13-prime-interface | s6d-interface | tai-mgmt-db }

remove

Remove the specified association definition from 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.
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 | s6a-interface | 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 equipment 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.

**Examples**

Link HO restriction list named \textit{HOrestrict1} with this call control profile:

\texttt{associate ho-restrict-list HOrestrict1}

The following command associates this SaMOG call control profile with an accounting policy called \textit{acct1}:

\texttt{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 code | r99-or-later failure code 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.
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.

**Usage Guidelines**

**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.

**Examples**

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 list_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 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.

list_id: Enter an integer between 1 and 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. 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.

Examples

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**

```plaintext
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.

timei-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.

**Examples**

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

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

Configures the system to restrict attaches based on access type 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 list_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 an 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 imsi-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 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.

Important
This keyword only applies to the SGSN.

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. 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.

Examples

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 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`

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
<tr>
<td>Specifies the network access type for which the authentication process will be performed:</td>
</tr>
<tr>
<td>• gprs- Currently, not supported functionally even though it appears as a selectable option and would appear in the configuration file as configured.</td>
</tr>
<tr>
<td>• umts</td>
</tr>
</tbody>
</table>
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.

**Examples**
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.  

`frequency` must be an integer from 1 to 16.

**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.

---

**Examples**

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 ]
authenticate attach periodicity duration [ access-type { gprs | umts } ]
authenticate attach periodicity duration [ access-type { gprs | umts } ]
no
```

- **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.

*frequency* must be an integer from 1 to 16.

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.

*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).

**Examples**
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:
  
  (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 ]

**Syntax Description**
- **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-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.

Examples

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.

**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.

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

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

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

```plaintext
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

**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.

**Examples**

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 beginning authentication towards the MS:

```plaintext
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 {gprs | 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}] [frequency frequency] [periodicity duration]
```

```
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.

*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 ]

**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.

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

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

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

```plaintext
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:

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

**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. **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.
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.

Examples
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

```plaintext
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```plaintext
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.

*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

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.

Examples
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 [ frequency 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.
frequency must be an integer from 1 to 16.

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.

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

```
authenticatetau periodicity 15
```

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

```
no authenticatetau
```
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 | local-value behavior bit_value profile index_bit | prefer { hlr-hss-value | local-value } }

no cc behavior-bit no-records

remove cc { behavior-bit no-records | local-value | prefer }

no

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

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.
local-value behavior \textit{bit\_value} profile \textit{index\_bit}  

Defaults: \textit{bit\_value} = 0x0, \textit{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.  

\textit{bit\_value} is a hexadecimal value between 0x0 and 0xFFF.  

\textit{index\_bit} is an integer value from 1 through 15.  

Setting the profile index bit 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 \textbf{prefer local-value} keyword.  

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

Default: \textit{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 \textbf{local-value behavior} command.  

- \textit{hlr-hss-value} sets the call control profile to use charging characteristics settings received from HLR or HSS. This is the default preference.  
- \textit{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.  

\textbf{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 \textbf{local-value behavior} keyword) can be used to enable or disable CDR generation.  

\textbf{Examples}  

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

```bash
[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.

**Examples**

Disable checking of the zone code:

```bash
no check-zone-code
```
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.

Examples
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 { not-allowed | not-preferred | sms-only | suppress-call-reject } | 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 { not-allowed | not-preferred | sms-only | suppress-call-reject }

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.
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.

**Examples**

The following command enforces the SMS-only functionality for UEs requesting circuit-switched fallback: `csfb policy sms-only`
**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.

**Examples**

```
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
```

Removes the mapping for the specified Diameter result code.

```
remove diameter-result-code-mapping 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.

### Examples

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.

**Examples**

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 ctx_name

no
dns-ggsn context ctx_name

no

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

context ctx_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.

**Examples**

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 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.

**Examples**

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.
**Examples**

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.

**Examples**

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.

**Examples**
```
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.

**Examples**
- `dns-sgw context sgw1`
**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 }

**Syntax Description**

- **remove**
  Erases the IE choice from the callcontrol 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-GW in 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.

**Examples**

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 |

**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.

**Examples**

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

```plaintext
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-eea { 0 | 1 | 2 } priority2 128-eea { 0 | 1 | 2 } priority3 128-eea { 0 | 1 | 2 }
remove encryption-algorithm-lte
```

**remove**
Deletes the priorities definition from the call control profile configuration.

```
priority1 128-eea { 0 | 1 | 2 }
```

Enter 0, 1, or 2 at the end of 128-eea to define the algorithm being given first priority.

```
priority2 128-eea { 0 | 1 | 2 }
```

Enter 0, 1, or 2 at the end of 128-eea to define the algorithm being given second priority.

```
priority3 128-eea { 0 | 1 | 2 }
```

Enter 0, 1, or 2 at the end of 128-eea to define the algorithm being given third priority.

**Usage Guidelines**
Set the order or priority in which the MME will select a 128-EEA 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.

**Examples**
Configure 128-EEA2 as first priority encryption algorithm:

```
encryption-algorithm-lte priority1 128-eea 2 priority2 128-eea 0 priority3 128-eea 1
```
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.
Examples

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 ue-local-ip-port |

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
Configures the options to be send.

ue-local-ip-port
This is used to Send UE Local IP IE and UE UDP Port IE.

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.

Examples
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
**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 list 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.

**Examples**
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
```
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

```
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.

**Examples**
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-subscribed**

  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.

Examples

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.

Examples
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**

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

**Syntax Description**

- `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`.
Examples

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 ] [ thenimei ]

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).

  • thenimei: 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.

Examples

The following command enables the SGSN to send "check IMEI" messages to the EIR:

gmm retrieve-equipment-identity imei verify-equipment-identity
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.

Examples

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.
Examples

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

```plaintext
    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.

Examples
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.

**Examples**

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.
Examples

The following command enables the NPU fast path processing for all new subscribers' session established with this call control profile:

gtpu fast-path
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.

**Examples**

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 { pgw | sgw } ] | 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.

- **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

<table>
<thead>
<tr>
<th>Option</th>
<th>Keyword Selected</th>
<th>Prefix in Hostname</th>
<th>Topological Match Nodes Selected</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>co-location</td>
<td>topon</td>
<td>Yes</td>
<td>Co-located nodes are selected if available as they are listed before topologically closer nodes in the DNS records.</td>
</tr>
<tr>
<td>2</td>
<td>co-location</td>
<td>topoff</td>
<td>Yes</td>
<td>Co-located nodes are selected if available as they are listed before topologically closer nodes in the DNS records.</td>
</tr>
<tr>
<td>3</td>
<td>topology</td>
<td>topon</td>
<td>Yes</td>
<td>Co-located nodes are selected if available as they are listed before topologically closer nodes in the DNS records.</td>
</tr>
<tr>
<td>4</td>
<td>topology</td>
<td>topoff</td>
<td>No</td>
<td>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.</td>
</tr>
<tr>
<td>5</td>
<td>co-location</td>
<td>neither</td>
<td>Yes</td>
<td>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.</td>
</tr>
<tr>
<td>Option</td>
<td>Keyword Selected</td>
<td>Prefix in Hostname</td>
<td>Topological Match Nodes Selected</td>
<td>Comments</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
<td>--------------------</td>
<td>----------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>6</td>
<td>topology</td>
<td>neither</td>
<td>No</td>
<td>No co-located node pair listing; topologically closer node listing used if available (Same behavior as defined for (4)).</td>
</tr>
</tbody>
</table>

**Examples**

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`

`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.

**Examples**

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
```
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.

Examples
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.

**Examples**

```
idle-mode-signaling-reduction access-type umts
```
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-eia{0|1|2} priority2 128-eia{0|1|2} priority3 128-eia{0|1|2}
remove integrity-algorithm-lte
```

`remove`

Deletes the priorities definition from the call control profile configuration.

`priority1 128-eia{0|1|2}`

Enter 0, 1, or 2 at the end of `128-eia` to define the algorithm being given first priority.

`priority2 128-eia{0|1|2}`

Enter 0, 1, or 2 at the end of `128-eia` to define the algorithm being given second priority.

`priority3 128-eia{0|1|2}`

Enter 0, 1, or 2 at the end of `128-eia` to define the algorithm being given third priority.

Usage Guidelines Set the order or priority in which the MME will select an integrity 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.

Examples Configure 128-EIA0 as first priority integrity algorithm:

```
integrity-algorithm-lte priority1 128-eia0 priority2 128-eia2 priority3 128-eia1
```
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.

Examples
default integrity-algorithm-umts
**Ics-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

```plaintext
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```plaintext
Ics-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.

**Examples**

Use the following command to disable or disallow mobile-originating Location Requests within a GPRS network:

```plaintext
Ics-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.

**Examples**

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:

(llocal)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.

**Examples**

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**
remove local-cause-code-mapping apn-mismatch

remove local-cause-code-mapping apn-mismatch

Removes the configured cause code mapping.


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.

**Examples**

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.

Examples 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 out 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.

**Examples**

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**

```
```

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.

### Examples

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


remove local-cause-code-mapping congestion

Removes the configured cause code mapping.


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**

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.

**Examples**

The following command maps the "network failure" cause code to the congestion event:

```bash
local-cause-code-mapping congestion ecm-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**

```
```

```
remove local-cause-code-mapping ctxt-xfer-fail-mme
```

Removes the configured cause code mapping.

```
```

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
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 \texttt{#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 \texttt{local-cause-code-mapping} command in the mme-service configuration mode. This command is described in the \textit{MME Service Configuration Mode Commands} chapter.

**Examples**

The following command maps the "network-failure" cause code to the context transfer failure from MME condition:

\texttt{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**


remove local-cause-code-mapping ctxt-xfer-fail-sgsn

removelocal-cause-code-mapping ctxt-xfer-fail-sgsn

Removes the configured cause code mapping.


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
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.

**Examples**

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

```plaintext
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```plaintext
```

Removes the configured cause code mapping.

```plaintext
remove local-cause-code-mapping gw-unreachable [ attach | tau ]
```

```plaintext
```

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
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.

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.

**Examples**
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**

- `remove local-cause-code-mapping hss-unavailable`

Removes the configured cause code mapping.


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`

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.

**Examples**

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.

Examples
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
command 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 local-cause-code-mapping no-active-bearers

Removes the configured cause code mapping.


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
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.

**Examples**

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`

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.
Examples

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

roamer-to-vplmn emm-cause-code cc_value [ esm-cause-code cc_value ]
```

Removes the configured cause code mapping.

```
remove local-cause-code-mapping odb roamer-to-vplmn
```

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.
Examples

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

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.

**Examples**

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**


remove local-cause-code-mapping peer-node-unknown

removes the configured cause code mapping.


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
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.

**Examples**

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

```bash
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```bash
```

```bash
remove local-cause-code-mapping pgw-selection-failure
```

Removes the configured cause code mapping.

```bash
```

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
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.

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.

**Examples**

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
```
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

Removes the configured cause code mapping.

```
remove local-cause-code-mapping restricted-zone-code
```

```
local-cause-code-mapping restricted-zone-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**
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.

**Examples**

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**  

remove local-cause-code-mapping sgw-selection-failure

Removes the configured cause code mapping.

sgw-selection-failure **emm-cause-code**  

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
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.

**Examples**

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
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.

**Examples**

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
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.

**Examples**

The following command maps the "network failure" EMM cause code to the VLR unreachable condition:

```bash
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 list.
Examples

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).

**Examples**
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
```

- **lte-zone-code**
  - allows or restricts the zone code list.
  - **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**
    - the list of zone codes.
  - **zc_id**
    - an identifier for the 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.

```
```

- 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.

**Examples**
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
```
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.

**Examples**
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.

Examples
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.

**Usage Guidelines**
Use this command to set the maximum number of bearers allowed per subscriber.

**Examples**
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.

Examples
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 initiation of a service area identity request (SAI).
  
  **min#_vectors**: Enter a digit between 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.

**Examples**
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
```
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.

**Examples**  
The following command configures mobility protocol to GTPv2:  
mobility-protocol GTPv2
**mps**

This command under the Call Control profile configuration mode is configured to support Multimedia Priority Service (MPS) in the CS 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 { 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.

subscribed

The keyword `subscribed` configures support for priority service in the CS domain.

none

The keyword `none` configures disables support for priority service in the CS 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.
Examples

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
```
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'.
**Examples**

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`
**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
c

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 |
remove network-feature-support-ie

**Syntax Description**

`network-feature-support-ie` `ims-voice-over-ps` | `not-supported` | `supported` |
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.

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.

**Examples**

The following command enables support for IMS Voice over PS on the MME:

```plaintext
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 sctp statistics verbose output.
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`
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.

**Examples**

Use this command to configure the SGSN to negotiate the ARP to be used as an overriding value:

```
override-arp-with-ggsn-arp
```
This command is configured to support sending of paging-priority value in S1AP paging-request message to the eNodeB.

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 |

remove
The remove keyword deletes the configured value of paging-priority to be sent to eNodeB for CS paging.

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.

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.

Examples
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.

Examples
The following configurations enables HSS-based P-CSCF Restoration:

pcscf-restoration
pdp-activate access-type

Configures the PDP context activation option 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**

```
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.

- **grps**: 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.

**Examples**

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.
    - **grps**: 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.
Examples

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 { gprs | 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.
pdp-activate restrict

- **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.

**Examples**
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 ipv4v6 { ipv4 | ipv6 } { access-type { eps | grps | umts } } remove pdn-type-override { access-type { eps | grps | umts } } remove
```

- `remove`
  - Removes the configured PDN type override.

- `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.

**Examples**

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.

**Examples**

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 1.1.1.1 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

```plaintext
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```plaintext
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.

**Examples**
Disable weight-based MSC selection when it has been configured:

```plaintext
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
DeletestheNRIlengthconfigurationforthenon-localRAIsandtheSGSNsendsnrai-FQDN-basedDNSSolution.

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 RAI s 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.

Examples

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 mnc mnc_num {s5-protocol | s8-protocol} {gtp | pmip}
remove plmn-protocol plmnid mcc mnc mnc_num

remove
Deletes the definition from the call control profile configuration.

plmn-id mcc 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.
Examples

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.

Examples

The following command specifies that "hss" for S6d is selected as the subscription-interface:

```
prefer subscription-interface hss
```
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 | 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 | no | remove | 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 one 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.

**Examples**

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.

Examples
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 update-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**
```
quos { gn-gp | ue-ambr }
quos 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 } }
quos ue-ambr { max-ul mbr_up max-dl mbr_dl | prefer-as-cap { both-hss-and-local minimum | local } }
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 (Release 16.1 and higher), or 0 to 1410065408.

- max-dl mbr-down: Defines the maximum bit rate for downlink traffic.
  
mbr-down: Enter a value from 1 to 1410065408 (Release 16.1 and higher), or 0 to 1410065408.


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**

Usage 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.

**Examples**

Configure the Gn/Gp interface ARP priority values:

```bash
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 } { 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 | 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 } }

default rau-inter ( accept use-auth-vector | access-type { { gprs | umts } { all | location-area-list instance instance } user-device-release { before-r99 | r99-or-later } failure-code fail_code } )

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 Request (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**

`list_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.

**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.

Examples
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

**Examples**

```
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 } { 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 } user-device-release { before-r99 failure-code | r99-or-later failure-code }
- `rau-intra { allow access-type | restrict access-type } { all | location-area-list instance instance }
- `no rau-intra { allow access-type | restrict access-type } { all | location-area-list instance instance }
- `default rau-intra { allow access-type | restrict access-type } { all | location-area-list instance instance }`  

- `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 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**
*list_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 via 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 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.

Examples

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.

**Examples**

`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

```bash
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.
Examples

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.

Important We recommend that Release Access Bearer be enabled (with this command) prior to enabling Subscriber Overcharging 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.

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 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.

Examples

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

```config
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 mme-event-record
```

**remove**

This command disables the reporting action configuration.

**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 parameters can also be configured 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.

**Examples**
The following configuration enables Event Logging in the MME:

```config
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.

**Examples**
```
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
command > 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.

**Examples**

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**

```plaintext
```

**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.

**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.

**Examples**
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
```
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.

**Examples**

Configure the MME to put the UE into idle-mode upon receipt of S1-reset:

```
s1-reset idle-mode-entry
```
**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 [ 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.

  **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 0xFFFF. 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.
Examples

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 [ filler filler_value ]
no samog-s2a-gtpv2 send imeisv

no
Disables a previously enabled configuration.

imeisv value ue-mac [ filler filler_value ]
Specifies to forward the UE Identity in the IMEIsV IE value. By default this configuration is disabled.
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.

Usage Guidelines
Use this command to enable SaMOG to forward:
• The User Equipment's (UE) Identity information over the GTPv2 interface in hexa-decimal format

Examples
Configure SaMOG to forward the UE identity with a padding value of 0xFEFE:
samog-s2a-gtpv2 send imeisv value ue-mac filler 0xFEFE
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.

Examples
Configure the MME to put the UE into idle-mode when the SCTP layer goes down:

sctp-down idle-mode-entry
**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 sgss-cause emm-cause-code emm_cause_code`
remove sgs-cause-code-mapping sgss-cause

remove sgs-cause-code-mapping sgss-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 interface 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.

**Examples**

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
call-control-profile configuration- 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.

Examples

Create a local peer-SGSN address mapping of an RAI with RAC of 123 and LAC of 4444 and an IPv4 address of 123.11.313.11 for the peer-SGSN:

```
sgsn-address rac 123 lac 4444 local address ipv4 123.11.313.11
```
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 with 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:

<table>
<thead>
<tr>
<th>Interface</th>
<th>sgsn-core-nw-interface gn</th>
<th>sgsn-core-nw-interface s4</th>
</tr>
</thead>
<tbody>
<tr>
<td>GTPv1 protocol</td>
<td>Proceed with call</td>
<td>Proceed with call</td>
</tr>
<tr>
<td>GTPv2 protocol</td>
<td>RAU fall back to GTPv1 and proceed with call</td>
<td>Proceed with call</td>
</tr>
</tbody>
</table>

**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.

---

**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.

**Examples**

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.
Examples

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.

**Examples**

```
sgtp-service context sgtp1 service sgtp-srvc1
```
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.

Examples
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.

Examples
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 location-area-list instance instance | location-area-list instance instance failure-code code | restrict location-area-list instance instance }
no srns-inter { all | location-area-list-instance instance | allow location-area-list instance instance | restrict location-area-list instance instance }
default srns-inter { all | location-area-list-instance instance } 
```

**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**
Identify the location area list Id (LAC Id) that will allow services in the defined location area.

**location-area-list instance instance**

`instance`: Must be an integer between 1 and 5 that identifies the previously defined location area list created with the `location-area-list` command.
restrict location-area-list instance instance

Identify the location area list Id (LAC Id) that indicates the location areas where services will be restricted.

Usage Guidelines
This command defines the operational parameters for inter-SRNS relocation.

Examples
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 location-area-list instance instance | location-area-list instance instance failure-code code | restrict location-area-list instance instance )

no srns-intra { all | location-area-list-instance instance }

default srns-intra { all | location-area-list-instance instance }

**no**

Deletes the intra-SRNS relocation configuration.

**default**

 Resets the configuration to default values.

**all failure-code code**

Define the failure code that will apply to all intra-SRNS relocations.

*code*: Must be an integer from 2 to 111.

**allow location-area-list instance instance**

Identify the location area list Id (LAC Id) that will allow services in the defined location area.

**location-area-list instance instance**

*instance*: Must be an integer between 1 and 5 that identifies the previously defined location area list created with the **location-area-list** command.
restrict location-area-list instance instance

Identify the location area list Id (LAC Id) of the target RNC to determine the location areas where services will be restricted.

Usage Guidelines

This command defines the operational parameters for intra-SRNS relocation.

Examples

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.
**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.

**Examples**

The following command enables multiple 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.
```

**detach**
```
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](image)

  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.

**Examples**

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:

```plaintext
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.

Examples  The following command enables the super charger feature:

    super-charger
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 security-ctxt { allow-mapped | native } }

remove tau { imei-query-type | inter-rat security-ctxt }

remove

Deletes this TAU configuration from the call control profile.

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 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.

**Examples**

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.

**Examples**
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

**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.
Examples

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

**Usage Guidelines**
Use this command to enable or disable the SGSN to treat an IMSI series as coming from the home PLMN.

**Examples**
The following command disables previously configured feature:

remove treat-as-hplmn
vplmn-address

Enables/disables the SGSN to override the VPLMN address-allowed flag.

**Product**  
SGSN

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration > Call Control Profile Configuration

```plaintext
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**

```plaintext
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 to set the VPLMN-Address-Allowed flag during GGSN selection - even if the flag was not received in the subscription data from the HLR.

**not-allowed**

Using **not-allowed** instructs the SGSN not to set the VPLMN-Address-Allowed flag during GGSN selection - even if the flag is received in the subscription data from the HLR.

**Usage Guidelines**

Use this command to override the VPLMN-Address-Allowed flag received in subscription data from HLR during GGSN 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. This override enables the operator to control selection of a different GGSN for a roaming subscriber by using/not-using VPLMN-OI in full-APN.
Examples

The following command instructs the SGSN to set the VPLMN-Address-Allowed flag during GGSN selection, even if the flag was not received in subscription data from the HLR:

`vplmn-address allowed`

The following command instructs the SGSN not to set the VPLMN-Address-Allowed flag during GGSN selection, even if the flag was received in subscription data from the HLR:

`vplmn-address not-allowed`

The following command instructs the SGSN not to override standard behavior regarding the VPLMN-Address-Allowed flag:

`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. A maximum of 10 zone code lists can be configured per Call Control Profile.

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 command with this parameter to include up to 100 LACs in the zone code list.

Usage Guidelines

Important

While there is no limit to the number of zone codes that can be created, only 10 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.

**Examples**

The following command defines multiple LACs for zone code 1:

```
zone-code 1 lac 413 212 113
```
Call-Home Configuration Mode

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.

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) #

Important

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

- activate, page 271
- alert-group, page 272
- contact-email-addr, page 274
- contract-id, page 275
- customer-id, page 276
- end, page 277
- exit, page 278
- mail-server, page 279
- phone-number, page 280
- profile, page 281
- rate-limit, page 282
- sender, page 283
- site-id, page 285
- street-address, page 286
**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.

**Examples**

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**

\[
\text{default} | \text{no} | \text{alert-group} \ { \text{all} | \text{configuration} | \text{crashinfo} | \text{diagnostic} | \text{environment} | \text{inventory} | \text{syslog} }
\]

**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.

Examples
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.

Examples
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.

**Examples**  
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.

**Examples**

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.

<table>
<thead>
<tr>
<th><strong>Product</strong></th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Privilege</strong></td>
<td>Security Administrator, Administrator</td>
</tr>
</tbody>
</table>

**Syntax Description**

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.

**Examples**

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.

**Examples**

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.

Examples

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.

Examples

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**

```plaintext
| 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.
Examples

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.

**Examples**

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 the 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.

Examples
The following command sets the street address to 123 Main St., Chicago, IL 60000:
street-address "123 Main St., Chicago, IL 60000"
Call-Home Profile Configuration Mode

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.

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) #

Important

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

- active, page 288
- destination, page 289
- end, page 291
- exit, page 292
- subscribe-to-alert-group, page 293
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.

Examples

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**

```
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 format 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.

Examples
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 | disaster | fatal | critical | major | minor | warning | notification | normal]} | configuration {periodic [daily | monthly | weekly]} | crashinfo | diagnostic {severity [catastrophic | disaster | fatal | critical | major | minor | warning | notification | normal]} | environment {severity [catastrophic | disaster | fatal | critical | major | minor | warning | notification | normal]} | inventory {periodic [daily | monthly | weekly]} | syslog {severity [catastrophic | disaster | fatal | critical | major | minor | warning | notification | normal | pattern pattern_to_match]}

default subscribe-to-alert-group

no subscribe-to-alert-group | all {severity [catastrophic | disaster | fatal | critical | major | minor | warning | notification | normal]} | configuration {periodic [daily | monthly | weekly]} | crashinfo | diagnostic {severity [catastrophic | disaster | fatal | critical | major | minor | warning | notification | normal]} | environment {severity [catastrophic | disaster | fatal | critical | major | minor | warning | notification | normal]} | inventory {periodic [daily | monthly | weekly]} | syslog {severity [catastrophic | disaster | fatal | critical | major | minor | warning | notification | normal | pattern pattern_to_match]}
```

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 | disaster | 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 | disaster | 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 | disaster | 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.
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.

**Examples**

The following command sets an alert group for the profile to send a daily inventory message:

```
subscribe-to-alert-group inventory periodic daily
```
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).

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.

**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)#
```

*Important*

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

- `associate-sccp-network`, page 298
- `end`, page 299
- `exit`, page 300
- `tcap destination-address`, page 301
- `timeout`, page 302
**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.

**Usage Guidelines**

The SCCP network must be configured prior to use this command.

CAMEL service will not function unless an SCCP network is associated.

**Examples**

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.

Examples
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

 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.

Examples
Set the tc-guard timer for 4:
tc-guard-timer 4
timeout
Card Configuration Mode Commands

Use the Card configuration mode to create and manage the physical cards in the chassis.

**Command Modes**

Exec > Global Configuration > Card Configuration

```bash
configure > card card_number
```

Entering the above command sequence results in the following prompt:

```bash
[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).

- aps, page 306
- end, page 308
- exit, page 309
- framing, page 310
- header-type, page 312
- initial-e1-framing, page 313
- link-aggregation, page 314
- mode, page 316
- redundancy, page 318
- redundant with, page 321
- service-type, page 322
- shutdown, page 324
aps

Configures the parameters for the automatic protection switching (APS) feature for SONET CLC2 and OLC2 line cards or for multiplexed section (or switching) protection (MSP) type APS for SDH CLC2 and OLC2 line cards. (ASR 5000 only)

Important
This command should only be used after APS has been enabled with the `aps-mode` keyword of the command.

Product
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
`aps [ 1+1 | [ uni-directional ] | [ non-revertive ] | -noconfirm ]`

`no aps`

`default aps`

`1+1`

Selects 1+1 line (linear) protection. Traffic is carried simultaneously by the working line and the protection line. GR-253 and ITU-T G.783 require the bridging to be done at the electrical level; therefore, the same payloads are transmitted over the working and protection lines.

`no`

This keyword has been deprecated for releases 14.0 and higher To disable APS, enter `redundancy port-mode` in this command mode.

For releases prior to 14.0, this keyword disables APS.

`default`

This option is equivalent to: `aps 1+1 uni-directional non-revertive`. This option is only available in releases 14.0 and higher.
uni-directional
Enables protection on one end of the connection.

non-revertive
Prevents the network from automatically reverting to the original working line/port when the original working line/port is recovered/restored.

-noconfirm
Executes the command without additional prompting for command confirmation.

Usage Guidelines

Important
At this time, it is not necessary to use the `aps` command to configure parameters as all of these parameters are enabled by default when the APS feature is enabled with the `aps-mode` keyword of the command.

Use this command to configure feature parameters for the APS function for SONET CLC2 and OLC2 line cards or to configure MSP-type APS for SDH CLC2 and OLC2 line cards. Based on the card framing configuration (SONET or SDH), the system automatically knows whether the feature is APS or MSP.

Examples

As all parameters are included by default it is only necessary to enter the command:

`aps`
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

dead

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.
framing

Configures the type of framing to be used for the signaling generated on a specific line card. (ASR 5000 only)

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

framing { ethernet | sdh[ds1 | e1 | ss-bits] | sonet[ds1 | e1 | unspecified] } -noconfirm

default framing -noconfirm

default

Resets the framing generated by the card to the default for the particular card type.

ethernet

Configures the system to use Ethernet framing for this line card. This type of framing can only be used on an Ethernet card.

Default: Ethernet framing type is the default for an Ethernet line card.

Important

Using this keyword with an OLC/OLC2 or CLC/CLC2 takes the card offline.

sdh | ds1 | e1 | ss-bits

Configures the system to use SDH signal framing for either an OLC/OLC2 or CLC/CLC2 line card in an SGSN.

Important

Using this keyword with an Ethernet line card takes the line card offline.

In releases 8.1 and higher, you can also set the type of signaling path for a CLC2.

ds1 - configures the card to support a DS1/T1.
**framing**

e1 - configures the card to support an E1. This is the default for SDH.

ss-bits - enables/disables use of ss-bits (per ITU 1997 G.783 specification) for SDH configured line card.

sonet \[ ds1 \mid e1 \]

Configures the system to use SONET signal framing for either an OLC/OLC2 or CLC/CLC2 line card in an SGSN.
Default: SONET is the default framing type for an OLC/OLC2 or CLC/CLC2 line card.

Important
Using this keyword with an Ethernet line card takes the line card offline.

In releases 8.1 and higher, you can also set the type of signaling path for a CLC2.

ds1 - configures the card to support a DS1/T. This is the default for SONET.
e1 - configures the card to support an E1.

unspecified

Configures the system to use the default framing type for the particular line card resident in the identified slot.

-noconfirm

Instructs the system to execute the command without additional prompting for command confirmation.

**Usage Guidelines**

Use the framing command to identify the type of signal framing to be used by the line card in the identified slot.

Note that each type of line card uses a different type of signal framing. If you configure the wrong framing type for a line card, the line card is taken offline.

Important
This command is not supported on all platforms.

**Examples**

Use the following command to configure SDH signal framing on a CLC2. If you do not include the path-type, the default of e1 is automatically included in the card's framing configuration:

framing sdh
**header-type**

Defines the size of the header frame for Frame Relay transmissions over a CLC or CLC2 channelized line card. (ASR 5000 only)

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Card Configuration

```plaintext
configure > card card_number
```

Entering the above command sequence results in the following prompt:

```plaintext
[local]host_name(config-card- slot_number)#
```

**Syntax Description**

```plaintext
header-type header_size | -noconfirm |
default header-type | -noconfirm |
```

- **default**
  
  Resets the configuration to the default header size of 2-bytes.

- **header_size**
  
  Sets the size for the header frame. `header_size` must be either 2-bytes or 4-bytes.

- **-noconfirm**
  
  Executes the command without additional prompting for command confirmation.

**Usage Guidelines**

Use this command to set the size of the header frame for Frame Relay messages emanating from the line card. The size (2-bytes or 4-bytes) determines the amount of information that can be transmitted in that first information frame.

- **Important**
  
  Not supported on all platforms

**Examples**

Set the header to the smallest size.

```plaintext
header-type 2-byte
```
**initial-e1-framing**

Configures the type of framing mode that will initially be available at the time the line card boots. (ASR 5000 only)

**Product**

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**

```
initial-e1-framing [ crc4 | standard ]
```

**default initial-e1-framing**

`default`

Returns the configuration to CRC4 as the default type.

`crc4`

Accepts the default CRC4, in the configuration, as the initial at-boot framing mode.

`standard`

Accepts the `standard` mode as the initialization framing mode.

**Usage Guidelines**

For a CLC-type line card, the default E1 framing mode is CRC4. When a card reboots, all E1s are initialized with CRC4 framing mode and then switch to the configured framing mode. With this keyword, you have the option to choose the initialization framing mode.

**Important**

Only supported on CLC/CLC2

**Examples**

```
initial-e1-framing standard
```
**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

```plaintext
configure > card card_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-card- slot_number)#
```

**Syntax Description**

```plaintext
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 5000 QGLCs or XGLCs, or 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

---

Examples

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.
Switching an active packet processing card to standby deletes all port configurations, including bindings, for the attached line cards.

**Caution**

Switching an active packet processing card to standby deletes all port configurations, including bindings, for the attached line cards.

-nofirm

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.

**Examples**

The following commands set the state of a card to active and standby, respectively.

mode active
mode standby
redundancy

Configures the type of redundancy for a line card or SPIO. (ASR 5000 only)

**Product**
- PDSN
- FA
- HA
- GGSN
- SSGN

**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**
- `redundancy {aps-mode | card-mode | port-mode} [-noconfirm]`
- `default redundancy [-noconfirm]`

**`default`**
Restores redundancy to **port-mode** type redundancy.

**`aps-mode`**

---

**Important**
This keyword works with SGSN only.

Enables automatic protection switching (APS), if the card is either a CLC2 or an OLC2 line card with card framing set to SONET. (Refer to the `framing` command.)

Enables multiplexed section (or switching) protection (MSP) type APS, if the card is a CLC2 line card with card framing set to SDH. (Refer to the `framing` command.)

---

**Important**
Using this keyword with any card type other than a CLC2 or an OLC2 will take the card offline.
Related parameters: You should consider setting appropriate SDSF BER (signal degrade/signal failure bit error rate) threshold settings. Access the hopath-sdfsl, lopath-sdfsl, and toh-sdfsl commands via the port channelized configuration mode -- for a CLC2 line card refer to the Channelized Port Configuration Mode Commands chapter and for an OLC2 line card refer to the ATM Port Configuration Mode Commands chapter.

**card-mode**

Specifies no port redundancy is used. This is used mostly for legacy products.

**Important**

This keyword has been deprecated beginning with Release 14.0.

**port-mode**

Enables port redundancy on line cards or on SPIO cards.

This is the default setting used by the system.

**Important**

Port-type redundancy does not affect line card failover/redundancy operations.

**pseudo-aps-mode**

This keyword has been deprecated.

**-noconfirm**

Instructs the system to execute the command without additional prompting for command confirmation.

**Usage Guidelines**

Use this command to configure redundancy on a line card (LC) or a SPIO card. With **port-mode** enabled, if an external network device or cable failure occurs that causes a link down failure on the port, the redundant port is used.

**Important**

Not supported on all platforms

**Important**

You do not need to enter this command for each line card or SPIO card, as the system intuitively understands that if the command is entered for an active line card or SPIO card, the standby line card or SPIO card switches to operate in the same mode. For example, if you enter the **port-mode** command for an LC in slot 17, you automatically enable a redundant line card in slot 33 for port redundant operation.

**Important**

**asp-mode** and **port-mode** are mutually exclusive.
Examples

The following command sets the redundancy mode to port redundancy.

`redundancy port-mode`

The following sets APS/MSP 1+1 inter-card redundancy for the specified OLC2 or CLC2 line card:

`redundancy aps-mode`
redundant with

Enables side-by-side (SBS) redundancy for XGLCs. (ASR 5000 only)

<table>
<thead>
<tr>
<th>Product</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
</tbody>
</table>
| 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 | `redundant with card_number`  
  `card_number`  
  Identifies the neighboring top slot number of the card to pair with the XGLC being configured. `card_number` is an integer between 1 and 48. |
| Important | Attempting to use this command with any card other than an XGLC takes the card offline. |
| Usage Guidelines | Use this command during configuration to identify the slot holding the XGLC card that will be used to provide redundancy to the XGLC you are configuring. Entering this command enables SBS redundancy when the two XGLCs occupy two upper (top) slots in a chassis. |
| Examples   | Pair the card in slot 30 with the card being configured:  
  `redundant with 30` |
service-type

Configures the type of service that the CLC or CLC2 line card will support. (ASR 5000 only)

Important

Supported in software releases 8.1 and higher.

Product

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

service-type { frame-relay | mtp2 | multi-service | pwe3-cesopsn | unspecified } [ -noconfirm ]

default service-type [ -noconfirm ]

default

Returns the card configuration to unspecified.

frame-relay

Configures the card to operate in Frame Relay service mode.

mtp2

Important

MTP2 functionality is not yet supported.

Enables MTP2 type service to support narrowband transmissions.

multi-service

Enables path-level service for multiple simultaneous services (such as frame-relay and mtp2) to run over a single port. For additional information, see the Channelized Port Configuration Mode Commands chapter
pwe3-cesopsn

**Important**  
pwe3-cesopsn functionality has been replaced by **mtp2**.

`unspecified`

This is the default mode for a CLC or CLC2.

**Important**  
You must configure the line card to one of the available service types or the card will not function.

`-noconfirm`

Executes the command without additional prompting for user input.

**Usage Guidelines**

Use this command to configure the operational service mode for the channelized line card (CLC or CLC2). Once you select the service-type, refer to the *Channelized Port Configuration Mode Commands* chapter to review the commands needed to configure the parameters for the port.

**Examples**

`service-type frame-relay`
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

Shutdown 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

Examples

The following command shuts down the card:

shutdown

The following command switches the card to online:

no shutdown
CBS Service Configuration Mode Commands

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, page 326`
- `cbc-address-validation, page 327`
- `cbc-server, page 328`
- `end, page 330`
- `exit, page 331`
- `sabp timer, page 332`
- `sabp-class2-aggregation, page 333`
- `tcp-keepalive, page 334`
- `tcp-mode, page 335`
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 protocol (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.

Examples

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.

**Examples**

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:

\(\{\text{context\_name}\}\text{host\_name}\) (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.

*ipv4_address*

Specifies the IPv4 type IP address of CBC server. *ipv_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 protocol (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.
Examples

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 previously 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.

**Examples**

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 previously 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.

**Examples**
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.

Examples

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 command 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.

**Examples**

The following command configures the HNBGW as Client and Server.

```
tcp-mode client-server
```
CGW Service Configuration Mode Commands

Creates Convergence Gateway (CGW) service and enters CGW service configuration mode.

**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)#
```

**Important**

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

- associate, page 338
- bind, page 341
- enable-bra-failure-handling, page 343
- end, page 344
- exit, page 345
- gre sequence-numbers, page 346
- reg-lifetime, page 347
- revocation, page 348
- session-delete-delay, page 350
- timestamp-option-validation, page 351
- timestamp-replay-protection, page 352
**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}
oassociate {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.
- `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.

Examples

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

```plaintext
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 | 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.
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.

**Important**

*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.

**Examples**

The following command binds an IPv4 address for lma driver.

```
bind ipv4-address 192.130.30.14
```
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.

Examples
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.

Examples

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.
Examples

The following command configures the retransmission timeout to 1000 milliseconds.

`
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 delete delay to its default value, disabled. Default timeout when enabled is 10000 msecs.

- **no**
  Enables / disables session delete 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.

**Examples**
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

Configures 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.

Examples

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.

**timeout-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.

**Examples**

The following command designates timestamp replay protection for 500 seconds.

```
timestamp-replay-protection  tolerance 500
```
Channelized Port Configuration Mode Commands

The commands described in this chapter only run on the ASR 5000 platform. Before using these commands, card framing should be configured for either SDH or SONET with the framing command described in the Card Configuration Mode chapter.

The channelized port configuration mode provides the commands to create, configure, bind, and manage the Frame Relay service ports on the channelized line card.

**Command Modes**

Exec > Global Configuration > Channelized Port Configuration

configure > port channelized *slot_number/port_number*

Entering the above command sequence results in the following prompt:

[local] *host_name*(config-port-*slot_number/port_number*) #

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

- alarm-disable, page 355
- alarm-soak-timer, page 357
- clock-source, page 358
- description, page 359
- dli, page 360
- end, page 362
- exit, page 363
- frame-relay, page 364
- hopath-sdsf, page 366
- line-timing, page 367
- loopback, page 368
- lopath-sdsf, page 369
- path, page 370
- preferred slot, page 374
- pwe3-cesopsn, page 375
- shutdown, page 376
- snmp trap link-status, page 377
- threshold high-activity, page 378
- threshold monitoring, page 380
- threshold rx-utilization, page 382
- threshold tx-utilization, page 384
- toh-sdsf, page 386
- vc-mapping, page 387
alarm-disable

Entering this command disables the alarm detection for designated sets of alarms.

Product | SGSN

Privilege | Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Channelized Port Configuration

configure > port channelized slot_number/port_number

Entering the above command sequence results in the following prompt:

[local] host_name(config-port-slot_number/port_number)#

Syntax Description

alarm-disable { all | ds1-e1 | none | sonet-sdh }
| no | default | alarm-disable

no
Deletesthedisableconfiguration.

default
Returns the settings for disabling alarms to the system default.

all
DisablesdetectionofallSONET/SDHandDS1/E1alarms.

ds1-e1
DisablesdetectionoftheDS1/E1alarms.

none
NoneofthealarmdetectionisdisabledsosethatallDS1/E1andSONET/SDHalarmsaredetected.

sonet-sdh
DisablesdetectionofSONE/SDHalarms.

Usage Guidelines

Configure selected alarm detection for the port.
Examples

Enter the following command to enable DS1/E1 and SONET/SDH alarm detection.

```
alarm-disable none
```
alarm-soak-timer

This command sets the timer for the duration that a detected alarm will be soaked before the alarm is reported.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Channelized Port Configuration

`configure > port channelized slot_number/port_number`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-port-slot_number/port_number)#
```

**Syntax Description**

```
alarm-soak-timer seconds
default alarm-soak-timer
```

**default**
Returns the timer settings to the system default.

**seconds**
Defines the number of seconds the system waits (soaks the alarm) before reporting the alarm.

*seconds*: any integer from 0 to 32767.

**Usage Guidelines**
Configures the delay before reporting detected alarms.

**Examples**
Configure a 20 second alarm report delay.
```
alarm-soak-timer 20
```
clock-source

This command sets the source of the port's transmit clock.

---

**Important**

This command is only available for releases 8.1 or higher.

---

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Channelized Port Configuration

configure > port channelized *slot_number/port_number*

Entering the above command sequence results in the following prompt:

[local] *host_name*(config-port-*slot_number/port_number*) #

**Syntax Description**

`clock-source { internal-timing | loop-timing }

default clock-source`

**default**

Using this command combination sets the port clock source to internal timing.

**internal-timing**

Sets the port clock to derive timing from the recovered receive clock.

**loop-timing**

Sets the port clock to transmit in sync with the system timing.

**Usage Guidelines**

Use this command for either SONET or SDH channelized (Frame Relay) ports on the SGSN.

**Examples**

The following command resets the transmit clock source to internal timing.

*default clock-source*
description

Defines descriptive text that provides useful information about the port.

**Product**  
SGSN

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration > Channelized Port Configuration  
`configure > port channelized slot_number/port_number`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax Description**

- `description text`
- `no description`

- `no`
  Erases the port's description from the configuration file.

- `text`
  `text` must be a string of 1 to 79 alphanumeric characters with no spaces or a string within double quotes that includes printable characters. The description is case-sensitive.

**Usage Guidelines**  
Set the description to provide helpful information, for example the port's primary function, services, end users. Define any information, the only limit is the number of characters.

**Examples**

- `description samplePortDescriptiveText`
- `description "This is a sample description"`
dlci

Identifies a data link connection identifier (DLCI), a frame relay logical connection, and binds it with a specific channelized path configuration. Once the DLCI is bound to the path, the system enters DLCI configuration mode.

Important
The path command must be configured prior to attempting configuration with the dlci command.

Syntax Description

dlci path path_id { ds1 | e1 } connects { dlci dlci_id | timeslots slot# dlci dlci_id }
no dlci path path_id { ds1 | e1 } connects

no
Disables the configured DLCI.

path path_id
Identifies a specific path configuration, set with the path command in this configuration mode, that will be associated with a DLCI.

path_id must be an integer from 1 to 3.

ds1 connects | e1 connects
Selects the framing speed for the connection.

DS1: Is associated with North American networks and would be the best choice to work with the SONET framing selected with the card configuration command.

connects: Defines the number of logical connections supported via the DS1. The selection must be an integer from 1 to 28.
E1: is associated with European networks and would be associated with the SDH framing selected with the `card` configuration command.

`connects`: Defines the number of logical connections supported via the E1. The selection must be an integer from 1 to 21.

```plaintext
dlci dlci_id
```

Identifies a specific Frame Relay PVC DLCI to associate with the path.

`dlci_id`: an integer from 16 to 991.

```plaintext	imeslot slot#
```

Identifies one of the timeslots within a timeslot group configured with the `path` command for the E1, DS1 or fractional E1 port. Identifying one slot in a group means that all the slots in that group will have the Frame Relay parameters configured in the same manner.

`slot#`: Must be an integer from 1 to 31.

**Usage Guidelines**

Associating a routing path with a specific frame relay DLCI is a significant part of the process for defining the frame relay interface.

**Examples**

Associate path 1 with DLCI 123.

```plaintext
dlci path / ds1 21 dlci 123
```
end

Ends the Channelized Port configuration mode and returns to the Exec mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax Description**
end

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

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax Description**
exit

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

Configures the parameters for the Frame Relay connections for E1, DS1 and fractional E1 ports created with the path command. Frame

Important

The path command must be configured prior to attempting configuration with the frame-relay command.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax Description

frame-relay path path_id { ds1 connects | e1 connects } timeslot slot# [ intf-type intf_type ] [ lmi_type

path path_id

Identifies a specific path configuration, set with the path command in this configuration model.

path_id must be an integer from 1 to 3.

ds1 connects | e1 connects

Selects the pipe splitting for the connection.

DS1: Is associated with North American networks and would be the best choice to work with the SONET framing selected with the card configuration command. DS1 splits the path into 28 logical connections.

connects: Defines the number of logical connections supported via the DS1. The selection must be an integer from 1 to 28.

E1: is associated with European networks and would be associated with the SDH framing selected with the card configuration command. E1 splits the path into 21 logical connections.

connects: Defines the number of logical connections supported via the E1. The selection must be an integer from 1 to 21.

timeslot slot#

Identifies one of the timeslots within a timeslot group configured with the path command for the E1, DS1 or fractional E1 port. Identifying one slot in a group means that all the slots in that group will have the Frame Relay parameters configured in the same manner.

slot#: Must be an integer from 1 to 31.
intf-type  *inf_type*

Selecting the interface type specifies signaling parameters for the DLCI, options include:

- **dce**: Selects data circuit-terminating equipment -type signaling.
- **dte**: Selects data terminal equipment -type signaling.
- **nni**: Selects the network-to-network interface

Default: DTE for Release 8.0
Default: DCE for Release 8.1

frame-relay lmi_type  *lmi_type*

Default: none.

Line management options include:

- **ansi** - ANSI ANNEXED LMI, may include option:
- **cisco** - Cisco/Gang Of Four LMI
- **none** - LMI Disabled
- **q933a** - Q.933A LMI

Any of the above LMI types can take one or more additional options

- **n391 value** - Number of keep exchanges before requesting a full status message. Default is 6. value must be an integer from 1 to 255.
- **n392 value** - Error Threshold value. Default is 2. value must be an integer from 1 to 10.
- **n393 value** - Monitored events count value. Default is 2. value must be an integer from 1 to 10.
- **t391 value** - Timer to send messages. Default is 10. value must be an integer from 5 to 30.
- **t392 value** - Polling verification timer value. Default is 15. value must be an integer from 5 to 30.

Usage Guidelines

Use this command to define LMI type and timers and to associate time group 2 with the Frame Relay connection.

Examples

```
frame-relay path le1 3 timeslot 2
```
**hopath-sdsf**

Configures the high-order path for degrade/signal failure (SDSF) bit error rate (BER) thresholds.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax Description**

```
hopath-sdsf hopath_value
```

- **hopath_value**
  - 0: Disabled
  - 1 - 1.E-03
  - 2 - 1.E-04
  - 3 - 1.E-05
  - 4 - 1.E-06
  - 5 - 1.E-07
  - 6 - 1.E-08
  - 7 - 1.E-09
  - 8 - 1.E-10

**Usage Guidelines**

Sets a standard option for the high-order path for SDSF.

The SD is kept at a value of 100 erroredBits/sec less than the corresponding value of the SF. So if the SD threshold is configured at 1 error in every 100000 bits/sec, then the SF threshold automatically becomes 1 error in every 1000 bits/sec.

**Examples**

```
hopath-sdsf /
```
line-timing

This command enables the SPIO to recover transmit timing source via the line attached to the selected port. By default, line-timing is not enabled.

**Important**
To employ line-timing recovery, the SPIO card(s) must be equipped with the optional Stratum 3 clock module.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax Description**

| no | line-timing |

**Usage Guidelines**
The port must be enabled (with the `no shutdown` command) to enable recovery of timing source via the line. As well, the card's slot number must be entered in the `recover line#` command of the BITS port configuration mode.

**Important**
If the SPIO is connected to an external Building Integrated Timing Supply (BITS) source, BITS timing always takes precedence over line-timing.

**Examples**
Disable timing clock recovery on this port.

`no line-timing`
loopback

Configures the type of loopback mode used for diagnostic testing.

**Note**
The `loopback` command under the Channelized Port Configuration Mode is now deprecated. The command will not be visible under the listing of available commands for Channelized Port Configuration Mode. If the command is executed accidentally, the following error message is displayed:

**Warning: loopback cli not supported for optical ports**

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax Description**

```
loopback { ds1-e1-diag | ds1-e1-line | none | sonet-sdh-diag | sonet-sdh-line }
```

- **ds1-e1-diag**
  Enables a system generated diagnostic lookback signal at the DS1/E1 layer.

- **ds1-e1-line**
  Loops back a network diagnostic signal at the DS1/E1 layer.

- **none**
  Stops diagnostic loopback signaling.

- **sonet-sdh-diag**
  Enables a system generated diagnostic lookback signal at the SONET/SDH layer.

- **sonet-sdh-line**
  Loops back a network diagnostic signal at the SONET/SDH layer.

**Usage Guidelines**
Setup diagnostic loopback signals for troubleshooting purposes.

**Examples**

```
loopback ds1-e1-diag
```
**lopath-sdsf**

Configures the low-order path for signal degrade/signal failure (SDSF) bit error rate (BER) thresholds.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax Description**

`lopath-sdsf lopath_value`

**lopath_value**

- 0: Disabled
- 1 - 1.E-03
- 10 - 1.E-12
- 2 - 1.E-04
- 3 - 1.E-05
- 4 - 1.E-06
- 5 - 1.E-07
- 6 - 1.E-08
- 7 - 1.E-09
- 8 - 1.E-10
- 9 - 1.E-11

**Usage Guidelines**

Sets a standard option for the low-order path for SDSF.

The SD is kept at a value of 100 erroredBits/sec less than the corresponding value of the SF. So if the SD threshold is configured at 1 error in every 100000 bits/sec, then the SF threshold automatically becomes 1 error in every 1000 bits/sec.

**Examples**

`lopath-sdsf /

Command Line Interface Reference, Modes C - D, StarOS Release 19 369`
This command configures the parameters that define the routing path for a DLCI. It must match with the DLCI configuration parameters. The values entered with these commands should be noted as they will be needed to configure the `frame-relay` and `dlci` commands also in this configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax Description**

```
path path_id { ds1 connects | e1 connects } service-type { frame-relay | mtp2 } frame-mapping multiplexing
index#index#framing mode mapping-mode { bit-sync | byte-sync } | timeslots slot# | slot# | frame-relay
| [ intf-type intf_type | lmi_type lmi_type ] ]
no path path_id { ds1 | e1 }connects
```

**no**
Deletes the routing path entry from the configuration.

**path path_id**
Identifies a specific path configuration that will be associated with a DLCI. The `path_id` must be an integer from 1 to 3.

**ds1 connects | e1 connects**
Selects the channelization for the connection.

**DS1:** (AKA: T1) Is associated with North American networks and would be the best choice to work with the SONET (can also work with SDH) framing selected with the `card` configuration command. DS1 splits the path into 28 logical connections.

`connects`: Defines the number of logical connections supported via the DS1. The selection must be an integer from 1 to 28.

**E1:** is associated with European networks and would be associated with the SDH (can also work with SONET) framing selected with the `card` configuration command. E1 splits the path into 21 logical connections.

`connects`: Defines the number of logical connections supported via the E1. The selection must be an integer from 1 to 21.

**service-type { frame-relay | mtp2 }**
Specifies the service type to be used for this path. When `multi-service` is enabled at the card level, different services are supported at the path-level for this port. For additional information, refer to the description of the `service-type` command in the *Card Configuration Mode Commands* chapter.
• **frame-relay**: Specifies Frame Relay mode for this path.

• **mtp2**: Specifies MTP2 service for this path.

### frame-mapping

Frame mapping sets the channelization according to the national standards that correlate with the framing/speed standards. This option selects the mapping of containers (C), virtual containers (VC), tributary units (TU), and tributary unit groups (TUG), that is appropriate for the channel characteristics:

• **tu11-au3**: Appropriate for DS1 in SDH. Maps as follows AU-3—VC-3—m#—TUG-2—m#—TU-12—VC-12—C-12

• **tu11-au4**: Appropriate for DS1 in SDH. Maps as follows AU-4—VC-4—TUG-3—m#—TUG-2—m#—TU-11—VC-11—C-11

• **tu12-au3**: Appropriate for E1 in SDH. Maps as follows AU-3—VC-3—m#—TUG-2—m#—TU-12—VC-12—C-12

• **tu12-au4**: Appropriate for E1 in SDH. Maps as follows AU-4—VC-4—TUG-3—m#—TUG-2—m#—TU-12—VC-12—C-12

• **vt1.5**: Only appropriate for DS1 in SONET framing.

• **vt2**: Only appropriate for E1 in SONET framing.

### multiplexing index# index#

*index#: TUG-2 index - Must be an integer from 1 to 7 to identify a multiplex channel between TUG-2 and VC-3 (E1) or TUG-3 (DS1).

*index#: TU index - Must be an integer from 1 to 4 (DS1) or 1 to 3 (E1) to identify a multiplex channel between TU-11 (DS1) and TUG-2 or between TU-12 (E1) and TUG-2.

### framing mode

Defines the framing modes to be used for the channelization to E1 or T1 of the (optical) port.

• options for E1:
  
  • **cas**: standard mapping with CAS
  
  • **cas-crc4**: CRC4 mapping with CAS
  
  • **crc4**: CRC4 mapping
  
  • **standard**: mapping

• options for DS1:
  
  • **esf**: extended superframe mapping
  
  • **sf**: superframe mapping
  
  • option for either E1 or DS1:
    
    • **unframed**
mapping-mode
  • bit-sync
  • byte-sync

timeslots timeslots
Defines up to 8 timeslot groupings for multiple fractional DS1/E1 channels. Each slot is 2.048/32 Mbytes. Slots 0 and 16 are reserved for synchronization and alarms. Slots 1-15 and 17-31 are used for data. Timeslots must be unique -- a timeslot can not be used in more than one grouping.

timeslots: Must be an integer from 1 to 31. Timeslot groups are separated by spaces and can consist of a single slot and/or a range indicated with a hyphen. Example: 3,7-10 is a single fractional group. NOTE there is no space after the comma. Timeslots must be unique -- a timeslot can not be used in more than one grouping.

frame-relay
Enables definition of a Frame Relay connection with the frame-relay command.

Important For release 8.1 and higher, this feature has been moved to the frame-relay command.

intf-type intf_type
Selecting the interface type specifies signaling parameters for the DLCI, options include:
  • dce: Selects data circuit-terminating equipment-type signaling.
  • dte: Selects data terminal equipment-type signaling.
  • nni: Selects the network-to-network interface

Default: DTE for Release 8.0
Default: DCE for Release 8.1

Important For release 8.1 and higher, this feature has been moved to the frame-relay command.

lmi_type lmi_type
Default: none.

Line management type options include:
  • ansi - ANSI ANNEXED LMI, may include option:
  • cisco - Cisco/Gang Of Four LMI
  • none - LMI Disabled
  • q933a - Q.933A LMI

Any of the above LMI types can take one or more additional options
• **n391** value - Number of keep exchanges before requesting a full status message. Default is 6. *value* must be an integer from 1 to 255.

• **n392** value - Error Threshold value. Default is 2. *value* must be an integer from 1 to 10.

• **n393** value - Monitored events count value. Default is 2. *value* must be an integer from 1 to 10.

• **t391** value - Timer to send messages. Default is 10. *value* must be an integer from 5 to 30.

• **t392** value - Polling verification timer value. Default is 15. *value* must be an integer from 5 to 30.

---

**Important**
For release 8.1 and higher, this feature has been moved to the **frame-relay** command.

---

**Usage Guidelines**
Defines the signaling characteristics of a frame relay connection or timeslots for a fractional connection.

Use this command to create E1 ports or fractional E1 ports. Fractional E1 ports are created with the timeslot definitions. The fractional E1 port can consist of one or more or all of the timeslots.

**Examples**
In the first example, define timers for the q933a LMI-type.
```
path 1 e1 1 tu12-au4 11 framing crc4 mapping-mode bit-async frame-relay intf-type dce lmi_type q933a n391 6 n392 2 n393 2 t391 10 t392 15
```

The next example defines 3 groups of fractional timeslots with group 1 having slots 1-5 and 8, group 2 having slot 22-25, and group 3 having slots 31.
```
path 1 e1 1 tu12-au3 11 framing cas mapping-mode bit-async timeslots 1-5,8 22-25 31
```
preferred slot

Identifies which card in a chassis should assume revertive (redundancy auto-recovery) functionality should the slot/port being configured go down. This command must be issued on a per port basis, allowing you to configure specific ports to be used on individual LCs or SPIO cards. For example, ports 1 through 4 could be configured as "preferred" on the LC in slot 17 while ports 5 through 8 are "preferred" on the LC in slot 33. In this scenario, both LCs would be in an Active operational state while still providing LC and port redundancy for the other.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax Description**

- `preferred slot slot#`
- `no preferred slot`

  `slot#`
  Identifies the physical slot in the chassis where the line card is installed.

  `no`
  Disables revertive, or auto-recovery, operation for the port.

**Usage Guidelines**
This command enables or disables revertive port redundancy. So after a port failover, when the original port is restored to service (i.e. link up) the system will return service to that port automatically.

Disabled, which is the default setting, causes non-revertive operation; requiring an administrative user to manually issue a port switch to command to return service to the original port.

**Examples**

```
preferred slot 17
```
pwe3-cesopsn

This command has been deprecated and replaced by the mtp2 command.
shutdown

Terminates all processes supporting the port or blocks the shutting down of the port. Conversely, this command with the no keyword enables the port.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax Description
| no | shutdown

no
Enables the port's administrative state. When omitted the card is shutdown (removed from service).

Usage Guidelines
Shut down a port prior to re-cabling and/or other maintenance activities.
This command with the no keyword is required to bring a port into service.

Examples
Use the following command to disable a port:
shutdown
Use the following command to enable a port for service:
no shutdown
**snmp trap link-status**

Enables/disables the generation and sending of an SNMP (notification) trap when the port experiences a change of state (up or down).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax Description**

```
[ no ] snmp trap link-status
```

- **no**
  Disables the sending of traps for link-status changes.

**Usage Guidelines**
Enable the sending of link-status change traps if there is a monitoring facility that can use the information or if there are troubleshooting activities in progress.

**Examples**

```
snmp trap link-status
```
threshold high-activity

Configures the port's high and low activity thresholds.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax Description**

```
threshold high-activity high_thresh [ clear low_thresh ]
```

- **high_thresh**
  - Default: 50
  - Sets the threshold for the highest percentage of port activity that must be met or exceeded, within the polling interval, to generate an alert or alarm.
  - `high_thresh_%` can be configured to any integer value between 0 and 100.

- **clear low_thresh**
  - Default: 50
  - Sets the threshold for the lowest percentage level of port activity that must be met to generate and send a clear alarm. If port activity does not drop to or below this threshold then the alarm is maintained.
  - `low_thresh_%` can be configured to any integer value between 0 and 100.

**Important**
This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage Guidelines**
High port activity thresholds generate alerts or alarms based on the utilization percentage of each configured port during the specified polling interval. This threshold is configured on a per-port basis.

Alerts or alarms are triggered for high port activity based on the following rules:

- **Enter condition**: Actual percent utilization of a port > High Threshold
- **Clear condition**: Actual percent utilization of a port < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command in the Global Configuration Mode Commands chapter of this reference to configure the polling interval and the `threshold monitoring` command in this chapter to enable thresholding for this value.

**Examples**

The following command configures a high port utilization threshold percent of 70 and a low threshold of 50 for a system using the Alarm thresholding model:

```
threshold high-activity 70 clear 50
```
threshold monitoring

Enables thresholding for port-level values.

Product: SGSN

Privilege: Security Administrator, Administrator

Syntax Description:

\[ \text{no} \] threshold monitoring

**no**

Disables threshold monitoring for port-level values. This is the default setting.

Usage Guidelines:

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e. high-activity) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps**: SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Complete descriptions and other information pertaining to these traps is located in the starentMIB(8164).starentTraps(2) section of the SNMP MIB Reference.

  The generation of specific traps can be enabled or disabled on the system allowing you to view only those traps that are most important to you.

- **Logs**: The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.

- **Alarm System**: High threshold alarms generated within the specified polling interval are considered "outstanding" until a the condition no longer exists and/or a condition clear alarm is generated.

"Outstanding" alarms are reported to through the system's alarm subsystem and are viewable through the system's CLI.

The following table indicates the reporting mechanisms supported by each of the above models.
Table 2: Thresholding Reporting Mechanisms by Model

<table>
<thead>
<tr>
<th>Model</th>
<th>SNMP Traps</th>
<th>Logs</th>
<th>Alarm System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Alarm</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

This command enables thresholding for port-level values. Refer to the `threshold high-activity`, `threshold rx-utilization`, and `threshold tx-utilization` commands in this chapter for information on configuring these values. In addition refer to the `threshold poll` command in the Global Configuration Mode Commands chapter of this reference for information on configuring the polling interval over which these values are monitored.

**Examples**

Use the following command to terminate thresholding:

`no threshold monitoring`
**threshold rx-utilization**

Configures thresholds for receive-port utilization.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax Description**

```
threshold rx-utilization high_thresh [ clear low_thresh ]
```

`high_thresh`

Default: 80
The high threshold receive port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
The percentage can be configured to any integer value between 0 and 100.

`clear low_thresh`

Default: 80
Allows the configuration of the low threshold.
The low threshold receive port utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated.
The percentage can be configured to any integer value between 0 and 100.

---

**Important**
This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage Guidelines**

Receive port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data received during the specified polling interval. This threshold is configured on a per-port basis.

---

**Important**
Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive or transmit utilization threshold be configured.
Alerts or alarms are triggered for receive port utilization based on the following rules:

- **Enter condition**: Actual percent utilization of a port for received data ≥ High Threshold
- **Clear condition**: Actual percent utilization of a port for received data < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command in the Global Configuration Mode Commands chapter of this reference to configure the polling interval and the `threshold monitoring` command in this chapter to enable thresholding for this value.

**Examples**

The following command configures a receive port high utilization threshold percent of 70 and a low threshold of 50 for a system using the Alarm thresholding model:

```
threshold rx-utilization 70 clear 50
```
**threshold tx-utilization**

Configures thresholds for transmit port utilization.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax Description**

`threshold tx-utilization high_thresh [ clear low_thresh ]`

- **high_thresh**
  
  Default: 80
  
  The high threshold transmit port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
  
  The percentage can be configured to any integer value between 0 and 100.

- **clear low_thresh**
  
  Default: 80
  
  Allows the configuration of the low threshold.
  
  The low threshold transmit port utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated.
  
  The percentage can be configured to any integer value between 0 and 100.

---

**Important**

This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

---

**Usage Guidelines**

Transmit port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data transmitted during the specified polling interval. This threshold is configured on a per-port basis.

---

**Important**

Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive or transmit utilization threshold be configured.
Alerts or alarms are triggered for transmit port utilization based on the following rules:

- **Enter condition:** Actual percent utilization of a port for transmit data \( \geq \) High Threshold
- **Clear condition:** Actual percent utilization of a port for transmit data \(<\) Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command in the Global Configuration Mode Commands chapter of this reference to configure the polling interval and the `threshold monitoring` command in this chapter to enable thresholding for this value.

**Examples**

The following command configures a transmit port high utilization threshold percent of 70 and a low threshold of 50 for a system using the Alarm thresholding model:

```
threshold tx-utilization 70 clear 50
```
**toh-sdsf**

Enable/disable line SDSF BER thresholds and configure the line transport overhead (TOH) signal degrade and signal failure (SDSF) bit error rate (BER) threshold.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
toh-sdsf toh_value
default toh-sdsf
```

**default**

Resets the default which disables this threshold.

**toh_value**

To facilitate configuration the SD and SF rates have been combined into a single setting.

- 0: Disabled
- 1 - 1.E-04
- 2 - 1.E-05
- 3 - 1.E-06
- 4 - 1.E-07
- 5 - 1.E-08
- 6 - 1.E-09
- 7 - 1.E-10
- 8 - 1.E-11

**Usage Guidelines**

This command can be used to configure the line threshold whether the port is active or standby and sets a standard option for the paired values of the line's signal degrade and signal failure (SDSF) BER.

The SD is kept at a value of 100 erroredBits/sec less than the corresponding value of the SF. So if the SD threshold is configured at 1 error in every 100000 bits/sec, then the SF threshold automatically becomes 1 error in every 1000 bits/sec.

The port will go operationally down as soon as the SD threshold is crossed.

**Examples**

```
toh-sdsf 1
```
vc-mapping

This command has been deprecated. Go to the frame-mapping keyword in the path command to configure this functionality.
vc-mapping
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.

**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) #
```

**Important**

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

- encryption, page 390
- end, page 391
- exit, page 392
- hmac, page 393
- key-exchange, page 394
**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**

```plaintext
equation { 3des | aes-128 | null | rc4 }
default encryption
```

default

Sets the encryption option to its default value of RC4.

**Usage Guidelines**

Use this command to specify encryption for the SSL cipher suite.

**Examples**

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**

```plaintext
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.

**Examples**

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.

Examples
The following command sets the key exchange option to its default value, which is RSA:

key-exchange rsa
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, page 396
- exit, page 397
- match any, page 398
- match dst-ip-address, page 399
- match dst-port-range, page 400
- match ip-tos, page 401
- match ipsec-spi, page 403
- match packet-size, page 404
- match protocol, page 405
- match src-ip-address, page 407
- match src-port-range, page 408
**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.

**Examples**
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.

**Examples**
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.

**Examples**
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.
**Examples**

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

<table>
<thead>
<tr>
<th>Product</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PDSN</td>
<td></td>
</tr>
<tr>
<td>HA</td>
<td></td>
</tr>
<tr>
<td>ASN-GW</td>
<td></td>
</tr>
<tr>
<td>HSGW</td>
<td></td>
</tr>
<tr>
<td>P-GW</td>
<td></td>
</tr>
<tr>
<td>SAEGW</td>
<td></td>
</tr>
<tr>
<td>SCM</td>
<td></td>
</tr>
</tbody>
</table>

### 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.

### Examples

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.

<table>
<thead>
<tr>
<th>Product</th>
<th>PDSN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HA</td>
</tr>
<tr>
<td></td>
<td>ASN-GW</td>
</tr>
<tr>
<td></td>
<td>HSGW</td>
</tr>
<tr>
<td></td>
<td>P-GW</td>
</tr>
<tr>
<td></td>
<td>SAEGW</td>
</tr>
<tr>
<td></td>
<td>SCM</td>
</tr>
</tbody>
</table>

| 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)#
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>match packet-size [ gt \mid lt \mid size ]</th>
</tr>
</thead>
</table>

\[ gt \mid lt \mid size \]

Specifies the packet length in bytes.

- \textit{gt}: indicates a packet size greater than the specified size.
- \textit{lt}: indicates a packet size less than the specified size.

\textit{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. |

<table>
<thead>
<tr>
<th>Examples</th>
<th>The following command specifies the packet length to be 1024 bytes.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>match packet-size 1024</td>
</tr>
</tbody>
</table>
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.

Examples
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.

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.

Examples

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.

**Examples**

The following command specifies the rule for packets having source port number from 23 to 88.

```
match src-port-range 23 to 88
```
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 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, page 410
- drop, page 412
- end, page 414
- exclude-emergency-events, page 415
- exclude-voice-events, page 416
- exit, page 417
- none, page 418
- reject, page 420
- report-overload, page 423
**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.
Examples

The following example shows DDN throttling with a throttling factor of 30 percent and a throttling 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.

Examples
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 connection 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

def

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:

![Command Prompt]

**Syntax Description**

```
[no] exclude-emergency-events
```

- **no**
  Removesthespecifiedoptionfromthesystem.

**Usage Guidelines**

Createacongestionactionprofilethatallowsemergencyeventstobeprocessedwhenacongestionthreshold
hasbeenreached.

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.

**Examples**
The following command allows emergency events to be processed:

``` exclusion-events ```
**Excluding 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.

**Examples**

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.

Examples
The following command configures the congestion action profile to take no Congestion 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 | 20 | 50 | 60 } | service-request | tau-request | lapi | [ apn-based ] none ddn | lapi | [ apn-based ] none ddn [lapi | [ apr-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.

**Examples**

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 connection 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 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 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 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.

enodeb-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 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 selects the eNodeBs at random, such that two overloaded MMEs in the same pool do not send overload messages to the same eNodeBs. When the MME 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.

Examples
The following command configures the MME 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 until the overload condition is cleared:
report-overload reject-non-emergency-sessions enodeb-percentage 50
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:

\langle context_name\rangle host_name\langle config-connectedapps\rangle #

- activate, page 426
- ca-certificate-name, page 427
- end, page 428
- exit, page 429
- ha-chassis-mode, page 430
- ha-network-mode, page 431
- rri-mode, page 432
- sess-ip-address, page 434
- sess-name, page 435
- sess-passwd, page 436
- sess-userid, page 437
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

Syntax Description
activate
no activate

activate

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.

Examples
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.

**Examples**
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

d

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.

**Examples**
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.

**Examples**
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.
## Examples

The following command sets the RRI mode to RAS.

```bash
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.

**Examples**

The following command sets an IPv4 address for a CA session.

```
sess-ip-address 10.10.1.1
```
**sess-name**

Sets the name for a CA session.

**Product**

SecGW (WSG)

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Connected Apps Configuration

```bash
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.

**Examples**

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**

```
sess-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.

**Usage Guidelines**

Use this password to set a password for a CA session.

**Examples**

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
```

Delete 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.

**Examples**

The following command sets the user identifier to *vsm-admin02*:

```
sess-userid vsm-admin02
```
sess-userid
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)#
```

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

- analyze, page 440
- discarded-flow-content-id, page 445
- end, page 446
- exit, page 447
- failure-action, page 448
- timeout action, page 450
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
• UNKNOWN
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.

### edr edr_format_name

**Important**: Static-and-Dynamic Content Filtering is only supported in 9.0 and later releases.

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.

Examples 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.

**Examples**

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

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.

**Examples**
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.
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, page 452
- deny-response code, page 453
- dictionary, page 455
- end, page 457
- exit, page 458
- failure-action, page 459
- icap server, page 462
- origin address, page 464
- response-timeout, page 465
- timeout action, page 466
- url-extraction, page 467
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.

**Examples**

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.
Examples

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 | custom2 | custom3 | 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.
**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.

**Examples**

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.

**Examples**

The following command sets the failure action to terminate:

```plaintext
failure-action terminate-flow
```
icap server

Adds an Internet Content Adaptation Protocol (ICAP) server configuration to the current Content Filtering Server Group (CFSG).

Important

In 8.1 and later releases, a maximum of five ICAP servers can be configured per Content Filtering Server Group. In 8.0 and earlier releases, 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]
nocap server ip_address [port port_number] [max messages] [priority priority] [standby]
n
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
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

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.

In 8.0, the ICAP solution supports only one connection between ACS Manager and ICAP server.

In 8.1, multiple ICAP server connections are supported per manager. At any time only one connection is active with the other connections acting as standby. In case of a connection failure, based on its priority, a standby connection becomes active. Any pending ICAP requests are moved to the new active connection. If a standby connection is unavailable, failure action is taken on all pending ICAP requests. See the command.

In 8.1 and later releases, 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.

In release 16.0, a maximum of ten active and standby servers per group can be configured.

**Examples**

The following command sets the ICAP server IP address to 10.2.3.4 and port to 1024:

```
icap server 10.2.3.4 port 1024
```

The following command specifies an ICAP server with IP address 10.6.7.8, port number 1024, and priority 3:

```
icap server 10.6.7.8 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.

Examples The following command sets the origin address of 10.1.1.1:

origin address 10.1.1.1
**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.

**Examples**

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 459 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`

**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.
**Examples**

The following command configures URLs sent from the ACF client to the ICAP server to contain the escape encoding as is:

```
url-extraction raw
```
Context Configuration Mode Commands A-D

This section includes the commands `aaa accounting` through `domain` service.

**Command Modes**

```
Exec > 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`, page 472
- `aaa authentication`, page 474
- `aaa constructed-nai`, page 476
- `aaa filter-id rulebase mapping`, page 478
- `aaa group`, page 479
- `aaa nai-policy`, page 481
- `access-list undefined`, page 483
- `administrator`, page 484
- `apn`, page 487
- `asn-qos-descriptor`, page 489
- `asn-service-profile`, page 491
- `asngw-service`, page 493
- `asnpc-service`, page 495
- `associate`, page 497
- bfd-protocol, page 499
- bgp extended-asn-cap, page 500
- bmsc-profile, page 501
- busyout ip, page 503
- busyout ipv6, page 505
- cae-group, page 507
- camel-service, page 508
- cbs-service, page 510
- cipher-suite, page 511
- class-map, page 513
- closedrp-rphandoff, page 515
- config-administrator, page 516
- content-filtering, page 519
- credit-control-service, page 520
- crypto dns-nameresolver, page 522
- crypto group, page 523
- crypto ipsec transform-set, page 525
- crypto map, page 527
- crypto template, page 529
- css server, page 531
- description, page 532
- dhcp-client-profile, page 533
- dhcp-server-profile, page 535
- dhcp-service, page 537
- dhcpv6-service, page 539
- diameter accounting, page 541
- diameter authentication, page 544
- diameter authentication failure-handling, page 547
- diameter dictionary, page 549
- diameter endpoint, page 550
- diameter-hdd-module, page 552
- diameter sctp, page 554
- diameter origin, page 556
- dns-client, page 557
- domain, page 559
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.

Examples

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**

```plaintext
| no | aaa authentication { administrator | subscriber } { local | none | radius-diameter } |
```  

**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.

**Examples**

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-context) #
```

**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.

---

**Examples**

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 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.

**Examples**

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.

**Examples**

The following command enters the AAA Server Group Configuration Mode for a AAA group named *test321*:

```bash
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 0x09 to their ASCII equivalent. For example; 0x00 0x01 0x2 0x03 will get remapped to 123.

Also by default the system accepts an NAI containing one or more 0x00 characters within the NAI ignoring all characters after the first 0x00.

When this keyword is disabled NAIs are processed as follows:

- Remapping of hexadecimal digits 0x00 through 0x09 within the user-provided NAI is disabled.
• When the NAI has an embedded 0x00 character anywhere within it (including if there is an extra 0x00 character at the end) the call is rejected.

**Usage Guidelines**

Use this command to disable or re-enable remapping of hexadecimal digits in the NAI.

**Examples**

The following command disables the remapping of hexadecimal digits in the NAI:

```plaintext
no aaa nai-policy reformat-alg-hex-0-9
```
**access-list undefined**

Configures the behavior of access control for the current context when an undefined access control list is specified.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > 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.

**Examples**

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 Security Administrator privileges in the current context.

**Product**

All

**Privilege**

Security Administrator

**Command Modes**

Exec &gt; Global Configuration &gt; Context Configuration

configure &gt; 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 | [ ecs | [ expiry-date date_time

`][ ftp | sftp-server sftp_name | ][ li-administration | [ nocli | [ noecs | [ timeout-absolute

`timeout_absolute | [ timeout-min-absolute timeout_min_absolute | [ timeout-idle timeout_idle |]

`[ timeout-min-idle timeout_min_idle |]

`no administrator user_name`

no

Removes Security Administrator privileges for the specified user name.

**user_name**

Specifies the 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.
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

**noecs**
Prevents the user from accessing ACS-specific commands.

**timeout-absolute timeout_absolute**

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 30000000.
The value 0 disables this timeout configuration.
Default: 0
**timeout-min-absolute timeout_min_absolute**

Specifies the maximum time (in minutes) the Security Administrator may have a session active before the session is forcibly terminated. `timeout_min_absolute` must be an integer from 0 through 525600. The value 0 disables this timeout configuration. Default: 0

**timeout-idle timeout_idle**

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.

**Examples**

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
```
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).

**Examples**

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 | af43 | ef ] [ -noconfirm ]
no asn-qos-descriptor qos_table_id [ default ] dscp [ be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | ef ] [ -noconfirm ]

no
```

Deletes a previously 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 | af43 | 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.

Examples

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>asn-service-profile</strong> id <strong>asn_profile_id</strong> direction { bi-directional</td>
<td>downlink</td>
</tr>
</tbody>
</table>

**no**

Deletes a previously 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.

Examples
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.

---

**Examples**

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 previously 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.

Examples

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.
Examples

The following command associates an internal QoS L2 mapping table to a VPN context:

```bash
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.

**Examples**

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**

```plaintext
[no ] bgp extended-asn-cap

no

Disables the ability of the router to send 4-octet ASN capabilities.
```

**Examples**

The following command enables the router to send 4-octet ASN Capabilities:

```plaintext
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

```plaintext
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```plaintext
(context_name)host_name(config-ctx)#
```

**Syntax Description**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>bmsc-profile name bmsc_profile_name [-noconfirm]</td>
</tr>
</tbody>
</table>

**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.

**Examples**

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 } | 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.

**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.

**Examples**
Assume an IPv4 pool named Pool10 with addresses from 192.168.100.1 through 192.168.100.254. To busy out the addresses from 192.168.100.50 through 192.169.100.100, enter the following command:

```
budget ip pool name Pool10 address-range 192.168.100.50 192.169.100.100
```
To restore the IPv4 addresses from the previous example and make them accessible again, enter the following command:

```
nobudget ip pool name Pool10 address-range 192.168.100.50 192.169.100.100
```
busout 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 ] busout ipv6 pool { all | all-dynamic | all-static | name pool_name } | address-range start_address end_address | lower-percentage percent | upper-percentage percent |
```

- **no**
  Disables the busout command specified.

- **ipv6**
  Configure IPv6 busout information.

- **pool**
  Configure IPv6 pool busout 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.

address-range start_address end_address
Busy out all addresses from start_address through end_address. start_address: The beginning IP address of the range of addresses to busy out entered in IPv6 colon-separated-hexadecimal notation.
end_address: The ending IP address of the range of addresses to busy out. This IP address must exist in the pool specified and entered in IPv6 colon-separated-hexadecimal notation.

lower-percentage percent
Busy out 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
Busy out 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 busy out 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.

Examples
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::
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.

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.

Examples
The following command creates a CAE group named group_1 and enters the Video Group Configuration Mode:

cae-group group_1
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 a CAMEL service

Examples

The following command creates a 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**

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.

**Examples**
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 an 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]host_name(config-ctx-cipher-suite)#
```

Cipher Suite Configuration Mode commands are defined in the *Cipher Suite Configuration Mode Commands* chapter.
Examples

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.

**Examples**

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.

**Examples**
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 | nocli | noecs | [ timeout-absolute abs_seconds ] | [ timeout-min-absolute abs_minutes ] | [ timeout-idle timeout_duration ] | [ timeout-min-idle idle_minutes ]

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.

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 value 0 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.

---

**Examples**
The following configures a context-level administration named user1 with ACS parameter control:
```
config-administrator user1 password secretPassword ecs
```
The following command removes a context-level administrator named user1:
```
no config-administrator user1
```
content-filtering

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.

**Examples**  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.

Examples

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
```

**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.

**Examples**

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).
Examples

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.

**Examples**
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.

Examples
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 and enters the Crypto Template 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**
- `crypto template name ikev2-dynamic`
- `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 configuring IPSec functionality.

**Usage Guidelines**
Use this command to create a new or enter an existing crypto template.

Entering this command results in the following prompt:

```
[context_name]host_name(config-crypto-tmpl-ikev2-tunnel)#
```

Crypto Template Configuration Mode commands are defined in the *Crypto Template Configuration Mode Commands* chapter.
The following command configures an IKEv2 dynamic crypto template called `crypto1` and enters the Crypto Template Configuration Mode:

```
crypto template crypto1 ikev2-dynamic
```
css server

In StarOS 9.0 and later releases, this command is obsolete. And, in earlier releases, this command is restricted.
**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.

**Examples**

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

```bash
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.

**Examples**

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.

Examples

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.

---

**Examples**

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 }
```

- **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.

Examples
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 { 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 { endpoint | max-retries | max-transmissions | server host_name }
```

- **endpoint**: Removes the authentication endpoint. The default server configured in default AAA group will be used.
- **max-retries**: Disables the retry attempts for Diameter authentication in this AAA group.
- **max-transmissions**: Disables the maximum transmission attempts for Diameter authentication in this AAA group.
- **server host_name**: Removes the Diameter host host_name from this AAA server group for Diameter authentication.

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

Configures default setting for specified parameter.

- **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).

```
```

Specifies the Diameter authentication dictionary.

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

**aaa-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 be an 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.

**Examples**

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.

---

**Usage Guidelines**

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

**Examples**

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

diameter authentication failure-handling eap-request result-code 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.
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 diam proxy" 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.

**Examples**

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.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command is license dependent. For more information, contact your Cisco account representative.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>no</th>
<th>diameter-hdd-module</th>
</tr>
</thead>
</table>

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.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

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.

**Examples**

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 { heartbeat-interval interval | path max-retransmissions retransmissions }
default diameter sctp { heartbeat-interval | path max-retransmissions }

default
Configures this command with the default settings.

- heartbeat-interval: Sets the heartbeat interval to the default value.
- path max-retransmissions: Sets the SCTP path maximum retransmissions to the default value.

heartbeat-interval interval
Specifies the time interval between heartbeat chunks sent to a destination transport address in seconds.
interval must be an integer from 1 through 255.
Default: 30 seconds

path max-retransmissions retransmissions
Specifies the maximum number of consecutive retransmissions over a destination transport address of a peer endpoint before it is marked as inactive.
retransmissions must be an integer from 1 through 10.
Default: 10
Usage Guidelines

Use this command to configure Diameter SCTP parameters for all Diameter endpoints within the context.

Examples

The following command configures the heartbeat interval to 60 seconds:
```
diameter sctp heartbeat-interval 60
```

The following command configures the maximum number of consecutive retransmissions to 6, after which the endpoint is marked as inactive:
```
diameter sctp path max-retransmissions 6
```
**diameter origin**

This command is deprecated and is replaced by the *diameter endpoint* command.
dns-client

Creates a DNS client and/or enters the DNS Client Configuration Mode.

Product
- 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] hostname (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.
Examples

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_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 subscriber's 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.

Examples

domain sampleDomain.net
no domain sampleDomain.net
Context Configuration Mode Commands E-H

This section includes the commands `edr-module active-charging-service` through `hss-peer-service`.

**Command Modes**

 Exec > 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`, page 564
- `edr-module active-charging-service`, page 565
- `egtp-service`, page 567
- `end`, page 569
- `epdg-service`, page 570
- `event-notif-endpoint`, page 572
- `exit`, page 574
- `external-inline-server`, page 575
- `fa-service`, page 576
- `firewall max-associations`, page 578
- `fng-service`, page 579
- `ggsn-service`, page 580
- `gprs-service`, page 582
- `gs-service`, page 584
• gtpc overload-protection egress, page 586
• gtpc overload-protection ingress, page 588
• gtp algorithm, page 590
• gtp attribute, page 592
• gtp charging-agent, page 603
• gtp data-record-format-version, page 605
• gtp data-request sequence-numbers, page 607
• gtp dead-server suppress-cdrs, page 609
• gtp deadtime, page 610
• gtp detect-dead-server, page 612
• gtp dictionary, page 614
• gtp duplicate-hold-time, page 617
• gtp echo-interval, page 619
• gtp egcdr, page 621
• gtp error-response, page 625
• gtp group, page 626
• gtp max-cdrs, page 628
• sgtp max-pdu-size, page 630
• gtp max-retries, page 632
• gtp node-id, page 634
• gtp redirection-allowed, page 635
• gtp redirection-disallowed, page 636
• gtp server, page 637
• gtp source-port-validation, page 640
• gtp storage-server, page 641
• gtp storage-server local file, page 643
• gtp storage-server max-retries, page 647
• gtp storage-server mode, page 648
• gtp storage-server timeout, page 650
• gtp suppress-cdrs zero-volume, page 651
• gtp suppress-cdrs zero-volume-and-duration, page 653
• gtp timeout, page 655
• gtp trigger, page 656
• gtp transport-layer, page 657
• gtpu-service, page 659
• ha-service, page 661
• hnbgw-service, page 663
• hsgw-service, page 665
• hss-peer-service, page 667
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-eap-profile)#
```

**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] host_name (config-ctx-eap-profile)#
```

EAP Configuration Mode commands are defined in the *EAP Configuration Mode Commands* chapter.

**Examples**

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)#
```

**Examples**

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:

```plaintext
[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.

- **-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.

**Important**
Service names must be unique across all contexts within a chassis.
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.

Examples

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

dend

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.

Examples

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 pdg-service sampleService
```
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

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.

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} host_name (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 cannot 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.

Examples

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.
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.

**Examples**

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.

**Examples**

The following command configures an FNG service named `fmg1` 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

```plaintext
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-ctx)>
```

**Syntax Description**

```plaintext
ggsn-service svc_name [-noconfirm ]
no ggsn-service svc_name
```

- **no**
  Deletes a previously 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.

**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.
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.

Examples

The following command creates a GGSN service named ggsn1:

ggsn-service ggsn1
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)#
```

**Examples**

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.

Examples

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 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.
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.

Examples

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 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] [default] gtpc overload-protection ingress
  - 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    |
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.

**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.

**Examples**
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
```
**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.
Examples

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

counture > 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 | diagnostics | abnormal-release-cause | direct-tunnel | duration-ms | dynamic-flag | dynamic-flag-extension | furnish-charging-information | imei | imsi-unauthenticated-flag | lapi | 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 { sgspdprecord | 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 | cell-plmn-id | diagnostics | direct-tunnel | duration-ms | dynamic-flag | dynamic-flag-extension | furnish-charging-information | imei | imsi-unauthenticated-flag | lapi | local-record-sequence-number | losdv | ms-timezone | msisdn | node-id | pdn-connection-id | pdp-address | pdp-type | pgw-ipv6-addr | pgw-plmn-id | plmn-id | qos | rat | recordextension | record-extensions rat | served-mnai | served-pdp-pdn-address-extension | served-pdp-pdn-address-prefix-length | sgsn-change | sgw-ipv6-addr | sms { destination-number | recording-entity | service-centre } | 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 | cell-plmn-id | diagnostics | direct-tunnel | duration-ms | dynamic-flag | dynamic-flag-extension |
furnish-charging-information | imei | imsi-unauthenticated-flag | lapi | local-record-sequence-number | losdv | ms-timezone | msisdn | node-id | pdn-connection-id | pdp-address | pdp-type | pgw-ipv6-addr | pgw-plmn-id | plmn-id | qos | rat | recordextension | record-extensions rat | record-type | served-mnai | served-pdp-pdn-address-extension | served-pdp-pdn-address-prefix-length | sgsn-change | sgw-ipv6-addr | served-mnai | sms | destination-number | recording-entity | service-centre | 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.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>This keyword option will be available only if a valid license is installed. For more information, contact your Cisco account representative.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>This CLI command and the associated options are not available for products other than S-GW and P-GW. The option &quot;non-gbr-bearers-only&quot; is available in S-GW and P-GW but the other options are available in S-GW only.</td>
</tr>
</tbody>
</table>

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.

**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.

**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.
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, GTTP group name is used. For default GTTP groups, GTTP 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 restart-value><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 GTTP CDRs as an alphanumeric string of 1 through 16 characters. Each Session Manager task generates a unique NodeID string per GTTP 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 GTTP group name will be used instead (For default GTTP groups, context-name will be used).

---

**Important**

If this `node-id-suffix` is not configured, the GGSN uses the GTTP context name as the Node-id-suffix (truncated to 16 characters) and the SGSN uses the GTTP group name 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 a hexadecimal number from 0x0 through 0xFFFFFFFF 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.
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.

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.

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.

Examples

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).

<table>
<thead>
<tr>
<th>Product</th>
<th>GGSN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SGSN</td>
</tr>
<tr>
<td></td>
<td>P-GW</td>
</tr>
<tr>
<td></td>
<td>SAEGW</td>
</tr>
</tbody>
</table>

| 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)#
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>gtp charging-agent address ip_address [ port port ]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>no gtp charging-agent</td>
</tr>
</tbody>
</table>

| 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 gtp 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.

Examples
The following command configures the system to use the interface with an IP address of 192.168.13.10 as the accounting interface with port 20000 to the CGF:

gtpp charging-agent address 192.168.13.10 port 20000
gtpp data-record-format-version

Encodes the data record format version. The version indicates the 3GPP release version.

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.

<table>
<thead>
<tr>
<th>Product</th>
<th>GGSN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>P-GW</td>
</tr>
<tr>
<td></td>
<td>SGSN</td>
</tr>
<tr>
<td></td>
<td>S-GW</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Administrator</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Exec &gt; Global Configuration &gt; Context Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure</td>
<td>context context_name</td>
</tr>
<tr>
<td></td>
<td>Entering the above command sequence results in the following prompt:</td>
</tr>
<tr>
<td></td>
<td>[context_name]host_name(config-ctx)#</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>gtpp data-record-format-version string</th>
</tr>
</thead>
</table>

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.
Examples

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.
Examples

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

```bash
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.
Examples

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**
Confirms this command with the default setting.
Default: 0

- **consecutive-failures max_number**
Specified 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.
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.

**Examples**

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
Configure 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.
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.

- 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.

Custom-defined dictionary.

This is a custom-defined dictionary for eG-CDR encoding.

These custom-defined dictionary have default behavior or "standard" dictionary.

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.

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.

---

**Examples**

The following command configures the system to use `custom3` dictionary to encode IP address in Binary format in G-CDRs:

```
gtp 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.
Examples

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.

### Examples

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
| rulebase-max-length | service-data-flow threshold | 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
```

**closing-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 ddfs. 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 eGCDR/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.

**Examples**

Use the following command to set the maximum number of LoSDV containers to 7:

```
gtp egcdr losdv-max-containers 7
```

The following command sets an eG-CDR threshold interval of 6000 seconds:

```
gtp 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.

**Examples**

```
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

```bash
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.

Examples

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 gtp max-pdu-size command is met.

Examples

The following command configures the system to place a maximum of 10 CDRs in a single GTPP packet before transmitting the packet:

gtp max-cdrs 10
sgtp 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
sgtp max-pdu-size pdu_size
default sgtp 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 to 65400. 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).

Examples

The following command configures a maximum PDU size of 2048 octets:

gtp 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 `gtp detect-dead-server` and `gtp timeout` commands for additional information.

**Examples**

The following command configures the maximum number of re-tries to be 8:

`gtp 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 alphanemic string of 1 through 16 characters.

Usage Guidelines
Use this command to configure the GTPP Node ID for all CDRs.

Examples
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.
In release 16.0, 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).

**Examples**

The following command configures a CGF with an IP address of 192.168.2.2 and a priority of 5.

```plaintext
gtpp server 192.168.2.2 priority 5
```

The following command deletes a previously configured CGF with an IP address of 100.10.35.7:

```plaintext
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**
\[default | no | gtpp source-port-validation\]

**Syntax Description**
- **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.

**Examples**
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.
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.

**Examples**

The following command configures a back-up server with an IP address of 192.168.1.2:

`gtpp storage-server 192.168.1.2`
gtpp storage-server local file

Configures the parameters for GTPP files stored locally on the GTPP storage server. This command is available for 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.
If the push is done through gtp context, then the push rate is lesser compared to via local context as the HDD is attached to the local context.

**Important**

rotation { cdr-count count | 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 aaaprox 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.

**Examples**

The following command configures rotation for every 1.5 hours (5400 seconds) for locally stored files.

gtp 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.

**Examples**
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.

Examples
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.

Examples

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.

**Examples**

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:

```bash
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:

```bash
gtpp suppress-cdrs zero-volume internal-trigger-cdr external-trigger-cdr
```

To suppress interim zero volume CDRs due to external triggers use:

```bash
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.
gtpp suppress-cdrs zero-volume-and-duration

**Examples**

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.

**Examples**
- 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).
The following command enables TCP as the transport layer protocol for the GSN's Ga interface.

```
gtp 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.

Examples

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
```
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 alphanumerical 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.
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.

Examples

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
```
**hnbgw-service**

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-cx)#
```

**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.

Examples

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.

Examples

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.

Examples

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
```
Context Configuration Mode Commands I-M

This section includes the commands `ikev1 disable-initial-contact` through `multicast-proxy` service.

**Command Modes**

Exec > 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).

- `ikev1 disable-initial-contact`, page 672
- `ikev1 disable-phase1-rekey`, page 673
- `ikev1 keepalive dpd`, page 674
- `ikev1 policy`, page 676
- `ikev2-ikesa`, page 678
- `ims-auth-service`, page 680
- `ims-sh-service`, page 682
- `inspector`, page 684
- `interface`, page 687
- `ip access-group`, page 690
- `ip access-list`, page 692
- `ip arp`, page 694
- `ip as-path access-list`, page 696
- `ip community-list`, page 698
• ip dns-proxy source-address, page 700
• ip domain-lookup, page 701
• ip domain-name, page 702
• ip extcommunity-list, page 703
• ip forward, page 705
• ip guarantee, page 706
• ip identification packet-size-threshold, page 707
• ip igmp profile, page 708
• ip localhost, page 709
• ip name-servers, page 710
• ip pool, page 712
• ip prefix-list, page 726
• ip prefix-list sequence-number, page 728
• ip route, page 729
• ip routing maximum-paths, page 732
• ip routing overlap-pool, page 733
• ip rri, page 734
• ip rri-route, page 735
• ip sri-route, page 737
• ip vrf, page 739
• ip vrf-list, page 741
• ipms, page 742
• ipne-service, page 744
• ipsec replay, page 745
• ipsec transform-set, page 746
• ipsg-service, page 747
• ipv6 access-group, page 749
• ipv6 access-list, page 750
• ipv6 dns-proxy, page 751
• ipv6 neighbor, page 752
• ipv6 pool, page 753
• ipv6 prefix-list, page 758
• ipv6 prefix-list sequence-number, page 760
- ipv6 route, page 761
- ipv6 route-access-list, page 764
- ipv6 rri, page 766
- ipv6 rri-route, page 767
- ipv6 sri-route, page 769
- isakmp disable-phase1-rekey, page 770
- isakmp keepalive, page 771
- isakmp policy, page 772
- iups-service, page 773
- l2tp peer-dead-time, page 775
- lac-service, page 776
- lawful-intercept, page 778
- lawful-intercept dictionary, page 779
- ima-service, page 780
- ins-service, page 782
- location-service, page 784
- logging, page 786
- mag-service, page 788
- map-service, page 790
- mipv6ha-service, page 792
- mme-service, page 794
- mobile-access-gateway, page 796
- mobile-ip fa, page 797
- mobile-ip ha assignment-table, page 799
- mobile-ip ha newcall, page 801
- mobile-ip ha reconnect, page 803
- mpls bgp forwarding, page 804
- mpls exp, page 805
- mpls ip, page 806
- mseg-service, page 807
- multicast-proxy, page 808
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 v1 protocol.

Examples
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 1 SAs 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.

**Examples**

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.
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.

If DPD is enabled while IPSec tunnels are up, it will not take effect until all of the tunnels are cleared.

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.
Examples

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.

**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 | transform-set transform_set_name }
```

- **no**
  - Removes the entered IKEv2 security association authentication method set or transform set from the system.

- **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.

- **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 Association 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.

Examples

The following command configures an IKEv2 security association transform set called `ikesa3` and enters the IKEv2 Security Association Configuration Mode:

```
iev2-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**
  Delete 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.
Servicenames 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.

Examples
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

**Syntax Description**

```plaintext
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.
```

**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.
Examples

The following example creates or enters an IMS Sh service named *ims-1*:

```yaml
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 ] [ noecs ] [ timeout-absolute abs_seconds ] [ timeout-min-absolute abs_minutes ] [ timeout-idle timeout_duration ] [ timeout-min-idle idle_minutes ]

no inspector user_name

no

Removes a previously configured inspector account.

user_name

Specifies a name for the context-level inspector account 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.

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.

---

**Examples**  
The following command creates a context-level inspector account named *user1*:

```
inspector user1 password secretPassword
```

The following command removes a context-level inspector account named *user1*:

```
no inspector user1
```
interface

Creates 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

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

Important
Refer to the Ethernet Interface Configuration Mode Command chapter for more information.
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`.

**Examples**
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 \textit{GRE\_tunnel1}, if necessary:

\texttt{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.

**Examples**

The following commands add `sampleGroup` to the context-level ACL with a priority of 0:

```
ip access-group sampleGroup 0
```
ip access-list

Enables creation, configuration or deletion of 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.
In Release 8.0, name is an alphanumeric string of 1 through 79 characters.
In Release 8.1 and later, 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.
A maximum of 64 rules can be configured per ACL. The maximum number of ACLs that can be configured per context is limited by the amount of available memory in the VPN Manager software task; it is typically less than 200.

The no version of this command deletes the ACL.

Refer to the Access Control Lists appendix of the System Administration Guide for more information on ACLs.

Examples

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)#
```
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.

**Examples**

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**


**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.
Examples

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 ... }

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.

**Examples**

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.

**Examples**

The following command identifies an interface with an address of 10.23.255.255 in a destination context where the system forwards all intercepted DNS requests:

```
ip dns-proxy source-address 10.23.255.255
```
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

```bash
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 lookup is necessary if the subscribers configured for the context are to be allowed to use logical host names for services which requires the host name resolution via DNS.

**Examples**

- `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.

**Examples**

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.

**Examples**

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.

Examples

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.

Examples
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.

**Examples**

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.

Examples

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
```bash
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.

**Examples**
```
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.

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.

**Examples**

```
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 ] low_thres [ clear high_thres ] ] [ explicit-route-advertise ] [ group-name group_name ] [ include-nw-bcast ] [ napts-users-per-ip-address users_per_ip ] [ alert-threshold { pool-free | pool-hold | pool-release | pool-used } low_thres [ clear high_thres ] ] + [ max-chunks-per-user max_chunks_per_user ] [ nat-binding-timer nat_binding_timer ] [ nat-pkt-drop-threshold high_thres [ clear low_thres ] ] [ next-hop-forwarding-address ip_address ] [ on-demand ] [ port-chunk-size port_chunk_size ] [ port-chunk-threshold port_chunk_threshold ] [ send-nat-binding-update ] + [ nat priority ] [ nat-one-to-one alert-threshold { pool-free | pool-hold | pool-release | pool-used } low_thres [ clear high_thres ] ] + [ nat-binding-timer nat_binding_timer ] [ nat-pkt-drop-threshold high_thres [ clear low_thres ] ] [ next-hop-forwarding-address ip_address ] [ on-demand ] [ respond-icmp-echo 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-vrf-list ] +
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 group_name ] [ include-nw-bcast ] [ next-hop-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-vrf-list ]
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.

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.

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.

dep_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
Advertise to the peer routes only if addresses are being used in pool.

alert-threshold { group-available | pool-free | pool-hold | pool-release | pool-used } low_thresh | clear high_thresh }
Default: All thresholds are disabled.
Configures IP address pool-level utilization thresholds. These thresholds take precedence over context-level IP pool thresholds.
group-available: Set an alert based on the available percentage of IP addresses for the entire IP pool group.
pool-free: Set an alert based on the percentage of IP addresses that are unassigned in this IP pool.
pool-hold: Set an alert based on the percentage of IP addresses from this IP pool that are on hold.
pool-release: Set an alert based on the percentage of IP addresses from this IP pool that are in the release state.
pool-used: This command sets an alert based on the percentage of IP addresses that have been assigned from this IP pool.

Important Refer to the threshold available-ip-pool-group and threshold monitoring commands in this chapter for additional information on IP pool utilization thresholding.

low_thresh: The IP pool utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured 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
Includes the network and broadcast addresses for ordinary pools and NAT pools.
To remove the include-nw-bcast option from the ip pool, use the no ip pool test include-nw-bcast command.

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.

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 ] +

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.

Important
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 keyword 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.
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

- **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

- **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.

- **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%
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.
The `nexthop-forwarding-address` support for NAT IP pools is functional only in later releases of Release 9.0 and in Release 10.0 and later releases.

- **on-demand**: Specifies allocating IP address when matching data traffic begins.
- **send-nat-binding-update**: Specifies sending NAT binding updates to AAA for this realm. Default: Disabled

**Important**  
send-nat-binding-update is 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.

**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.

**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-listvrf_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.
Examples

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:

```
oip 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** `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 IPv4 dotted-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
```
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 |

**Usage Guidelines**

Use this command to enable and disable the inclusion of IP prefix list sequence numbers in the configuration file.

**Examples**

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**

Indicates the route specified by this options is to be removed from the configuration.

**ip_address/ip_mask | ip_address/ip_mask**

Specifies a destination IP address or group of addresses that will use this route.

*ip_address/ip_mask*: Specifies a combined IP address subnet mask bits to indicate what IP addresses to which the route applies. *ip_address* 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.

**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.

*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.

**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

**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 (BFD_sessUp and BFD_sessDown).

**Examples**

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 10.2.3.0/32 192.168.1.2 egressSample1 precedence 160
no ip route 10.2.3.4 255.224.0.0 10.1.2.3 egressSample2 cost 43
```

The following command adds a route using the combined IP address and subnet mask form and specifies the egress interface as tunnel type:

```
ip route 10.2.3.0/32 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 from 1 through 10 (releases prior to 18.2) or 1 through 32 (release 18.2+). 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.

**Examples**
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 alphanumeric string of 1 through 63 characters.

Usage Guidelines
Use this command to configure RRI regress clear port IPv4 parameters.

Examples
ip rri 10.1.1.1 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.

**Examples**

`ip rri-route network-mode L3 rri-ip 10.1.1.23 next-hop 10.1.1.25 interface rriroute04`
ip sri-route

Configures Layer 3 (L3) High Availability (HA) IPv4 routing parameters for Service Route Injection (SRI). (VPC-VSM only)

Important
The ip sri-route CLI command is deprecated, and not supported in 19.0 and later releases.

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 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.

Examples
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.

**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.

**Examples**

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 ]`

The `no` command 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 alphanumerical 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.

**Examples**

The following command creates a VRF list named `corp103` and adds a VRF named `vrf3567`:

`ip vrf-list corp103 permit vrf3567`
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:

```plaintext
[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.

**Examples**

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.

Examples

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.

**Examples**
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.

**Examples**

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**

```plaintext
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
```

- **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.

```plaintext
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**.

### Examples

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.

**Examples**

```
ipv6 access-group group_1
```
**ipv6 access-list**

Configures access list (or packet filter) name and enters the IPv6 ACL Configuration Mode.

**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 access-list name |

**no**

Indicates the access list specified is to be removed from the configuration.

**name**

Specifies the access list for which to enter the IPv6 ACL Configuration Mode or the list to remove. *name* is an alphanumeric string of 1 through 79 characters.

**Usage Guidelines**

Executing this command enters the IPv6 ACL Configuration Mode in which rules and criteria are defined for the ACL.

**Examples**

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.

Examples
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**
  
  **ipv6_address** is the IP address of node to be added to the table.

  **hardware_address**
  
  **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.

**Examples**

Add the ipv6 address fe80::210:83ff:feff:7a9d::24 and associated 48 bit MAC address 0:10:83:ff:7f:7a:9d to the table.

```
ipv6 neighbor fe80::210:83ff:feff:7a9d::24 0:10:83:ff:7f: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_address end_address | suppress-switchover-arps | prefix-length prefix_length | private priority | public priority | shared priority | static priority | group-name name | vrf vrf-name }
```

**no ipv6 pool name**

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.

**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} | prefix | pool-free | pool-used | 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.
ipv6 pool

- **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.
- **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.

**Examples**
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.

**Examples**
`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.

**Examples**

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).
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.

SNMP traps are generated when BFD sessions go up and down (BFDsSessUp and BFDsSessDown).

Examples

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.

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

**Important**

**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.

**Examples**

```
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.

**Examples**

```
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.

Examples
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

UsethiscommandtoconfigureL3HAIPv6routingparametersforSRI.

Examples
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.
**Examples**

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.

**Examples**

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.
Examples

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:

```
nolac-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.
ima-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**

```
ima-service service_name [-noconfirm]
no ima-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).

**Examples**

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 | Ins-service name |

- **no**
  - Removes the specified LNS 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.
Examples

To add a new LNS service named LNS1 and enter the LNS Service Configuration Mode, enter the following commands:

```
Ins-service LNS1
```

To configure an existing LNS service named LNS2, enter the following command:

```
Ins-service LNS2
```

To delete an existing LNS service named LNS3, enter the following command:

```
no Ins-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`

**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.

**-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)#
```

**Examples**

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 | pdu-data { none | hex | hex-ascii } | pdu-verbosity pdu_level | rate value |
```

**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**
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.

**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.

**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

**Usage Guidelines**

Set the log servers to enable remote review of log data.

**Examples**

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
```
**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.

Examples

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.

For details about the commands and parameters, check the MAP Service Configuration Mode Commands chapter.
Examples

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
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.
Examples

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-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 ]
no mme-service service_name
```

- **no**
  Removes the specified MME service from the context.

  **service_name**
  Specifies the name of the MME service. If service_name does not refer to an existing service, the new service is created if resources allow.
  service_name 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 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.
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.

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.

Examples

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
```
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.

Examples
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.

Examples

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

- 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.
Examples

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

```bash
configure > context context_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```bash
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**—disables 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.

**Examples**

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**

```
```

- **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.

**Examples**

```
mobile-ip ha reconnect
mobile-ip ha reconnect static-homeaddr
mobile-ip ha reconnect static-homeaddr dynamic-pool-allocation
no mobile-ip ha reconnect
no mobile-ip ha reconnect static-homeaddr
```
**mpls bgp forwarding**

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 next hop for the BGP routes must be reachable via LDP.

**Caution**

This command should always be enabled when next hop is not reachable through LSP.

**Examples**

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>`.

**Examples**

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.

**Examples**

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 IPv4 dotted-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.
**Usage Guidelines**

Use this command to create/configure/delete a multicast proxy host configuration.

**Examples**

The following command creates an IGMP multicast host configuration:

```
multicast proxy igmp interface 192.155.1.34 range-start 255.0.0.0 range-end 255.0.0.1
```
multicast-proxy
Context Configuration Mode Commands N-R

This section includes the commands `nw-reachability server` through `router` service.

**Command Modes**

`Exec > 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`, page 814
- `network-requested-pdp-context activate`, page 816
- `network-requested-pdp-context gsn-map`, page 818
- `network-requested-pdp-context hold-down-time`, page 820
- `network-requested-pdp-context interval`, page 821
- `network-requested-pdp-context sgsn-cache-time`, page 822
- `operator`, page 823
- `optimize pdsn inter-service-handoff`, page 826
- `pcc-af-service`, page 827
- `pcc-policy-service`, page 829
- `pcc-service`, page 831
- `pcc-sp-endpoint`, page 833
- `pdg-service`, page 835
- `pdif-service`, page 836
• pdsn-service, page 837
• pdsnclosedrp-service, page 839
• pgw-service, page 841
• pilot-packet, page 843
• policy, page 846
• policy-group, page 847
• policy-map, page 848
• ppp, page 849
• ppp magic-number, page 854
• ppp statistics, page 855
• proxy-dns intercept-list, page 857
• radius accounting, page 859
• radius accounting algorithm, page 862
• radius accounting apn-to-be-included, page 864
• radius accounting billing-version, page 865
• radius accounting gtp trigger-policy, page 866
• radius accounting ha policy, page 867
• radius accounting interim volume, page 868
• radius accounting ip remote-address, page 870
• radius accounting keepalive, page 872
• radius accounting rp, page 874
• radius accounting server, page 877
• radius algorithm, page 881
• radius allow, page 882
• radius attribute, page 884
• radius authenticate null-username, page 887
• radius authenticate apn-to-be-included, page 888
• radius authenticator-validation, page 889
• radius change-authorize-nas-ip, page 890
• radius charging, page 893
• radius charging accounting algorithm, page 895
• radius charging accounting server, page 897
• radius charging algorithm, page 899
• radius charging server, page 900
• radius deadtime, page 902
• radius detect-dead-server, page 904
• radius dictionary, page 906
• radius group, page 908
• radius ip vrf, page 909
• radius keepalive, page 911
• radius max-outstanding, page 913
• radius max-retries, page 914
• radius max-transmissions, page 915
• radius mediation-device, page 917
• radius probe-interval, page 918
• radius probe-max-retries, page 919
• radius probe-message, page 920
• radius probe-timeout, page 921
• radius server, page 922
• radius strip-domain, page 925
• radius timeout, page 926
• radius trigger, page 927
• remote-server-list, page 929
• route-access-list extended, page 931
• route-access-list named, page 933
• route-access-list standard, page 935
• route-map, page 937
• router, page 939
nw-reachability server

Add 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: 60s

- **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.

Examples

To set a network device called Internet Device with the IP address of 192.168.100.10 as the remote address that is pinged to determine network reachability and use the address 192.168.200.10 as the origination address of the ping packets sent, enter the following command:

nw-reachability server InternetDevice local-addr 192.168.200.10 remote-addr 192.168.100.10
network-requested-pdp-context 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.

**Examples**

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 ispl:

```
network-requested-pdp-context activate address 20.13.5.40 dst-context pdn1 imsi 3319784450 apn ispl
```
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.

**Examples**

The following command configures the system to communicate with a gsn-map node having an IP address of `192.168.2.5`:

```
network-requested-pdp-context gsn-map 192.168.2.5
```
network-requested-pdp-context hold-down-time

Configures the time duration to that the system will wait after the SGSN rejects an attempt for a network-requested PDP context creation for the subscriber.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > 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.

**Examples**

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:

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

Syntax Description
network-requested-pdp-context interval \textit{time}
default network-requested-pdp-context interval

default
Returns the command to its default setting of 60.

\textit{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. \textit{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.

Examples
The following command specifies that the system waits \textit{120} seconds before allowing another network requested PDP context for an MS:

\texttt{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.

**Examples**

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 ] | [ noecs ] | [ timeout-absolute abs_seconds ] | [ timeout-min-absolute abs_minutes ] [ | timeout-idle timeout_duration ] | [ timeout-min-idle idle_minutes ]

no operator user_name

no

Removes a previously configured context-level operator account.

user_name

Specifies a name for the account 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.

cs
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.

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.

Examples

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
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.

**Examples**

```
optimize pdsn inter-service-handoff
```
**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.

**Examples**

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 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.

Examples

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.

Examples

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-context)#
```

**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.

---

**Examples**

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
```

- **noname**
  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.

**Examples**
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.

**Examples**

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.
**Examples**

The following command will enter the PDSN Service Configuration Mode creating the service `sampleService`, if necessary.

```bash
pdsn-service sampleService
```

The following command will remove `sampleService` as being a defined PDSN service.

```bash
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.
**Examples**

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.
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.

**Examples**

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
```
pilot-packet

Configures Pilot Packets containing key pieces of information about a subscriber session to third party network elements.

**Product**
- HA
- NAT
- PDSN
- P-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**

```
pilot-packet { attribute { foreign-agent-ip-address | nai | rat-type | serving-nw-id } | name server_name | source-ip-address source_ip_address destination-ip-address destination_ip_address destination-udp-port udp_port_value | dscp-marking dscp_value } | trigger rat-change generate { nat-info-only | user-info-and-nat-info | user-info-only } } 

default pilot-packet { attribute { foreign-agent-ip-address | nai | rat-type | serving-nw-id } | trigger rat-change } 

no pilot-packet { attribute { foreign-agent-ip-address | nai | rat-type | serving-nw-id } | name server_name | trigger rat-change }

default
```

Configures the default settings for the specific command/keyword.

**no**

Disables the Pilot packet option.

```
attribute { foreign-agent-ip-address | nai | rat-type | serving-nw-id }
```

Configures the optional attributes to be sent in pilot packet.

- **foreign-agent-ip-address**: Specifying this option includes the optional field "Foreign Agent IP Address" in pilot packet.
nai

Specifying this option includes the optional field "NAI" in pilot packet.

rat-type

Specifying this option includes the optional field "RAT Type" in pilot packet.

serving-nw-id

Specifying this option includes the optional field "Serving Network Identifier" in pilot packet.

name server_name

Specifies Pilot packet server name.

candidate-ip-address source_ip_address

Specifies the IP addresses for the sourcing and terminating Pilot Packets. The IP address must be entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

  • source_ip_address: Specifies the IP address of the source for sending Pilot Packets.
  • destination_ip_address: Specifies the IP address of the destination for the Pilot Packets.

destination-udp-port udp_port_value

Specifies the UDP port value as an integer from 1 through 65535.

dscp-marking dscp_value

Enables DSCP marking. DSCP is used for control plane packets.

dscp_value must be a hexadecimal number between 0x0 and 0x3F.

Important

For Pilot Packet, the generated UDP packet is currently expected to use DSCP 0x20 (32).

trigger rat-change generate { nat-info-only | user-info-and-nat-info | user-info-only }

Configures triggers for pilot packet.

  • rat-change: Enables the pilot packet trigger on RAT type change.
  • generate: Configures the generate option for rat-change trigger.
  • nat-info-only: Specifying this option sends pilot packet for only NAT IP alloc on RAT type change.
  • user-info-and-nat-info: Specifying this option sends pilot packet for both subscriber and NAT IP alloc on RAT type change.
  • user-info-only: Specifying this option sends pilot packet for only subscriber IP alloc on RAT type change.

Usage Guidelines

Use this command to configure Pilot Packet parameters.

Repeat this command to send Pilot Packets to up to four destinations.
Examples

The following command configures pilot packets with source and destination IPv4/IPv6 addresses along with the destination port:

```
pilot-packet
source-ip-address 10.2.3.4
destination-ip-address 10.3.4.5
destination-udp-port 221
```
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 a new policy.

Entering this command results in the following prompt:

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

Accounting Policy Configuration Mode commands are defined in the Accounting Policy Configuration Mode Commands chapter.

Examples

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.

**Examples**
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**

```bash
[ 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.

**Examples**

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 | renegotiation-timeout milliseconds }
no ppp { auth-retry suppress-aaa-auth | chap fixed-challenge-length | dormant send-lcp-terminate |
  lcp-authentication-discard retry-alternate num_discard | lcp-authentication-reject retry-alternate |
  lcp-start-delay | lcp-terminate connect-state | reject-peer-authentication | renegotiation retain-ip-address |
  default lcp-authentication-discard retry-alternate num_discard }
```

**default**

Restores the system defaults for the specific command/keyword.

**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.
**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

---

**chap fixed-challenge-length length**

Normally PPP CHAP use a random challenge length from 17 to 32 bytes. This command allows you to configure a specific fixed challenge length of from 4 through 32 bytes. length must be an integer from 4 through 32.

Default: Disabled. PAP/CHAP 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
Specifysthenumberofmillisecondstowaitbeforeattemptingtoretransmitcontrolpackets. 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
SpecifystheactiontobetakeniftheauthenticationoptionisrejectedduringLCPnegotiationandretriesthe allowed alternate authentication option.
Default: Disabled. No alternate authentication option will be retried.

lcp-start-delay delay
Specifysthe_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

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 PFC 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.

**Examples**

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.

Examples

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.
Examples

The following command alters the statistic "ppp successful session" so that it displays the sum of successful sessions and lcp-max-retry:

```plaintext
ppp statistics success-sessions lcp-max-retry
```

The following command disables the alteration of the statistic ppp successful session:

```plaintext
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.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>HA Proxy DNS Intercept is a license-enabled feature.</td>
</tr>
</tbody>
</table>

**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.

**Examples**

The following command creates a proxy DNS rules list named *list1* and places the CLI in the HA Proxy DNS Configuration Mode:

```
proxy-dns intercept-list list1
```
radius accounting

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 ] | deadliest 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 { deadliest | 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.

**Examples**

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.

**Examples**

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.

**Examples**
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.

Examples
The following command configures the billing-system version of RADIUS accounting servers as 10:
radius accounting billing-version 10
radius accounting gtp trigger-policy

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

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration

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.

**Examples**

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

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

This command configures the RADIUS accounting policy for 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.

**Examples**
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.

**Examples**

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

```
radius accounting interim volume total 110000
```
**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.

**Examples**

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
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.
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.

**Examples**

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.

---

**Examples**

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
```

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 plain 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 AAmgr 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.

**Examples**

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.

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

radius algorithm round-robin
radius allow

This command configures the system behavior 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.
Examples

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

`radius allow accounting-down`
radius attribute

This command configures the system's RADIUS identification parameters.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration
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 an 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

Examples

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).

Examples
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.

**Examples**
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.

**Examples**

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

```
no radius authenticator-validation
```

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

```
radius authenticator-validation
```
radius 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

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.

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.

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.

---

**Examples**

The following command specifies the IP address 192.168.100.10 as the NAS IP address, a key value of 123456 and uses the default port of 3799:

```
radius change-authorize-nas-ip 192.168.100.10 key 123456
```

The following command disables the nas-identification-check for the above parameters:

```
radius change-authorize-nas-ip 192.168.100.10 key 123456 no-nas-identification-check
```
radius charging

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.

defeadtime 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 server, the subscriber is failed once all of the configured RADIUS servers have been exhausted or once the configured number of maximum transmissions is reached.

For example, if 3 servers are configured and if the configured max-retries is 3 and max-transmissions is 12, then the primary server is tried 4 times (once plus 3 retries), the secondary server is tried 4 times, and then a third server is tried 4 times. If there is a fourth server, it is not tried because the maximum number of transmissions (12) has been reached.

**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.

**Examples**

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

```
radius charging detect-dead-server consecutive-fails 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.

**Examples**  
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 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 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.

Examples
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:

\[(\text{context}_\text{name})\text{host}_\text{name}(\text{config-ctx})\#\]

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.

Examples

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.

Examples
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.
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 StarOS 14.0 or a later release, refer to the AAA Interface Administration and Reference.

Important

Examples

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.

---

**Examples**

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 3: RADIUS Dictionary Types

<table>
<thead>
<tr>
<th>Dictionary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3gpp</td>
<td>This dictionary consists of all the attributes in the standard dictionary, and all of the attributes specified in 3GPP 32.015.</td>
</tr>
<tr>
<td>3gpp2</td>
<td>This dictionary consists of all the attributes in the standard dictionary, and all of the attributes specified in IS-835-A.</td>
</tr>
<tr>
<td>3gpp2-835</td>
<td>This dictionary consists of all the attributes in the standard dictionary, and all of the attributes specified in IS-835.</td>
</tr>
</tbody>
</table>
These are customized dictionaries. For information on custom dictionaries, contact your local service representative.

**NOTE:** RADIUS dictionary `customXX` should be used in conjunction with Active Charging Service (ACS).

`standard` is the integer of the custom dictionary.

This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC2869.

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.

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.

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.

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.

### Examples

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. See the 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.

**Examples**

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

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

This command configures the 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.

Examples
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**
Confugures 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.

**Examples**
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".

Examples
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 server, the subscriber is failed once all of the configured RADIUS servers have been exhausted, or once the configured number of maximum transmissions is reached.

  For example, if three servers are configured and if the configured max-retries is 3 and max-transmissions is 12, then the primary server is tried four times (once plus three retries), the secondary server is tried four times, and then a third server is tried four times. If there is a fourth server, it is not tried because the maximum number of transmissions (12) has been reached.

**Usage Guidelines**

Use this command to configure the maximum number of re-transmissions for RADIUS authentication requests.
Examples

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.

**Examples**

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.

**Examples**

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:

\( \text{(context_name)}host \_name (config-ctx) \# \)

**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
```

**radius probe-message local-service-address**
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.

**Examples**
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 be an 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.

Examples                      The following command sets the authentication probe timeout to 120 seconds:
                                 radius probe-timeout 120
**radius server**

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

**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.
**radius server**

**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.

**Examples**

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.

Examples

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

context_name

Entering the above command sequence results in the following prompt:

\[ \text{context_name} \text{host_name} (config-ctx) \#

Syntax Description:

radius timeout \textit{timeout_duration}

default radius timeout

default

Configures the default setting.

\textit{timeout_duration}

Specifies the time duration (in seconds) to wait for a response from the RADIUS server before resending the messages. \textit{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.

Examples: 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.

Examples
The following command enables RADIUS trigger for RAT change:

radius trigger rat-change
**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}host_name(config-remote-server-list)#
```

Remote Server List Configuration Mode commands are defined in the remote Server List Configuration Mode Commands chapter.

**Examples**

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.

**Examples**

Use the following command to create an extended route-access-list:

```
route-access-list extended 100 permit ip 192.168.100.0 0.0.0.255
```
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 10.1.1.1/24).

- **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.

**Examples**

Use the following command to create a route access list named `list27` that permits routes that match `192.168.1.0/24` exactly:

```
route-access-list named list27 permit 192.168.1.0/24 exact-match
```

To delete the list, use the following command:

```
no route-access-list named list27 permit 192.168.1.0/24 exact-match
```
route-access-list standard

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 having 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.

Examples
Use the following command to create a route access list with an identifier of 10 that permits routes:

```
route-access-list standard 10 permit 192.168.1.0 255.255.255.0
```

To delete the list, use the following command:

```
noroute-access-list standard 10 permit 192.168.1.0 255.255.255.0
```
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.

Examples

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.

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.

Examples
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
```
Context Configuration Mode Commands S-Z

This section includes the commands **s102-service** through **wsg-service** service.

**Command Modes**

Exec > 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, page 943
- saegw-service, page 945
- sbc-service, page 947
- server, page 948
- service-redundancy-protocol, page 950
- session-event-module, page 951
- sgsn-service, page 952
- sgs-service, page 954
- sgtp-service, page 956
- sgw-service, page 958
- sls-service, page 960
- ssh, page 962
- ssl, page 964
- subscriber, page 965
• threshold available-ip-pool-group, page 967
• threshold ha-service init-rrq-rcvd-rate, page 969
• threshold ip-pool-free, page 971
• threshold ip-pool-hold, page 973
• threshold ip-pool-release, page 975
• threshold ip-pool-used, page 977
• threshold monitoring, page 979
• threshold pdsn-service init-rrq-rcvd-rate, page 981
• twan-profile, page 983
• udr-module active-charging-service, page 984
• wsg-service, page 985
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.
Examples

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.
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.

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.

**Examples**

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.

**Examples**  
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

```console
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```console
(context_name)host_name(config-ctx)#
```

**Syntax Description**

```console
server { ftpd | named | sshd | telnetd | tftpd }
no server { ftpd | named | sshd | telnetd | tftpd } [ kill ]

no

Disables the specified service.

```console
ftpd
```

Enters the FTP Server Configuration Mode.

---

**Important**

The FTPD server can only be configured in the local context.

---

**Caution**

For maximum system security, you should **not** enable FTP functionality. SFTP is the recommended file transfer protocol.

```console
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.

---

**telnetsd**

Enters the Telnet Server Configuration Mode.

---

**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 TFTP 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`, `telnetsd`, 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.

---

**Examples**

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.

**Examples**

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.

<table>
<thead>
<tr>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-GW</td>
</tr>
<tr>
<td>SAEGW</td>
</tr>
<tr>
<td>S-GW</td>
</tr>
<tr>
<td>SGSN</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exec &gt; Global Configuration &gt; Context Configuration</td>
</tr>
<tr>
<td>configure &gt; context context_name</td>
</tr>
</tbody>
</table>

Entering the above command sequence results in the following prompt:

```
[context_name] hostname(config-ctx)#
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ no ] session-event-module</td>
</tr>
</tbody>
</table>

```
no
```

Disables the event module configuration.

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

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.
Examples

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.

Examples

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]host_name(config-sgtp-service)#
    ```

**Examples**
- 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:

```plaintext
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.
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.

**Examples**

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 *sgw-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>hostname(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.

**Examples**

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
```
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 } }

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 the 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 concealed 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.

**Examples**

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)hostname(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(config-ctx-ssl-subscriber-template)#

SSL Template Configuration Mode commands are defined in the SSL Template Configuration Mode Commands chapter.

Examples

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.
A maximum of 128 subscribers and/or administrative users may be locally configured per context.

**Examples**

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
```
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 \( \leq \) Low Threshold
- **Clear Condition**: Actual IP address utilization percentage per pool group \( > \) High Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

The following table describes the possible methods for configuring IP pool utilization thresholds:

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context-level</td>
<td>A single IP pool utilization threshold can be configured for all IP pool groups within a given system context. If a single threshold is configured for all pool groups, separate alerts or alarms can be generated for each group. This command configures that threshold.</td>
</tr>
<tr>
<td>IP address pool-level</td>
<td>Each individual IP address pool can be configured with its own threshold. Thresholds configured for individual pools take precedence over the context-level threshold that would otherwise be applied (if configured). In the event that two IP address pools belonging to the same pool group are configured with different thresholds, the system uses the pool configuration that has the greatest low threshold for that group.</td>
</tr>
</tbody>
</table>

**Examples**

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:

```plaintext
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

**Examples**

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.

**Examples**

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.

**Examples**
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:

```plaintext
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 in 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.

---

**Examples**

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 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 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.

**Examples**
The following command configures a context-level IP pool percentage of IP addresses that are used high threshold percentage of 35 and a low threshold of 10 for an system using the Alarm thresholding model:

```
threshold ip-pool-used 35 clear 10
```
threshold monitoring

Enables 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 5: Thresholding Reporting Mechanisms by Model*

<table>
<thead>
<tr>
<th>Model</th>
<th>SNMP Traps</th>
<th>Logs</th>
<th>Alarm System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

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.

**Examples**

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

**Examples**

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.

---

**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
```

**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)#
```

**Examples**
The following command creates the UDR module for the context, and enters the UDR Module Configuration Mode:

```
udr-module active-charging-service
```
**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.

**Examples**

The following command enters the WSG Service Configuration Mode:

`wsg-service wsg01`
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, page 990
- app-level-retransmission, page 991
- associate, page 992
- charging-rulebase-name, page 994
- diameter dictionary, page 996
- diameter disable-final-reporting-in-ccru, page 998
- diameter dynamic-rules request-quota, page 1000
- diameter enable-quota-retry, page 1001
- diameter exclude-msce-in-ccr-terminate, page 1002
- diameter fui-redirected-flow, page 1003
- diameter gsu-with-only-infinite-quota, page 1004
- diameter hdd, page 1005
- diameter ignore-returned-rulebase-id, page 1007
• diameter ignore-service-id, page 1008
• diameter mscc-final-unit-action terminate, page 1009
• diameter mscc-per-ccr-update, page 1011
• diameter msg-type, page 1013
• diameter origin host, page 1016
• diameter origin endpoint, page 1017
• diameter peer-select, page 1018
• diameter pending-timeout, page 1021
• diameter reauth-blacklisted-content, page 1023
• diameter redirect-url-token, page 1025
• diameter redirect-validity-timer, page 1027
• diameter result-code, page 1029
• diameter send-ccri, page 1031
• diameter service-context-id, page 1033
• diameter session failover, page 1034
• diameter update-dictionary-avps, page 1036
• end, page 1038
• event-based-session, page 1039
• exit, page 1041
• failure-handling, page 1042
• gy-rf-trigger-type, page 1046
• imsi-imeisv-encode-format, page 1048
• mode, page 1049
• pending-traffic-treatment, page 1050
• quota, page 1053
• quota request-trigger, page 1054
• quota time-threshold, page 1056
• quota units-threshold, page 1057
• quota volume-threshold, page 1059
• radius usage-reporting-algorithm, page 1061
• redirect-indicator-received, page 1062
• redirect-require-user-agent, page 1064
• servers-unreachable, page 1065
- subscription-id service-type, page 1071
- timestamp-rounding, page 1073
- trigger type, page 1075
- usage-reporting, page 1077
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.

Examples

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.

**Examples**

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.

Examples

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.
Examples

The following command defines a charging rulebase name called `rb1` in the credit control group:

```
charging-rulebase-name rb1
```
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**

```
```

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.

**Examples**
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.

---

**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.

---

**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 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.

**Examples**

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.

**Examples**

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 blacklisted 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 blacklisted 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 blacklisted 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.

Examples

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.

**Examples**  
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

```plaintext
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 appear in the output of the `show configuration` command.

**Examples**

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-chargingservice 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.

**Examples**

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.
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.

**Examples**

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.

**Examples**

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

**Syntax Description**

<table>
<thead>
<tr>
<th>default</th>
<th>no</th>
<th>diameter ignore-service-id</th>
</tr>
</thead>
</table>

**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.

**Examples**

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
```

- **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.

**Examples**
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.
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
```

**Important**

This default behavior is applicable to all dictionaries except for dcca-custom12 and dcca-custom13 dictionaries. In the case of dcca-custom12 and dcca-custom13, the FINAL reporting will always be sent in CCR-T even if MSCC is in FUI Redirect/Restrict-access state 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 ccru 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 ccrt 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.
This feature is available only in 18.3, 19.2 and later releases.

**Important**

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.

**Examples**

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 1017 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.

**Examples**

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:

\[
\text{diameter peer-select peer peer\_name [ realm realm\_name ] | [ secondary-peer secondary\_peer\_name [ realm realm\_name ] | [ imsi-based start-value imsi\_start\_value end-value imsi\_end\_value ] | no diameter peer-select [ imsi-based start-value imsi\_start\_value end-value imsi\_end\_value ]}
\]

In 9.0 and later releases, for UMTS deployments:

\[
\text{diameter peer-select peer peer\_name [ realm realm\_name ] | [ secondary-peer secondary\_peer\_name [ realm realm\_name ] | [ imsi-based { { prefix | suffix } imsi/prefix/suffix\_start\_value } | to imsi/prefix/suffix\_end\_value ] | [ msisdn-based { { prefix | suffix } msisdn-based/prefix/suffix\_start\_value } | to msisdn-based/prefix/suffix\_end\_value ] ] | no diameter peer-select [ imsi-based { { prefix | suffix } imsi/prefix/suffix\_start\_value } | to imsi/prefix/suffix\_end\_value ] | [ msisdn-based { { prefix | suffix } msisdn-based/prefix/suffix\_start\_value } | to msisdn-based/prefix/suffix\_end\_value ] ]}
\]

**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 ims_start_value** specifies the start of range in integer value of IMSI, and **end-value ims_end_value** specifies the end of range in integer value of IMSI.

**imsi-based { { prefix | suffix } ims/prefix/suffix_start_value } [ to ims/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 **r_diameter-sessionfailover.xml** 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.

**Examples**

The following command configures a Diameter credit control peer named `test` and the realm `companyx`:

```bash
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:

```bash
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:

```bash
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 "deciseconds" 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 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 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 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.

Examples

The following command configures a Diameter Credit Control Pending Timeout setting of 20 seconds:

diameter pending-timeout 20
**diameter reauth-blacklisted-content**

This command allows reauthorization of blacklisted 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**
- `diameter reauth-blacklisted-content [content-based-rar]`
- `no diameter reauth-blacklisted-content`

`no`

Configures this command with the default setting. That means, the reauthorization of blacklisted RG will not happen.

`content-based-rar`

Reauthorizes blacklisted RG only when RG specific RAR is received.

**Usage Guidelines**

The current Gy implementation does not allow reauthorization of Blacklisted 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 blacklisted RG only when RG specific RAR is received.
- to reauthorize blacklisted RG on any kind of RAR (both RG specific or generic)
do not reauthorize blacklisted 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:

- 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:

- 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.

**Examples**

The following command enables reauthorization of blacklisted content on receiving RG specific RAR:

`diameter reauth-blacklisted-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.

For example:

When the original URL was http://homepage/

OCS provided URL:

```
```

The text in bold in the following sample indicates the current configuration for implementing the dynamic AoC redirection.

```
```

**Examples**

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 matching traffic. 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.
Examples

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.

Examples
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

**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.

Examples  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:

```plaintext
[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.

**Examples**

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/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 1042 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.
Examples

The following command enables Diameter Credit Control Session Failover:

```
diameter session failover
```
**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 } |
  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.
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.

Examples

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

\[ \text{no} \] 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.

**Examples**

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 ]
```

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.

<table>
<thead>
<tr>
<th>CCFH Setting</th>
<th>CLI Command</th>
<th>Behavior at Tx</th>
<th>Behavior at RT</th>
<th>Secondary is Up</th>
<th>Secondary is Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial-request Message Type</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continue</td>
<td>initial-request continue</td>
<td>N/A</td>
<td>Continue</td>
<td>Secondary takes over after RT</td>
<td>Offline after another RT. No more quota requests are performed for any rating group within the session after DCCA failure (even if connectivity to DCCA is restored)</td>
</tr>
</tbody>
</table>
### Credit Control Configuration Mode Commands

#### Failure-handling

<table>
<thead>
<tr>
<th>CCFH Setting</th>
<th>CLI Command</th>
<th>Behavior at Tx</th>
<th>Behavior at RT</th>
<th>Secondary is Up</th>
<th>Secondary is Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>initial-request</td>
<td>continue</td>
<td>Offline</td>
<td>N/A</td>
<td>Offline at Tx</td>
<td>Offline at Tx</td>
</tr>
<tr>
<td>Retry-and-terminate</td>
<td>initial-request</td>
<td>Continue</td>
<td>N/A</td>
<td>Secondary takes over after Tx</td>
<td>Offline after another Tx</td>
</tr>
<tr>
<td>Terminate</td>
<td>initial-request</td>
<td>Terminate</td>
<td>N/A</td>
<td>Terminate after Tx</td>
<td>Terminate after Tx</td>
</tr>
</tbody>
</table>

#### Update-request Message Type

| Continue | update-request | N/A | Continue | Secondary takes over after RT | Offline after another RT |
| Retry-and-terminate | update-request | Offline | N/A | Offline at Tx | Offline at Tx |
| Terminate | update-request | Terminate | N/A | Sends CCR-T after another Tx | Sends CCR-T after another Tx |

#### Terminate-request Message Type

<p>| Continue | terminate-request | N/A | Retry | CCR-T is sent to secondary after RT | Terminate after another RT |</p>
<table>
<thead>
<tr>
<th>CCFH Setting</th>
<th>CLI Command</th>
<th>Behavior at Tx</th>
<th>Behavior at RT</th>
<th>Secondary is Up</th>
<th>Secondary is Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>terminate-request continue go-offline-after-expiry</td>
<td>Retry</td>
<td>N/A</td>
<td>CCR-T is sent to secondary after Tx</td>
<td>Terminate after another Tx</td>
<td></td>
</tr>
<tr>
<td>terminate-request continue retry-after-expiry</td>
<td>Retry</td>
<td>N/A</td>
<td>CCR-T is sent to secondary after Tx</td>
<td>Terminate after another Tx</td>
<td></td>
</tr>
<tr>
<td>Retry-and-Terminate</td>
<td>terminate-request retry-and-terminate</td>
<td>N/A</td>
<td>Retry</td>
<td>CCR-T is sent to secondary after RT</td>
<td>Terminate after another RT</td>
</tr>
<tr>
<td>retry-and-terminate</td>
<td>terminate-request retry-and-terminate</td>
<td>N/A</td>
<td>Retry</td>
<td>CCR-T is sent to secondary after Tx</td>
<td>Terminate after another Tx</td>
</tr>
<tr>
<td>Terminate</td>
<td>terminate-request terminate</td>
<td>Terminate</td>
<td>N/A</td>
<td>Terminate after Tx</td>
<td>Terminate after Tx</td>
</tr>
</tbody>
</table>

**Examples**

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.

Examples
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.

<table>
<thead>
<tr>
<th>Product</th>
<th>GGSN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>HA</td>
</tr>
<tr>
<td></td>
<td>IPSG</td>
</tr>
<tr>
<td></td>
<td>PDSN</td>
</tr>
<tr>
<td></td>
<td>P-GW</td>
</tr>
</tbody>
</table>

| Privilege        | Security Administrator, Administrator |

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Exec &gt; ACS Configuration &gt; Credit Control Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>active-charging</td>
<td>service service_name &gt; credit-control</td>
</tr>
<tr>
<td></td>
<td>Entering the above command sequence results in the following prompt:</td>
</tr>
<tr>
<td></td>
<td>[local] host_name(config-dcca)#</td>
</tr>
</tbody>
</table>

**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.

**Examples**

The following command specifies the encoding format of IMSI/IMEISV as ASCII:

```plaintext
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.

`radius`

Enables RADIUS Credit Control for prepaid charging.

**Usage Guidelines**

Use this command to configure the prepaid charging application mode to Diameter or RADIUS credit control.

**Examples**

The following command specifies to use RADIUS prepaid credit control application:

```
mode radius
```
pending-traffic-treatment

This command controls the pass/drop treatment of traffic while waiting for definitive credit information from the server.

**Product**

All

**Privilege**

Security Administrator, Administrator

**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-exhausted**. 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.
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 holding_time | validity-time validity_time }
{ default | no } quota { holding-time | validity-time }

holding-time holding_time
```

Specifies the Quota Holding Time (QHT) in seconds. The value must be an integer from 1 through 4000000000.

```
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.

**Examples**

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.
Examples

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.

Examples

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.
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.
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.

**Examples**

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.
Examples

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
```

**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-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 ] }.
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 | terminate [ after-timer-expiry `timeout_period` ] server-retries `retry_count` | 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 | } server-retries retry_count | } server-retries retry_count | } server-retries retry_count | | after-quota-expiry | after-timer-expiry timeout_period | } server-retries retry_count | } server-retries retry_count | | after-quota-expiry | after-timer-expiry timeout_period | } server-retries retry_count | | after-quota-expiry | after-timer-expiry timeout_period | }

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.

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.

**Examples**

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

**Syntax Description**
```
subscription-id service-type { closedrp | ggsn | ha | ipsg | l2tplls | mipv6ha | pdsn | pgw } { e164 | imsi | nai }

| no | subscription-id service-type { closedrp | ggsn | ha | ipsg | l2tplls | mipv6ha | pdsn | pgw }

default
Configures the default timestamp-rounding setting.
Default: floor
```

closedrp | ggsn | ha | ipsg | l2tplls | 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.

Examples

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).
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.

Examples
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

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.

Examples
The following command configures to report usage based only on granted quota:
usage-reporting quotas-to-report based-on-grant
usage-reporting
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, page 1080
- diameter endpoint, page 1081
- end, page 1082
- exit, page 1083
- failure-handling, page 1084
- request timeout, page 1086
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.

**Examples**

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.

**Examples**

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

**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.
action { continue | retry-and-continue | retry-and-terminate | terminate }

Specifies the failure handling action.

**continue**: Continue the session without credit control.

**retry-and-continue**: Retry and, even if credit control is not available, continue.

**retry-and-terminate**: Retry and then terminate.

**terminate**: Terminate the session.

**Usage Guidelines**

Use this command to configure the Diameter failure handling behavior.

**Examples**

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).

Examples

The following command configures the timeout period to 150 seconds:

request timeout 150
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, page 1088
- exit, page 1089
- match address, page 1090
- match ip pool, page 1092
- switchover, page 1094
**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.

**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.

**Examples**

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

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-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.

**Examples**
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.

**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.

**Examples**

The following command disables the automatic secondary-to-primary switchover:

```
switchover auto do-not-revert
```
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.

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.

### 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)#
```

*Important*

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

- `end`, page 1098
- `exit`, page 1099
- `set`, page 1100
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.

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 nat | 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 | 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 AGGRESSIVE 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.

*transform_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.

**Examples**

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
```
set
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, page 1106
- exit, page 1107
- replay window-size, page 1108
- transform-set, page 1110
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**

Configure 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.

**Examples**

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 string 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 Security 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 protocol to use for securing communications.

**Examples**

The following command specifies the use of IPSec AH with HMAC = MD5.

crypto ipsec transform-set tset013 ah hmac md5-96
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.

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)#

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

- end, page 1115
- exit, page 1116
- match address, page 1117
- set control-dont-fragment, page 1119
- set ip mtu, page 1121
- set ipv6 mtu, page 1123
- set peer, page 1125
- set session-key, page 1127
- set transform-set, page 1130
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

dend

Usage Guidelines

Use this command to return to the Exec mode.
exit

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

exit

Usage Guidelines

Use this command to return to the parent configuration mode.
**match address**

Matches or associates the crypto map to an access control list (ACL) configured in the same context.

**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.

**Examples**

The following command sets the crypto map ACL to the ACL named *ACLlist1* and sets the crypto maps priority to the highest level.

```
match address ACLlist1 0
```
set control-dont-fragment

Controls the Don't Fragment (DF) bit in the outer IP header of the IPSec tunnel data packet.

**Product**
- 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.

Examples
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
```

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.

**Examples**

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

**Examples**

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.

**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.

Examples

The following command configures a security gateway address of 192.168.1.100 for the crypto map with which to establish a tunnel.

set peer 192.168.1.100
set session-key

Configures session key parameters for the manual crypto map.

**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**

```plaintext
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.

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.

**Examples**

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 \textit{sd23r9skd0fi3as}.
- Authentication key is \textit{sfd23408imi9yn}.

\texttt{set session-key outbound esp 310 cipher sd23r9skd0fi3as authenticator sfd23408imi9yn}
set transform-set

Configures the name of a transform set that the crypto map is associated with.

**Product**
- 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.

**Examples**

The following command associates a transform set named `esp_tset` with the crypto map:

```
set transform-set esp_tset
```
set transform-set
Crypto Map IKEv2-IPv4 Configuration Mode Commands

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.

Command Modes

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, page 1135
- authentication, page 1136
- blacklist, page 1138
- ca-certificate list, page 1139
- ca-crl list, page 1141
- certificate, page 1143
- control-dont-fragment, page 1145
- end, page 1147
- exit, page 1148
- ikev2-ikesa, page 1149
- keepalive, page 1152
- match, page 1154
- natt, page 1156
- ocsp, page 1157
- payload, page 1159
- peer, page 1161
- remote-secret-list, page 1163
- whitelist, page 1164
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

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.

Examples
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.

**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 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.

Examples
The following command sets the authentication method to an open key value of 6d7970617373776f7264:
```
authentication pre-shared-key key 6d7970617373776f7264
```
blacklist

Enables or disables a blacklist (access denied) for this map.

Product

All products supporting IPSec blacklisting

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] blacklist

no

Disables blacklisting for this crypto map. By default blacklisting is disabled.

Usage Guidelines

Use this command to enable blacklisting for this crypto map. A blacklist is a list or register of entities that are denied a particular privilege, service, mobility, access or recognition. With blacklisting, any peer is allowed to connect as long as it does not appear in the list. For additional information on blacklisting, refer to the System Administration Guide.

Examples

The following command enables blacklisting:

blacklist
ca-certificate list

Used to bind an X.509 Certificate Authority (CA) certificate to a crypto map.

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.

crert-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.
Examples

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.

**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.

Examples
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.

**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.
Examples

Use the following example to prevent a certificate from being included in the Auth Exchange payload:

no certificate
control-dont-fragment

Controls the Don't Fragment (DF) bit in the outer IP header of the IPSec tunnel data packet.

Product

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).
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.

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.
ikey2-ikesa

Configures parameters for the IKEv2 IKE Security Associations within this crypto template.

<table>
<thead>
<tr>
<th>Product</th>
<th>ePDG</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FA</td>
</tr>
<tr>
<td></td>
<td>GGSN</td>
</tr>
<tr>
<td></td>
<td>HA</td>
</tr>
<tr>
<td></td>
<td>HeNBGW</td>
</tr>
<tr>
<td></td>
<td>HNBGW</td>
</tr>
<tr>
<td></td>
<td>HSGW</td>
</tr>
<tr>
<td></td>
<td>MME</td>
</tr>
<tr>
<td></td>
<td>P-GW</td>
</tr>
<tr>
<td></td>
<td>PDSN</td>
</tr>
<tr>
<td></td>
<td>S-GW</td>
</tr>
<tr>
<td></td>
<td>SAEGW</td>
</tr>
<tr>
<td></td>
<td>SCM</td>
</tr>
<tr>
<td></td>
<td>SecGW</td>
</tr>
<tr>
<td></td>
<td>SGSN</td>
</tr>
</tbody>
</table>

**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 ikey2-ikesa { allow-empty-ikesa | max-retransmissions | policy error-notification | rekey | disallow-param-change | setup-timer }

no ikey2-ikesa { allow-empty-ikesa name | policy { error-notification | use-rfc5996-notification } | rekey sec | transform-set list }

no ikey2-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-major-version | invalid-syntax | 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 CHILD_SA_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.

**Examples**

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.

**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.

Examples
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.

**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.

**Examples**
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**

```plaintext
[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.

**Examples**

The following command disables NAT-T for this crypto template:

```plaintext
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.

**Examples**

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.

## 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.

Examples

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.

**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.
Examples

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 through 127 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.

**Examples**

The following command enables a remote-secret-list named *rs-list*:

remote-secret-list rs-list
whitelist

Enables or disables a whitelist (access granted) for this crypto map.

Product

All products supporting IPSec whitelisting

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 ] whitelist

no

Disables whitelisting for this crypto map. By default whitelisting is disabled.

Usage Guidelines

Use this command to enable whitelisting for this crypto map. A whitelist is a list or register of entities that are being provided a particular privilege, service, mobility, access or recognition. With whitelisting, no peer is allowed to connect unless it appears in the list. For additional information on whitelisting, refer to the System Administration Guide.

Examples

The following command enables whitelisting:

whitelist
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.

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).

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)#
```

Important

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

- `end`, page 1166
- `exit`, page 1167
- `match address`, page 1168
- `match crypto group`, page 1170
- `match ip pool`, page 1172
- `set`, page 1174
**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.

<table>
<thead>
<tr>
<th>Product</th>
<th>ePDG</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FA</td>
</tr>
<tr>
<td></td>
<td>GGSN</td>
</tr>
<tr>
<td></td>
<td>HA</td>
</tr>
<tr>
<td></td>
<td>HeNBGW</td>
</tr>
<tr>
<td></td>
<td>HNBGW</td>
</tr>
<tr>
<td></td>
<td>HSGW</td>
</tr>
<tr>
<td></td>
<td>MME</td>
</tr>
<tr>
<td></td>
<td>P-GW</td>
</tr>
<tr>
<td></td>
<td>PDSN</td>
</tr>
<tr>
<td></td>
<td>S-GW</td>
</tr>
<tr>
<td></td>
<td>SAEGW</td>
</tr>
<tr>
<td></td>
<td>SCM</td>
</tr>
<tr>
<td></td>
<td>SecGW</td>
</tr>
<tr>
<td></td>
<td>SGSN</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>The priorities are only compared for ACLs matched to other crypto maps or to policy ACLs (those applied to the entire context).</td>
</tr>
</tbody>
</table>

**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.

**Examples**

The following command sets the crypto map ACL to the ACL named `ACLlist1` and sets the crypto maps priority to the highest level.

```plaintext
match address ACLlist1 0
```
# match crypto group

Matches or associates the crypto map a crypto group configured in the same context.

## 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.

**Examples**

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**

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 pool that 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 IPv6 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 an 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.

**Examples**
The following command sets a rule for the current crypto map that will match an IP pool named `ippool1`:

```
mcast ip pool pool-name ippool1
```
set

Configures parameters for the dynamic crypto map.

**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 nat | 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 nat | keepalive time |
Specifies IKE parameters.

nat: 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 AGGRESSIVE 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.

Examples

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
```
set
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, page 1180
- exit, page 1181
- ipsec, page 1182
- lifetime, page 1183
- rekey, page 1185
**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.

| 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 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.

Examples

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.

**Product**
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

**Privilege**
- Security Administrator

**Syntax Description**

```bash
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 \textit{kbytes}\\
Specifies lifetime in kilobytes for IPSec Child Security Associations derived from this Crypto Map. \textit{kbytes} must be an integer from 1 through 2147483648.

\textbf{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.

\textbf{Examples}\\
The following command configures the IPSec child SA lifetime to be 120 seconds:\
\texttt{lifetime 120}
rekey

Configures child security association rekeying.

**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 rekeying.

**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.
Examples

The following command disables rekeying:

```
no rekey
```
Crypto Map IKEv2-IPv6 Configuration Mode Commands

The Crypto Map IKEv2-IPv6 Configuration Mode is used to configure an IKEv2 IPsec policy for secure X3 interface tunneling between a P-GW and a lawful intercept server.

**Exec > 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, page 1189
- authentication, page 1190
- blacklist, page 1192
- ca-certificate list, page 1193
- ca-crl list, page 1195
- certificate, page 1197
- control-dont-fragment, page 1199
- end, page 1201
- exit, page 1202
- ikev2-ikesa, page 1203
- keepalive, page 1206
- match, page 1208
• ocs, page 1210
• payload, page 1212
• peer, page 1214
• remote-secret-list, page 1216
• whitelist, page 1217
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

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.

Examples
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.

**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.

**Examples**

The following command sets the authentication method to an open key value of `6d7970617373776f7264`:

```
authentication pre-shared-key key 6d7970617373776f7264
```
blacklist

Enables or disables a blacklist (access denied) for this map.

Product

All products supporting IPSec blacklisting

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 ] blacklist

no

Disables blacklisting for this crypto map. By default blacklisting is disabled.

Usage Guidelines

Use this command to enable blacklisting for this crypto map. A blacklist is a list or register of entities that are denied a particular privilege, service, mobility, access or recognition. With blacklisting, any peer is allowed to connect as long as it does not appear in the list. For additional information on blacklisting, refer to the System Administration Guide.

Examples

The following command enables blacklisting:

blacklist
ca-certificate list

Used to bind an X.509 Certificate Authority (CA) certificate list to a crypto template.

**Product**
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

**Privilege**
- Security Administrator

**Syntax Description**

certificate list 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 crypto map.

certificate-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.

Examples

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.

<table>
<thead>
<tr>
<th>Product</th>
<th>ePDG</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FA</td>
</tr>
<tr>
<td></td>
<td>GGSN</td>
</tr>
<tr>
<td></td>
<td>HA</td>
</tr>
<tr>
<td></td>
<td>HeNBGW</td>
</tr>
<tr>
<td></td>
<td>HNBGW</td>
</tr>
<tr>
<td></td>
<td>HSGW</td>
</tr>
<tr>
<td></td>
<td>MME</td>
</tr>
<tr>
<td></td>
<td>P-GW</td>
</tr>
<tr>
<td></td>
<td>PDSN</td>
</tr>
<tr>
<td></td>
<td>S-GW</td>
</tr>
<tr>
<td></td>
<td>SAEGW</td>
</tr>
<tr>
<td></td>
<td>SCM</td>
</tr>
<tr>
<td></td>
<td>SecGW</td>
</tr>
<tr>
<td></td>
<td>SGSN</td>
</tr>
</tbody>
</table>

| Privilege | Security Administrator |

**Syntax Description**

```bash
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.

Examples 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.

**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.

**Examples**

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.

**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.

Examples
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.

**Product**
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBBGW
- 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.

Examples

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.

**Product**
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

**Privilege**
- Security Administrator, Administrator

**Syntax Description**

```plaintext
keepalive [ interval sec ] [ timeout ] [ 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.

Examples

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.

**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.

**Examples**  
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.

**Examples**

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**
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 `ipv-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.

**Examples**

The following command configures a crypto template payload called `payload5` and enters the Crypto Template IKEv2-IPv6 Payload Configuration Mode:

```
payload payload5 match ipv6
```
peer

Configures the IP address of a peer IPSec server.

**Product**
- 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.
Examples

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 through 127 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.

**Examples**
The following command enables a remote-secret-list named `rs-list`:

`remote-secret-list rs-list`
**whitelist**

Enables or disables a whitelist (access granted) for this crypto map.

**Product**

All products supporting IPSec whitelisting

**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 ] whitelist

- **no**
  
  Disables whitelisting for this crypto map. By default whitelisting is disabled.

**Usage Guidelines**

Use this command to enable whitelisting for this crypto map. A whitelist is a list or register of entities that are being provided a particular privilege, service, mobility, access or recognition. With whitelisting, no peer is allowed to connect unless it appears in the list. For additional information on whitelisting, refer to the *System Administration Guide*.

**Examples**

The following command enables whitelisting:

whitelist
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

```plaintext
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, page 1220
- exit, page 1221
- ipsec, page 1222
- lifetime, page 1224
- rekey, page 1226
**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.

**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 | [ 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 set to 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.

Examples

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.

**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

```bash
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.

Examples
The following command configures the IPSec child SA lifetime to be 120 seconds:
lifetime 120
**rekey**

Configures child security association rekeying.

**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.

#### Examples

The following command disables rekeying:

```bash
no rekey
```
rekey
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, page 1231
- allow-custom-fqdn-idr, page 1232
- authentication, page 1233
- blacklist, page 1235
- ca-certificate list, page 1236
- ca-crl list, page 1237
- certificate, page 1238
- configuration-payload, page 1239
- control-dont-fragment, page 1240
- dns-handling, page 1241
- dos cookie-challenge notify-payload, page 1243
- end, page 1245
• exit, page 1246
• identity local, page 1247
• ikev2-ikesa, page 1248
• ip, page 1251
• ipv6, page 1253
• keepalive, page 1254
• max-childsa, page 1255
• nai, page 1256
• natt, page 1258
• notify-payload, page 1259
• ocsp, page 1261
• payload, page 1263
• peer network, page 1265
• remote-secret-list, page 1266
• timeout, page 1267
• whitelist, page 1268
**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

**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.

**Examples**
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.

**Examples**

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 } | 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 | pre-shared-key }
```

default authentication

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.

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.

Examples

The following command enables authentication via an EAP profile named eap23 for subscribers using the service with this crypto template:

authentication eap-profile eap23
blacklist

Enables the use of a blacklist (access denied) file to be used by a security gateway.

**Product**
All products supporting IPSec blacklisting

---

**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 ] blacklist

**no**
Disables the use of a blacklist.

---

**Usage Guidelines**
Enable the use of a previously created blacklist to deny access to prohibited peers via a security gateway. A blacklist is a list or register of entities that are being denied a particular privilege, service, mobility, access or recognition. With blacklisting, any peer is allowed to connect as long as it does not appear in the list. Each entry in the blacklist 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.

---

**Examples**
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 ] no ca-certificate

no
Unbinds the ca-certificate(s) bound to the crypto template.

c-aert-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.

Examples
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.

**Examples**

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.

**Examples**
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 default value for mapping of the configuration payload attributes.

private-attribute-type
Defines the private payload attribute.

imei integer
Defines an International Mobile Equipment 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.

Examples
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.

**Examples**

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 prescribed circumstances described below.

**Product**
PDIF

**Privilege**
Security Administrator

**Syntax Description**
```bash
{ 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).

Examples

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**

```plaintext
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.
Examples

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
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
```

**id-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.

**Examples**

The following command configures the local IPSec Client.

```bash
identity local id-type der-ans1-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 } | ignore-notify-protocol-id |
ignore-rekeying-requests | keepalive-user-activity | max-retransmissions number | policy {
congestion-rejection { notify-status-value value } | error-notification | invalid-major-version |
invalid-message-id | invalid-maj"or-version | invalid-syntax | invalid-maj"or-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 | 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 | ignore-notify-protocol-id | ignore-rekeying-requests |
| keepalive-user-activity | list name | mobike | policy error-notification | rekey }

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.

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
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

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.

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 ... name6**

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.

### Examples

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
```
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-tmpl-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.

Examples

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
```

`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.

**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.

**Examples**

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.

**Examples**
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.

Examples

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

\[\text{nai } \{ \text{idr name [id-type \{ der-asn1-dn | der-asn1-gn | fqdn | ip-addr | key-id | rfc822-addr \} ] | use-received-idr \} \} \]

\[\text{default nai idr} \]

\[\text{no nai } \{ \text{idr | use-received-idr} \} \]

\[\text{default} \]

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.

\[\text{no} \]

**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.

\[\text{idr name} \]

Specifies the name of the IDr crypto template as an alphanumeric string of 1 through 79 characters.

\[\text{id-type \{ der-asn1-dn | der-asn1-gn | fqdn | ip-addr | key-id | rfc822-addr \} } \]

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.

**Examples**

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.

**Product**

All Security Gateway products

**Privilege**

Security Administrator

**Syntax Description**

```plaintext
[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.

```plaintext
no
```

Disables NAT-T for all security associations associated with this crypto template.

```plaintext
include-header
```

Includes the NAT-T header in IPSec packets.

```plaintext
send-keepalive | idle-interval idle_secs | [ interval interval_secs ]
```

Sends NAT-Traversal keepalive messages.

```plaintext
id-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.
```

```plaintext
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.

**Examples**

The following command disables NAT-T for this crypto template:

```plaintext
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-tmpl-ikev2-tunnel)#

default notify-payload error-message-type { network-permanent | network-transient-major | network-transient-minor | ue } base value

default
Sets / restores default value assigned for the parameters to be sent in NOTIFY payload.

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.

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.
Examples

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 [port_value]]]
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.

**Examples**

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.

**Examples**

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**

```plaintext
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` | `encrypted pre-shared-key encrypt_key` | `pre-shared-key key`

Specifies the IP address of the peer network in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

`/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.

**Examples**

The following command configures a set of IP addresses with starting address of 10.2.3.4 and a bit mask of 8:

```plaintext
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 through 127 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.

Examples

The following command enables a remote-secret-list named rs-list:

remote-secret-list rs-list
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.

**Examples**

The following command configures Certificate Server timeout as 50 seconds:

```
timeout cert-server 50
```
whitelist

Enables the use of an existing whitelist (access permitted) file by a security gateway.

**Product**  
All products supporting IPSec whitelisting

**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**  

```plaintext
[ no ] whitelist
```

- **no**  
  Disables the use of a whitelist.

**Usage Guidelines**  
Enable the use of a previously created whitelist to allow privileged peers access via a security gateway.

A whitelist is a list or register of entities that are being provided a particular privilege, service, mobility, access or recognition. With whitelisting, no peer is allowed to connect unless it appears in the list.

Each entry in the whitelist 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.

**Examples**  
The following command enables the use of a whitelist:

```plaintext
whitelist
```
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, page 1271
- exit, page 1272
- ignore-rekeying-requests, page 1273
- ip-address-allocation, page 1274
- ipsec transform-set, page 1276
- lifetime, page 1277
- maximum-child-sa, page 1278
- rekey, page 1279
- tsi, page 1280
- tsr, page 1281
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.

**Examples**
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.

**Examples**
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

```plaintext
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:

```plaintext
{context_name}@host_name (cfg-crypto-tmpl-ikev2-tunnel-payload)#
```

**Syntax Description**

```plaintext
[ 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 alphanumerical 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 alphanumerical 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.

**Examples**

The following command configures IPSec transform sets named *ipset1* and *ipset2* to be used in this crypto template payload:

```plaintext
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.

**Examples**

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.

Examples
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

```plaintext
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.

**Examples**
The following command disables rekeying:

```plaintext
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

```
create > 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.

Examples
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.

Examples

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
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, page 1284
- exit, page 1285
- mode, page 1286
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.

**Examples**

The following command configures the transforms set's encapsulation mode to transport:

```
mode transport
```
CSCF ATCF-ATGW Policy Configuration Mode Commands

The CSCF ATCF-ATGW Policy Configuration Mode is used to configure ATCF (Access Transfer Control Function) policy in the context.

**Command Modes**

Exec > Global Configuration > Context Configuration > ATCF Configuration

configure > context context_name > atcf policy name policy_name

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-atcf-atgw-policy)#`

- criteria, page 1288
- end, page 1290
- exit, page 1291
- ps-cs-alerting, page 1292
criteria

This command enables criteria to invoke ATCF functionality.

Product

SCM, P-CSCF, A-BG

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > ATCF Configuration

configure > context context_name > atcf policy name policy_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-atcf-atgw-policy)#

Syntax Description

criteria { access-type { 3gpp-e-utran-fdd | 3gpp-e-utran-tdd | 3gpp-geran | 3gpp-utran-fdd | 3gpp-utran-tdd | any | cellular | docsis | dsl | ethernet | wlan } | all | any | ics-capability | roaming }

default criteria access-type

no criteria { access-type { 3gpp-e-utran-fdd | 3gpp-e-utran-tdd | 3gpp-geran | 3gpp-utran-fdd | 3gpp-utran-tdd | cellular | docsis | dsl | ethernet | wlan } | ics-capability | roaming }

default

Configures this command with its default setting.

no

If previously configured, disables the configuration.

criteria { access-type { 3gpp-e-utran-fdd | 3gpp-e-utran-tdd | 3gpp-geran | 3gpp-utran-fdd | 3gpp-utran-tdd | any | cellular | docsis | dsl | ethernet | wlan } | all | any | ics-capability | roaming }

Specifies the access type of UE to invoke ATCF.

The supported access types are:

- **3gpp-e-utran-fdd**: Access type of UE is E-UTRAN-FDD
- **3gpp-e-utran-tdd**: Access type of UE is E-UTRAN-TDD
- **3gpp-geran**: Access type of UE is GERAN
- **3gpp-utran-fdd**: Access type of UE is UTRAN_FDD
- **3gpp-utran-tdd**: Access type of UE is UTRAN_TDD
• **any**: Access type of UE is any of the following: UTRAN, E-UTRAN, GERAN, DSL, ETHERNET, CELLULAR, WLAN or DOCSIS

• **cellular**: Access type of UE is CELLULAR

• **docsis**: Access type of UE is DOCSIS

• **dsl**: Access type of UE is DSL

• **ethernet**: Access type of UE is ETHERNET

• **wlan**: Access type of UE is WLAN

**all**

Specifies that all criteria must be met.

**any**

Specifies that any criteria must be met.

**ics-capability**

Specifies that UE is ICS capable.

**roaming**

Specifies that UE is in visited network.

**Usage Guidelines**

Use this command to enable criteria based on UE's access type to invoke ATCF functionality.

**Examples**

The following command enables ATCF to be invoked based on UE’s access type of E-UTRAN-TDD:

```
criteria access-type 3gpp-utran-tdd
```
**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.
**ps-cs-alerting**

This command configures access transfer during alerting support in ATCF service.

**Product**
SCM, P-CSCF, A-BG

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > ATCF Configuration

```plaintext
configure > context context_name > atcf policy name policy_name
```

Entering the above command sequence results in the following prompt:

```
/context_name/host_name/config-atcf-atgw-policy#
```

**Syntax Description**

| no | ps-cs-alerting

**Usage Guidelines**

Use this command to configure access transfer during alerting support in ATCF service.
CSCF Access Profile Configuration Mode Commands

The Access Profile Configuration Mode is used to set commands supporting the use of signaling compression, authentication, and SIP timers for subscribers accessing the system from varying network types.

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Access Profile Configuration

configure > context context_name > cscf access-profile { default | name profile_name }

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-access-profile) #
```

**Important**

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

- access-security-type, page 1294
- authentication, page 1295
- diameter-selection, page 1296
- end, page 1297
- exit, page 1298
- pcrf-policy-control, page 1299
- sigcomp, page 1300
- timeout, page 1301
access-security-type

Sets the type of access security for a P-CSCF/A-BG.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Access Profile Configuration
configure > context context_name > cscf access-profile { default | name profile_name }

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-cscf-access-profile)#
```

**Syntax Description**
| no | access-security-type ipsec-3gpp-cscf |

- **no**
  Disables the selected access security type.

- **ipsec-3gpp-cscf**
  Security mechanism 3GPP/3GPP2 IPSec.

**Usage Guidelines**
Use this command to enable or disable an access security type for a P-CSCF or A-BG.

**Examples**
Enables 3GPP/3GPP2 IPSec access security on P-CSCF or A-BG:
```
access-security-type ipsec-3gpp-cscf
```

Disables 3GPP/3GPP2 IPSec access security on P-CSCF or A-BG:
```
no access-security-type ipsec-3gpp-cscf
```
authentication

Sets the authentication method to use for subscribers using this access profile.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Access Profile Configuration

```
configure > context context_name > cscf access-profile { default | name profile_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-access-profile)#
```

**Syntax Description**
```
[ no ] authentication { aka-v1 | custom-md5 | md5 }
```

- **no**
  Disables the selected authentication type.

- **aka-v1 | custom-md5 | md5**
  - **aka-v1**: Specifies that the AKA-v1 algorithm will be used for subscribers using this access profile.
  - **custom-md5**: Specifies that custom algorithm HTTP-Digest-MD5 will be used for subscribers using this access profile.
  - **md5**: Specifies that the MD5 algorithm will be used for subscribers using this access profile. This is the default setting for this command.

**Usage Guidelines**
Use this command to set the authentication method used for subscribers using this access profile.

**Examples**
The following command sets the authentication type for subscribers using this access profile to **md5**:

```
authentication md5
```
diameter-selection

Enables or disables prefix and capability-based CDF server selection for this access profile. By default, this command is disabled.

Product

SCM (S-CSCF)

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Access Profile Configuration

configure > context context_name > csf access-profile { default | name profile_name }

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-cscf-access-profile)#

Syntax Description

| no | diameter-selection cdf

no

Disables prefix and capability-based CDF server selection.

Usage Guidelines

Use this command to enable or disable prefix and capability-based CDF server selection per access-type.
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.
**pcrf-policy-control**

Enables PCRF policy control for this access profile. By default, this command is disabled.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Access Profile Configuration

```
configure > context context_name > cscf access-profile { default | name profile_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-access-profile)#
```

**Syntax Description**

```
| default | no | pcrf-policy-control
```

**Usage Guidelines**

Use this command to enable or disable PCRF policy control for this access profile.

When a subscriber sends a REGISTER message, P-CSCF extracts the access-type mentioned in the P-Access-Network-Info and stores it. When P-CSCF needs to trigger an AAR for a subscriber, either for signaling-loss-detection or media-authorization, it will check if pcrf-policy-control is enabled for that subscriber's stored access-type. If pcrf-policy-control is enabled, AAR will be sent to PCRF for that subscriber.
**sigcomp**

Enables signalling compression for the Access Profile.

**Product**

SCM (P-CSCF, A-BG)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Access Profile Configuration

configure > context context_name > cscf access-profile { default | name profile_name }

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-cscf-access-profile)#

**Syntax Description**

[ no ] sigcomp [ force ]

**no**

Disables signalling compression for the Access Profile.

**force**

Specifies that signaling compression is to be forced for the access type. When this feature is enabled, messages received by the P-CSCF/A-BG that are not compressed are rejected.

**Usage Guidelines**

Use this command to enable signalling compression for the specific Access Profile.
timeout

Sets timeout values for CSCF and SIP transactions for subscribers using this Access Profile.

**Product**

SCM (P-CSCF, A-BG)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Access Profile Configuration

```
configure > context context_name > csf access-profile { default | name profile_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-access-profile)#
```

**Syntax Description**

```
timeout sip { 3gpp-d sec | 3gpp-t1 msec | 3gpp-t2 sec | 3gpp-t4 sec | c sec | d sec | invite-expiry sec | t1 msec | t2 sec | t4 sec }

default timeout sip { 3gpp-d | 3gpp-t1 | 3gpp-t2 | 3gpp-t4 | c | d | invite-expiry | t1 | t2 | t4 }
```

sip { 3gpp-d sec | 3gpp-t1 msec | 3gpp-t2 sec | 3gpp-t4 sec | c sec | d sec | invite-expiry sec | t1 msec | t2 sec | t4 sec }

Sets transaction and expiry timers for SIP.

- **3gpp-d sec**: This time is used to control the retransmission of 200OK messages to INVITEs after an ACK is sent. The ACK transaction is cleared after this period. This timer is applicable only for unreliable transport. sec must be an integer from 0 to 2147483646. Default: 64*T1 (128 seconds, recommended minimum)

- **3gpp-t1 msec**: This timer is used to control the time interval between each retransmission. The interval doubles after each retransmission. This is used by P-CSCF/A-BG only when it sending message toward the UE. Example: T1, 2T1, 4T2, etc. This timer is applicable only for unreliable transport. msec must be an integer from 0 to 2147483646. Default: 2000 ms (2 secs, recommended minimum).

- **3gpp-t2 sec**: This timer is used to control the period for which the request continues to get retransmitted. This is used by P-CSCF/A-BG only when it sending message toward the UE. This timer is applicable both for reliable and unreliable transport. sec must be an integer from 0 to 2147483646. Default: 16 seconds (recommended minimum).
### 3gpp-t4 sec

This timer is used to control the period for which the final response to non-invite transaction should be buffered. The buffered response for the retransmitted non-invite request should be sent within that interval. This timer is applicable only for unreliable transport.

- **sec** must be an integer from 0 to 2147483646.
- Default: 17 seconds (recommended minimum).

### c sec

This timer is used for an INVITE transaction; if the response is a provisional response with status codes 101 to 199 inclusive (anything but 100), the proxy must reset timer C for that client transaction. The timer may be reset to a different value, but this value must be greater than 3 minutes (180 seconds). When timer C in S-CSCF fires first, S-CSCF will send CANCEL request to Terminating P-CSCF and Terminating P-CSCF will send CANCEL request to UAS.

- **sec** must be an integer from 180 to 2147483646.
- Default: 180 seconds

### d sec

This time is used to control the retransmission of 200 OK to INVITE after ACK is sent. The ACK transaction will be cleared after this interval. This timer is applicable only for unreliable transport.

- **sec** must be an integer from 0 to 2147483646.
- Default: 64*T1 (32 seconds, recommended minimum)

### invite-expiry sec

This timer is used by SIP while acting as UA Role and no final response is received for the INVITE request sent. This timer is applicable for both reliable and unreliable transport.

- **sec** must be an integer from 0 to 2147483646.
- Default: 100 seconds (recommended minimum).

### t1 msec

Specifies the time interval (in milliseconds) between each retransmission. The interval doubles after each retransmission, for example: T1, 2T1, 4T2, etc. This timer is applicable only for unreliable transport.

- **msec** must be an integer from 0 to 2147483646.
- Default: 500 milliseconds (recommended minimum).

### t2 sec

This timer is used to control the period for which the request keeps getting retransmitted. This timer is applicable both for reliable and unreliable transport.

- **sec** must be an integer from 0 to 2147483646. The recommended minimum value for this parameter is 4 seconds.
- Default: 64*T1 (32 seconds)

### t4 sec

This timer is used to control the period for which the final response to non-invite transaction should be buffered so as to send the buffered response for the retransmitted non-invite request within that interval. This timer is applicable only for unreliable transport.

- **sec** must be an integer from 0 to 2147483646.
- Default: 5 seconds (recommended minimum).

### default

Sets/restores default value assigned for specified parameter.

#### Usage Guidelines

Use this command to configure SIP Stack timers and CSCF service specific timers for subscriber traffic using this Access Profile.
**Examples**

The following command sets the SIP d timer to 64 seconds:

```
timeout sip d 64
```
timeout
CSCF ACL Configuration Mode Commands

The CSCF ACL (Access Control List) Configuration Mode is used to configure session permissions (permit/deny access) within the system.

**Command Modes**

```
Exec > Global Configuration > Context Configuration > CSCF ACL Configuration

configure > context context_name > cscf acl { default | name list_name }
```

Entering the above command sequence results in the following prompt:

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

**Important**

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

- after, page 1306
- before, page 1307
- deny, page 1308
- end, page 1311
- exit, page 1312
- permit, page 1313
- redirect, page 1316
**after**

Places the CSCF ACL entry at the bottom or end of the ACL. Use this command in conjunction with the *permit* and/or *deny* commands.

**Product**

SCM

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF ACL Configuration

```plaintext
configure > context context_name > cscf acl { default | name list_name }
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-cscf-acl)#
```

**Syntax Description**

`after`

**Usage Guidelines**

Add this command before the *permit* and/or *deny* commands to place the entry at the end of the ACL.
before

Places the CSCF ACL entry at the beginning or top of the ACL. Use this command in conjunction with the permit and/or deny commands.

**Product**

SCM

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF ACL Configuration

configure > context context_name > cscf acl { default | name list_name }

Entering the above command sequence results in the following prompt:

(context_name)host_name(config-cscf-acl)#

**Syntax Description**

before

**Usage Guidelines**

Add this command before the permit and/or deny commands to place the entry at the beginning of the ACL.
deny

Configures the system to deny subscriber sessions based on criteria matching the received packet.

Product  
SCM

Privilege  
Administrator

Command Modes  
Exec > Global Configuration > Context Configuration > CSCF ACL Configuration
configure > context context_name > cscf acl { default | name list_name }

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

Syntax Description  
deny { any | destination aor aor | log { any | destination aor aor | source { address ip_address | aor aor } | subscriber-capability capability_type | user-agent device-type device_type | source { address ip_address | aor aor } | subscriber-capability capability_type | user-agent device-type device_type } | no deny { any | destination aor aor | source { address ip_address | aor aor } | subscriber-capability capability_type }

any
Filters all CSCF sessions.

destination aor aor
Filters sessions based on the destination AoR. aor must be an existing AoR from 1 to 79 characters in length.

Important  
AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

log { any | destination aor aor | source { address ip_address | aor aor } | subscriber-capability { capability_type | user-agent device-type device_type }

Enables logging for CSCF sessions meeting the criteria specified in the ACL. The logs can be viewed by executing the logging filter active facility acl-log command in the Exec mode.

Specifies the criteria that packets will be compared against. The following criteria are supported:

• any
• destination aor aor
• source address ip_address
• source aor aor
• subscriber-capability capability_type
• user-agent device-type device_type

source { address ip_address | aor aor }
Filters session based on the source IP address or AoR.

• ip_address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
• aor must be an existing AoR from 1 to 79 characters in length.

Important AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Cisco ASR 5000 Series Session Control Manager Administration Guide for more information about regular expressions.

subscriber-capability { capability_type }
Filters session based on one of the following subscriber capability types:

• at - Custom AT Type
• audio - Audio Capability Type
• chat - Custom CHAT Type
• cs - Custom CS Type
• ft - Custom FT Type
• im - Custom IM Type
• lte-voip - Custom LTE-VOIP Type
• lte-vt - Custom LTE-VT Type
• mms - Custom MMS Type
• msg - Custom MSG Type
• oma-sip-im - Custom OMA SIP-IM Type
• rcs-dp - Custom RCS-DP Type
• rcs-e - Custom RCS-E Type
• rcs-ft - Custom RCS-FT Type
• rcs-im - Custom RCS-IM Type
• rcs-is - Custom RCS-IS Type
• rcs-sp - Custom RCS-SP Type
deny

- **rcs-vs** - Custom RCS-VS Type
- **smart-edu** - Custom SMART-EDU Type
- **text** - Text Capability Type
- **video** - Video Capability Type
- **vt** - Custom VT Type
- **vt-ft** - Custom VT-FT Type
- **vt-is** - Custom VT-IS Type
- **vt-loc** - Custom VT-LOC Type
- **vt-memo** - Custom VT-MEMO Type

**user-agent device-type device_type**
Filters session based on device-type in user-agent header.

*device_type* must be from 1 to 15 characters in length. The following user agent device types are supported.

- feature_phone
- smart_phone
- pad
- tablet_pc
- pc
- soft_phone
- modem

+ This symbol indicates that the keywords can be entered multiple times within a single command.

**no deny { any | destination aor aor | source { address ip_address | aor aor } | subscriber-capability { capability_type } }**
Removes specified filter criteria.

**Usage Guidelines**
Specifies the subscriber sessions to deny based on the criteria specified.

**Examples**
The following command denies access to subscribers with a source address of 1.2.3.4:

deny source address 1.2.3.4
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

end

Usage Guidelines

Use this command to return to the Exec mode.
exit

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

<table>
<thead>
<tr>
<th>Product</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
</tbody>
</table>

**Syntax Description**

exit

**Usage Guidelines**

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

Configures the system to allow subscriber sessions based on criteria matching the received packet.

Product

SCM

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF ACL Configuration

configure > context context_name > cscf acl { default | name list_name }

Entering the above command sequence results in the following prompt:

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

Syntax Description

permit { any | destination aor aor | log { any | destination aor aor | source { address ip_address | aor aor } | subscriber-capability capability_type | user-agent device-type device_type } | source { address ip_address | aor aor } | subscriber-capability capability_type } |

no permit { any | destination aor aor | source { address ip_address | aor aor } | subscriber-capability capability_type } |

any

Filters all CSCF sessions.

destination aor aor

Filters sessions based on the destination AoR.

aor must be an existing AoR from 1 to 79 characters in length.

Important

AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Cisco ASR 5000 Series Session Control Manager Administration Guide for more information about regular expressions.

log { any | destination aor aor | source { address ip_address | aor aor } | subscriber-capability { capability_type } | user-agent device-type device_type }

Enables logging for CSCF sessions meeting the criteria specified in the ACL. The logs can be viewed by executing the logging filter active facility acl-log command in the Exec mode.

Specifies the criteria that packets will be compared against. The following criteria are supported:
permit

• any
• destination aor aor
• source address ip_address
• source aor aor
• subscriber-capability capability_type
• user-agent device-type device_type

source { address ip_address | aor aor }
Filters session based on the source IP address or AoR.
  • ip_address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
  • aor must be an existing AoR from 1 to 79 characters in length.

Important
AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

subscriber-capability { capability_type }
Filters session based on one of the following subscriber capability types:
  • at - Custom AT Type
  • audio - Audio Capability Type
  • chat - Custom CHAT Type
  • cs - Custom CS Type
  • ft - Custom FT Type
  • im - Custom IM Type
  • lte-voip - Custom LTE-VOIP Type
  • lte-vt - Custom LTE-VT Type
  • mms - Custom MMS Type
  • msg - Custom MSG Type
  • oma-sip-im - Custom OMA SIP-IM Type
  • rcs-dp - Custom RCS-DP Type
  • rcs-e - Custom RCS-E Type
  • rcs-ft - Custom RCS-FT Type
  • rcs-im - Custom RCS-IM Type
  • rcs-is - Custom RCS-IS Type
permit

- **rcs-sp** - Custom RCS-SP Type
- **rcs-vs** - Custom RCS-VS Type
- **smart-edu** - Custom SMART-EDU Type
- **text** - Text Capability Type
- **video** - Video Capability Type
- **vt** - Custom VT Type
- **vt-ft** - Custom VT-FT Type
- **vt-is** - Custom VT-IS Type
- **vt-loc** - Custom VT-LOC Type
- **vt-memo** - Custom VT-MEMO Type

**user-agent device-type device_type**
Filters session based on device-type in user-agent header.

*device_type* must be from 1 to 15 characters in length. The following user agent device types are supported.

- feature_phone
- smart_phone
- pad
- tablet_pc
- pc
- soft_phone
- modem

+  
This symbol indicates that the keywords can be entered multiple times within a single command.

**no permit** { any | destination aor |or | source { address ip_address | aor aor | subscriber-capability { capability_type } }
Removes specified filter criteria.

**Usage Guidelines**
Specifies the subscriber sessions to permit based on the criteria specified.

**Examples**
The following command permits access to subscribers with a destination AoR of $.@abc123.com:
permit destination aor $.@abc123.com
**redirect**

Configures the system to redirect subscriber sessions to another CSCF based on criteria matching the received packet.

**Product**

SCM

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF ACL Configuration

classicmode > context context_name > scf acl { default | name list_name }

Entering the above command sequence results in the following prompt:

```
({context_name}host_name(config-cscf-acl)#
```

**Syntax Description**

```
redirect { address ip_address | host host_name } | port port_number } | any | destination aor aor | log { any | destination aor aor | source { address ip_address | aor aor } | subscriber-capability capability_type | user-agent device-type device_type } | source { address ip_address | aor aor } | subscriber-capability capability_type | user-agent device-type device_type } +
```

**address ip_address**

The address to which UE should be redirected.

`ip_address` must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

**host host_name**

The host to which UE should be redirected.

`host_name` must be an existing name from 1 to 79 characters in length.

**port port_number**

The port at which request should be redirected.

`port_number` must be an integer from 1 to 65535.

**any**

Redirect UE to address/host.
**destination aor aor**
Redirect UE to address/host if destination AoR matches.

*aor* must be an existing AoR from 1 to 79 characters in length.

---

**Important**
AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

---

```
log { any | destination aor aor | source { address ip_address | aor aor } | subscriber-capability { capability_type } | user-agent device-type device_type }
```

Enables logging for redirected UE meeting the criteria specified in the ACL. The logs can be viewed by executing the `logging filter active facility acl-log` command in the Exec mode.

Specifies the criteria that packets will be compared against. The following criteria are supported:

- *any*
- *destination aor aor*
- *source address ip_address*
- *source aor aor*
- *subscriber-capability capability_type*
- *user-agent device-type device_type*

```
source { address ip_address | aor aor }
```

Redirect UE to address/host if source IP address or AoR matches.

- *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
- *aor* must be an existing AoR from 1 to 79 characters in length.

---

**Important**
AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

---

```
subscriber-capability { capability_type }
```

Redirect UE to address/host if contact has one of the following subscriber capability types:

- *at* - custom AT type
- *audio* - audio capability type
- *chat* - custom CHAT type
- *cs* - custom CS type
- *ft* - custom FT type
- *im* - custom IM type
user-agent device-type device_type

Redirect UE to address/host according to device-type in user-agent header.

device_type must be from 1 to 15 characters in length. The following user agent device types are supported.

- feature_phone
- smart_phone
- pad
- tablet_pc
- pc
- soft_phone
- modem

+ This symbol indicates that the keywords can be entered multiple times within a single command.
no redirect { address ip_address | host host_name } | port port_number | { any | destination aor aor | source { address ip_address | aor aor } | subscriber-capability { capability_type } }

Removes specified redirect location and filter criteria.

Usage Guidelines
Specifies the subscriber sessions to redirect based on the criteria specified.

Examples
The following command redirects subscribers with a destination AoR of $.@abc123.com to host scscf.com:
redirect host scscf.com destination aor $.@abc123.com
redirect
CSCF AoR Policy Rules Configuration Mode Commands

The CSCF AoR Policy Rules Configuration Mode is used to manage AoR policy profiles within the system. Both default and user-defined profiles can be managed in this mode.

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Rules Configuration

configure > context context_name > csf policy { default | name policy_name } > aor-policy-rules

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-policy_name=aor)#

Important

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

- after, page 1322
- aor, page 1323
- before, page 1324
- end, page 1325
- exit, page 1326
after

Places the CSCF policy entry at the bottom or end of the policy list. Use this command in conjunction with the aor command.

**Product**

SCM

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Rules Configuration

```plaintext
configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-policy_name-aor)#
```

**Syntax Description**

`after`

**Usage Guidelines**

Add this command before the aor command to place the entry at the end of the policy list.
aor

Configures an AoR profile and enters the CSCF Policy Rules Configuration Mode.

**Product**  
SCM

**Privilege**  
Administrator

**Command Modes**  
Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Rules Configuration

```
configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-policy_name-aor)#
```

**Syntax Description**

- `| no | aor aor_name`

  - **no**  
    Removes the AoR profile from the system.

  - **aor_name**  
    Specifies a name for the AoR profile.  
    `aor_name` must be from 1 to 79 alpha and/or numeric characters in length.

**Usage Guidelines**  
Use this command to create or modify an AoR profile and enter the CSCF Policy Rules Configuration Mode. Entering this command results in the following prompt:

```
{context_name}hostname(config-aor_name-aor)#
```

CSCF Policy Rules Configuration Mode commands are defined in the *CSCF Policy Rules Configuration Mode Commands* chapter of this guide.

**Examples**  
The following command creates an AoR profile named *aor5* and enters the CSCF Policy Rules Configuration Mode:

```
aor aor5
```
before

Places the CSCF policy entry at the top or beginning of the policy list. Use this command in conjunction with the aor command.

**Product**
SCM

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Rules Configuration

```
configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules
```

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-policy_name-aor)>
```

**Syntax Description**
before

**Usage Guidelines**
Add this command before the aor command to place the entry at the beginning of the policy list.
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.
CSCF ATCF-ATGW Configuration Mode Commands

The CSCF ATCF (Access Transfer Control Function)/ATGW (Access Transfer Gateway) Configuration Mode is used to configure the ATCF-ATGW functionality in the Proxy-CSCF service.

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF ATCF-ATGW Configuration

`configure > context context_name > csf service service_name > proxy-cscf > atcf-atgw`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-atcf-atgw)#
```

**Important**

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

- `call-linger-timer`, page 1328
- `end`, page 1329
- `exit`, page 1330
- `mgmt-uri`, page 1331
- `policy name`, page 1332
- `stn-sr`, page 1333
- `trusted scc-as`, page 1334
call-linger-timer

This command configures the timeout value after call termination request for ATCF service.

**Product**
SCM: P-CSCF, A-BG

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF ATCF-ATGW Configuration

configure > context context_name > csf service service_name > proxy-cscf > atcf-atgw

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-cscf-atcf-atgw)#
```

**Syntax Description**
call-linger-timer timer_seconds
| default | no | call-linger-timer

default
Configures this command with the default setting.

no
Disables the timeout configuration.

timer_seconds
Specifies the call linger timer value in seconds.
timer_seconds must be an integer from 1 to 32.

**Usage Guidelines**
Use this command to enable or disable call linger timer after call termination request. This determines the timeout value of session for abnormal procedure parameters in ATCF service.

**Examples**
The following command sets the call linger timer value to 20 seconds:
call-linger-timer 20
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.
**mgmt-uri**

This command supports PSI-based routing mode in I-CSCF.

**Product**

SCM: P-CSCF, A-BG, I-CSCF

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF ATCF-ATGW Configuration

configure > context context_name > cscf service service_name > proxy-cscf > atcf-atgw

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-atcf-atgw)#
```

**Syntax Description**

`mgmt-uri` `mgmt_uri`

`default mgmt-uri`

`default`

Configures this command with its default setting.

`mgmt_uri`

Specifies the ATCF management URI, and indicates SIP URI or hostname with domain.

`mgmt_uri` must be an alphanumeric string of 1 to 127 characters.

Example format of management URI:

- `sip:xyz@abc.com` for SIP URI
- `sip:atcf.xyz.net` for hostname with domain

**Usage Guidelines**

Use this command to configure ATCF management URI for PSI based routing in I-CSCF.

**Examples**

The following command configures the ATCF management URI for hostname with domain `sip:atcf.xyz.net`

```
mgmt-uri sip:atcf.xyz.net
```

policy name

This command assigns or removes an existing ATCF policy.

Product
SCM: P-CSCF, A-BG

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF ATCF-ATGW Configuration

configure > context context_name > csf service service_name > proxy-cscf > atcf-atgw

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-cscf-atcf-atgw)#

Syntax Description
| no | policy name policy_name

no
If previously configured, disables the configuration.

policy_name
Specifies the name of the ATCF policy list.

policy_name must be an alphanumeric string of 1 to 127 characters.

Usage Guidelines
Use this command to assign or remove an existing ATCF policy.

Examples
The following command sets the ATCF policy named access:

generic_set policy name access
**stn-sr**

This command specifies a Session Transfer Number for Single Radio (STN-SR) for the ATCF service.

**Product**

SCM: P-CSCF, A-BG

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF ATCF-ATGW Configuration

```plaintext
configure > context context_name > cscf service service_name > proxy-cscf > atcf-atgw
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-atcf-atgw)#
```

**Syntax Description**

- `stn-sr stnsr_num`
- `no stn-sr`

- **no**
  If previously configured, disables the configuration.

- **stnsr_num**
  Specifies the STN-SR.
  `stnsr_num` must be a string of up to 15 digits.

**Usage Guidelines**

Use this command to configure the STN-SR number for ATCF service. The same STN-SR number will be used for all subscribers.

**Examples**

The following command sets STN-SR number to `1005002115000`:

```plaintext
stn-sr 1005002115000
```
trusted scc-as

This command allows you to configure trusted Service Centralization and Continuity - Application Server (SCC-AS) addresses in ATCF service.

**Product**
SCM: P-CSCF, A-BG

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF ATCF-ATGW Configuration

```
configure > context context_name > cscf service service_name > proxy-cscf > atcf-atgw
```

Entering the above command sequence results in the following prompt:

```
/context_name/host_name(config-cscf-atcf-atgw)#
```

**Syntax Description**

```
[ no ] trusted scc-as scc_as
```

- **no**
  If previously configured, disables the configuration.

- **scc_as**
  Specifies the list of trusted SCC-AS.
  `scc_as` must be an alphanumeric string of 1 to 79 characters.

**Usage Guidelines**
Use this command to add or delete an SCC-AS address in ATCF service.

**Examples**
The following command adds SCC-AS address `cscfscc`

```
trusted scc-as scc1
```
CSCF Charging Configuration Mode Commands

The CSCF Charging Configuration Mode is used to manage CSCF service policy profiles within the system.

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > CSCF Charging Configuration

```
configure > context context_name > cscf service service_name > charging
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-cscf-charging) #
```

**Important**

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

- end, page 1336
- exclude, page 1337
- exit, page 1339
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**

Configures the service to exclude SIP requests from the Rf charging configuration.

**Product**  
SCM

**Privilege**  
Administrator

**Command Modes**  
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > CSCF Charging Configuration

```
configure > context context_name > cscf service service_name > charging
```

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-cscf-charging)#
```

**Syntax Description**

| no | exclude { custom sip_method | invite | message | notify | register | subscribe | update } |

- **no**  
  Removes the exclusion of the specified SIP request message type.

- **custom sip_method**  
  Specifies CUSTOM SIP requests that are to be excluded from Rf charging.
  
  *sip_method* can be a name of any SIP method and be from 1 to 31 alpha and/or numeric characters.

- **invite**  
  Specifies that INVITE SIP requests are to be excluded from Rf charging.

- **message**  
  Specifies that MESSAGE SIP requests are to be excluded from Rf charging.

- **notify**  
  Specifies that NOTIFY SIP requests are to be excluded from Rf charging.

- **register**  
  Specifies that REGISTER SIP requests are to be excluded from Rf charging.
subscribe
Specifies that SUBSCRIBE SIP requests are to be excluded from Rf charging.

update
Specifies that UPDATE SIP requests are to be excluded from Rf charging.

Usage Guidelines
Use this command to exclude specific SIP requests from Rf charging.

Examples
The following command configures the service to exclude SIP REGISTER requests from Rf charging:
exclude register
exit

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

exit

Usage Guidelines

Use this command to return to the parent configuration mode.
CSCF Crypto Template Configuration Mode Commands

The CSCF Crypto Template Configuration Mode is used to configure a P-CSCF IPsec policy. It includes most of the IPsec parameters and Internet Key Exchange version 1 (IKEv1) parameters for cryptographic and authentication algorithms etc. A P-CSCF service will not support IPsec without a configured crypto template. Only one crypto template can be configured per P-CSCF service.

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Crypto Template Configuration

configure > context context_name > crypto template template_name ipsec-3gpp-cscf

Entering the above command sequence results in the following prompt:

```
{context_name} host_name (cfg-crypto-tmpl-ims-cscf-tunnel) #
```

**Important**

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

- end, page 1342
- exit, page 1343
- ipsec, page 1344
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 parameters for the 3GPP/3GPP2 P-CSCF security associations within this crypto template.

Product

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Crypto Template Configuration
configure > context context_name > crypto template template_name ipsec-3gpp-cscf

Entering the above command sequence results in the following prompt:

{context_name}host_name{cfg-crypto-tmpl-ims-cscf-tunnel}#

Syntax Description

ipsec transform-set list list_name

transform-set list name

transform-set: Specifies a context-level IPSec security association transform set to be used for deriving 3GPP/3GPP2 P-CSCF security associations from this crypto template.

list list_name: A space separated list of 3GPP/3GPP2 P-CSCF security association transform sets. list_name must be an existing 3GPP/3GPP2 P-CSCF transform set and be from 1 to 127 alpha and/or numeric characters.

Important

A minimum of one transform set is required. A maximum of four transform sets may be specified.

Usage Guidelines

Use this command to configure parameters for the 3GPP/3GPP2 P-CSCF security associations within this crypto template.

Examples

The following command configures the 3GPP/3GPP2 P-CSCF transform set list name to ikev1list1:

ipsec transform-set list ikev1list1
CSCF Diameter Selection Configuration Mode

The Diameter Selection Configuration Mode is used to configure AAA group selection criteria that will be used for all CDF (enabled for a given access type) or HSS interactions for a subscriber.

**Command Modes**

```
Exec > Global Configuration > Context Configuration > CSCF Diameter Selection Configuration
configure > context context_name > cscf diameter-selection type { cdf | hss }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-diameter-selection)#
```

**Important**

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

- `aaa-group`, page 1346
- `end`, page 1349
- `exit`, page 1350
aaa-group

Configures diameter selection entries.

Product

SCM

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Diameter Selection Configuration

configure > context context_name > cscf diameter-selection type { cdf | hss }

Entering the above command sequence results in the following prompt:

(context_name)host_name(config-cscf-diameter-selection)#

Syntax Description

aaa-group name { | preference value | | skiplir | | criteria { aor aor_prefix | subscriber-capability capability_type | subscriber-ip-type { v4 | v6 } | user-agent value | } } +

no aaa-group name preference value

name

Specifies a name for the diameter selection entry.

name must be from 1 to 63 alpha and/or numeric characters.

preference value

Configures preference that will be associated with each diameter selection entry. If preference is specified, the entry matching the preference is updated and a new entry is created in the prefix table. If preference is not specified, it is assigned a preference one greater than the last entry's preference in the diameter selection table.

value must be an integer from 1 to 65535.

skiplir

Configures selected AAA group to skip LIR-LIA (Location-Info-Request — Location-Info-Answer). This is applicable only for HSS.

criteria

Specifies AAA group selection criteria.

aor aor_prefix

Filters based on the source or destination AoR.
aor_prefix must be an existing AoR from 1 to 79 characters in length.

**Important**
AoR regular expressions are supported. Refer to the *SCM Engineering Rules Appendix* in the *Cisco ASR 5000 Series Session Control Manager Administration Guide* for more information about regular expressions.

**subscriber-capability capability_type**
Filters based on the capability of the subscriber.

- **at** - Custom AT Type
- **audio** - Audio Capability Type
- **chat** - Custom CHAT Type
- **cs** - Custom CS Type
- **ft** - Custom FT Type
- **im** - Custom IM Type
- **lte-voip** - Custom LTE-VOIP Type
- **lte-vt** - Custom LTE-VT Type
- **mms** - Custom MMS Type
- **msg** - Custom MSG Type
- **oma-sip-im** - Custom OMA SIP-IM Type
- **rcs-dp** - Custom RCS-DP Type
- **rcs-e** - Custom RCS-E Type
- **rcs-ft** - Custom RCS-FT Type
- **rcs-im** - Custom RCS-IM Type
- **rcs-is** - Custom RCS-IS Type
- **rcs-sp** - Custom RCS-SP Type
- **rcs-vs** - Custom RCS-VS Type
- **smart-edu** - Custom SMART-EDU Type
- **text** - Text Capability Type
- **video** - Video Capability Type
- **vt** - Custom VT Type
- **vt-ft** - Custom VT-FT Type
- **vt-is** - Custom VT-IS Type
- **vt-loc** - Custom VT-LOC Type
- **vt-memo** - Custom VT-MEMO Type
subscriber-ip-type \{ v4 | v6 \}
Filters based on the IP type of the subscriber.

v4 - IPv4 type
v6 - IPv6 type

user-agent value
Filters based on the User-Agent Header value.

value must be from 1 to 127 alpha and/or numeric characters.

+ 
This symbol indicates that the keywords can be entered multiple times within a single command.

no
Removes configured diameter selection entry.

Usage Guidelines
This command configures matching criteria for selecting a AAA group name. When a subscriber registers, the selection criteria are compared and the AAA group name from the matching entry will be picked up. The selected aaa-group will be used for all CDF (enabled for a given access type) or HSS interactions for that subscriber.

Note
A maximum of three criteria can be configured per entry. A maximum of 1024 such entries can be configured.

Examples
The following command creates a diameter selection entry named aaa1, with a destination AoR criteria of $.@abc123.com and preference 125 associated with it:

```bash
aaa-group aaa1 preference 125 criteria aor $.@abc123.com
```

The following command (immediately following in the configuration file) creates a diameter selection entry named aaa2, with a destination AoR criteria of user@cisco.com and preference 126 automatically associated with it:

```bash
aaa-group aaa2 criteria aor user@cisco.com
```
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

d

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.
CSCF EATF Configuration Mode Commands

The CSCF EATF Configuration Mode is used to set commands for enabling service continuity of IMS emergency sessions.

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Emergency-CSCF Configuration > CSCF EATF Configuration

`configure > context context_name > cscf service service_name > emergency-cscf > eatf`

Entering the above command sequence results in the following prompt:

`{context_name}host_name(config-cscf-eatf)#`

**Important**

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

- e-stn-sr, page 1352
- end, page 1353
- exit, page 1354
e-stn-sr

This command adds the Emergency Session Transfer Number for Single Radio (E-STN-SR) to the EATF.

Product
SCM: E-CSCF

Privilege
Administrator

Syntax Description

```
e-stn-sr estnsr_num
no e-stn-sr
```

- `no`
  Removes E-STN-SR number from the E-CSCF.

- `estnsr_num`
  Specifies the E-STN-SR.
  `estnsr_num` must be a string of up to 15 digits (+ prefix may be added).

Usage Guidelines
Use this command to configure E-STN-SR number for EATF service. EATF performs session continuity when the Access Transfer request indicated by the E-STN-SR is received.

Examples
The following command sets the E-STN-SR number to 5656565:
```
e-stn-sr 5656565
```
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.
CSCF Emergency-CSCF Configuration Mode Commands

The Emergency-CSCF Configuration Mode is used to set commands supporting the role of the CSCF service as an Emergency CSCF.

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Emergency-CSCF Configuration

```
configure > context context_name > cscf service service_name > emergency-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-emergency-cscf)#
```

**Important**

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

- eatf, page 1356
- end, page 1357
- exit, page 1358
- plani, page 1359
- privacy, page 1361
- psap-file, page 1362
**eatf**

This command enables Emergency Call Access Transfers (EATF) functionality for the service. Default is disabled.

**Product**

SCM: E-CSCF

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Emergency-CSCF Configuration

```
configure > context context_name > cscf service service_name > emergency-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-emergency-cscf)#
```

**Syntax Description**

```
[ no ] eatf
```

**no**

Removes EATF support from the E-CSCF.

**Usage Guidelines**

Use this command to enable or disable EATF functionality in emergency-CSCF service.  
On entering this command, the CLI prompt changes to:

```
[context_name]host_name(config-cscf-eatf)#
```
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.
plani

Sets parameters associated with P-LANI (P-Last-Access-Network-Info) header.

Product

SCM: E-CSCF

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Emergency-CSCF Configuration

configure > context context_name > csf service service_name > emergency-cscf

Entering the above command sequence results in the following prompt:

<context_name>host_name(config-cscf-service-emergency-cscf)#

Syntax Description

plani age seconds

[ default | no ] plani age

default

Sets the acceptable P-LANI age to 7200 seconds.

no

Removes the acceptable P-LANI age configured for the E-CSCF.

age seconds

Specifies the acceptable P-LANI age from registration time.

seconds must be an integer from 1 to 65535.

Default: 7200

Usage Guidelines

This command is used to identify location aging of subscriber is within acceptable limits.

Two timestamps are included in Emergency SIP INVITES P-LANI header to determine the "location age" of the last known cellular information at registration. The first timestamp shall be the date/time the P-LANI was captured. The second timestamp shall be the data and time of the Initial registration for voice services. The E-CSCF shall calculate the delta between the two timestamps to determine the P-LANI location age at registration. E-CSCF will compare the P-LANI location age to the "p-lani-acceptable-age" specified in this command. E-CSCF will omit/disregard the LDAP query for CGI location when "p-lani-acceptable-age" is exceeded.
Example

The following command sets the acceptable P-LANI age for the E-CSCF to 5000 seconds:
\texttt{plani age 5000}

The following command sets the acceptable P-LANI age for the E-CSCF to 7200 seconds:
\texttt{default plani age}

The following command removes the acceptable P-LANI age configured for the E-CSCF:
\texttt{no plani age}
privacy

Enables privacy support on the E-CSCF.

Product

SCM

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Emergency-CSCF Configuration

configure > context context_name > csf service service_name > emergency-cscf

Entering the above command sequence results in the following prompt:

{(context_name)host_name}(config-cscf-service-emergency-cscf) #

Syntax Description

| no | default | privacy |

no | default

Removes privacy support from the E-CSCF.

Usage Guidelines

Use this command to enable privacy support for Emergency CSCF service.
**psap-file**

Sets the location of the PSAP-Database file to maintain and access the ESRK-Ranges provided by the operator for the E-CSCF.

**Product**

SCM

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Emergency-CSCF Configuration

```
configure > context context_name > cscf service service_name > emergency-cscf
```

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-cscf-service-emergency-cscf)#
```

**Syntax Description**

- `psap-file file_name`
- `no psap-file`

- `no`

Removes the PSAP-Database file from the E-CSCF.

- `file_name`

Specifies the PSAP-Database file in one of the following formats:

- `ftp://[username]:[password]@host[/directory]/<filename>` - URL
- `file:/flash[/directory]/<filename>` - URL
- `sftp://[username]:[password]@host[/directory]/<filename>` - URL

**Usage Guidelines**

This command is used by the SRDB proclet for ESRK-PSAP database management for the E-CSCF.

**Example**

The following command specifies a PSAP-Database file for the E-CSCF:

```
psap-file ftp://[username]:[password]@10.6.2.246/home/nthattil/psap_profile_CSV_new1.csv
```
CSCF Enforce Codec Policy Configuration Mode Commands

The CSCF Enforce Codec Policy Configuration Mode is used to manage audio and video codec policies within the system. The parameters defined in this chapter are derived from IETF RFC 3551: "RTP Profile for Audio and Video Conferences with Minimal Control".

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration > Enforce Codec Policy Configuration

`configure > context context_name > cscfpolicy { default | name policy_name } > service-policy-rules > enforce-codec-policy`

-or-


`configure > context context_name > cscfpolicy { default | name policy_name } > aor-policy-rules > aor aor_name > enforce-codec-policy`

Entering the above command sequences results in the following prompt:

`[context_name]host_name(config-policy-enforce-code)#`

**Important**

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

- dynamic-codec, page 1364
- end, page 1366
- exit, page 1367
- static-codec, page 1368
**dynamic-codec**

Creates a list of dynamic codecs supported by the system.

**Product**

SCM

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration > Enforce Codec Policy Configuration
configure > context context_name > cscf policy { default | name policy_name } > service-policy-rules > enforce-codec-policy

~or~

configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules > aor
aor_name > enforce-codec-policy

Entering the above command sequences results in the following prompt:

{context_name|host_name}(config-policy-enforce-code)#

**Syntax Description**

**dynamic-codec** { audio encoding_name | video encoding_name } { | clock_rate | | channels | }  
**default dynamic-codec**

**no dynamic-codec** { encoding_name | | clock_rate | | channels | }  

**default**

Specifies that the default list of dynamic codecs is added to the allowed codecs list. Default dynamic codecs: H263 and AMR.

**no**

 Specifies that all dynamic codecs are removed from the allowed codecs list. If an encoding_name is specified, then only the codec specified by the encoding_name is removed. Furthermore, if a supporting clock_rate and/or channels are specified, then only the encoding_name with the specified clock_rate and/or channels is removed.

**audio encoding_name | video encoding_name**

**audio encoding_name**: Specifies the encoding name of the dynamic audio codec added to the allowed codec list. encoding_name must be from 1 to 49 alpha and/or numeric characters.
**video encoding_name**: Specifies the encoding name of the dynamic video or audio-video codec added to the allowed codec list. `encoding_name` must be from 1 to 49 alpha and/or numeric characters.

```
[ clock_rate ] [ channels ]
```

- **clock_rate**: Specifies the sampling rate of the codec. `clock_rate` must be an integer from 0 to 1000000.
- **channels**: Specifies the number of channels required by the codec. `channels` must be an integer from 1 to 1000000.

Valid dynamic audio codecs:

<table>
<thead>
<tr>
<th>Encoding Name</th>
<th>Clock Rate (Hz)</th>
<th>Channels</th>
</tr>
</thead>
<tbody>
<tr>
<td>G726-40</td>
<td>8,000</td>
<td>1</td>
</tr>
<tr>
<td>G726-32</td>
<td>8,000</td>
<td>1</td>
</tr>
<tr>
<td>G726-24</td>
<td>8,000</td>
<td>1</td>
</tr>
<tr>
<td>G726-16</td>
<td>8,000</td>
<td>1</td>
</tr>
<tr>
<td>G729D</td>
<td>8,000</td>
<td>1</td>
</tr>
<tr>
<td>G729E</td>
<td>8,000</td>
<td>1</td>
</tr>
<tr>
<td>GSM-EFR</td>
<td>8,000</td>
<td>1</td>
</tr>
<tr>
<td>L8</td>
<td>Variable</td>
<td>Variable</td>
</tr>
<tr>
<td>RED</td>
<td>See RFC3551</td>
<td></td>
</tr>
<tr>
<td>VDVI</td>
<td>Variable</td>
<td>1</td>
</tr>
</tbody>
</table>

Valid dynamic video codecs:

<table>
<thead>
<tr>
<th>Encoding Name</th>
<th>Clock Rate (Hz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>H263-1998</td>
<td>90,000</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to create a list of supported dynamic audio and video codecs in the system. When a request is received by the CSCF, the SDP fields in the message are checked to determine the codec being used. The codec in the SDP fields must match a codec in the allowed codec list or the CSCF rejects the request.

**Examples**

The following command adds the GSM-EFR codec to the allowed dynamic codec list:

```
dynamic-codec GSM-EFR
```
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.
static-codec

Creates a list of static codecs supported by the system.

Product
SCM

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration > Enforce Codec Policy Configuration

configure context context_name csf policy { default | name policy_name } service-policy-rules enforce-codec-policy

-or-


configure context context_name csf policy { default | name policy_name } aor-policy-rules aor aor_name enforce-codec-policy

Entering the above command sequences results in the following prompt:

<context_name>host_name(config-policy-enforce-code)#

Syntax Description
static-codec { audio payload_type | video payload_type }
default static-codec
no static-codec [ payload_type ]

default
Specifies that the default list of static codecs is added to the allowed codecs list.
The default static codec is 5: DVI4.

no
Specifies that all static codecs are removed from the allowed codecs list. If a payload_type is specified, then only the codec specified by the payload_type is removed.

audio payload_type | video payload_type

audio payload_type: Specifies the audio codec added to the allowed codecs list. payload_type must be an integer from 0 to 95. Default value is 5.

Valid static audio codecs:
video payload_type: Specifies the video or audio-video codec added to the allowed codecs list. payload_type must be an integer from 0 to 95. Default value is 5.

Valid static video codecs:

<table>
<thead>
<tr>
<th>Number</th>
<th>Codec</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>unassigned</td>
</tr>
<tr>
<td>25</td>
<td>CelB</td>
</tr>
<tr>
<td>26</td>
<td>JPEG</td>
</tr>
<tr>
<td>27</td>
<td>unassigned</td>
</tr>
<tr>
<td>28</td>
<td>nv</td>
</tr>
<tr>
<td>29</td>
<td>unassigned</td>
</tr>
<tr>
<td>30</td>
<td>unassigned</td>
</tr>
<tr>
<td>31</td>
<td>H261</td>
</tr>
<tr>
<td>32</td>
<td>MPV</td>
</tr>
<tr>
<td>33</td>
<td>MP2T</td>
</tr>
<tr>
<td>34</td>
<td>H263</td>
</tr>
<tr>
<td>35-71</td>
<td>unassigned</td>
</tr>
<tr>
<td>72-76</td>
<td>reserved</td>
</tr>
<tr>
<td>77-95</td>
<td>unassigned</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this commands to create a list of supported static audio and video codecs in the system. When a request is received by the CSCF, the SDP fields in the message are checked to determine the codec being used. The codec in the SDP fields must match a codec in the allowed codec list or the CSCF rejects the request.

Examples

The following command adds the G729 audio codec to the allowed codecs list:

```
static-codec 18
```
static-codec
CSCF IFC SPT Group Mode Commands

The CSCF iFC SPT Group Configuration Mode is used to associate individual SPT conditions with an Initial Filter Criteria (iFC) Service Point Trigger (SPT) group.

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF IFC SPT Group Configuration

```
configure > context context_name > cscf ifc-spt-group id group_id
```

Entering the above command sequence results in the following prompt:

```
/context_name/host_name(config-cscf-ifc-spt-group)#
```

**Important**

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

- end, page 1372
- exit, page 1373
- spt-condition, page 1374
end

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

dend

**Usage Guidelines**

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

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

exit

**Usage Guidelines**

Use this command to return to the parent configuration mode.
**spt-condition**

Assigns iFC SPT conditions to an existing iFC SPT group.

**Product**

SCM (S-CSCF, SIP Proxy)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF IFC SPT Group Configuration

```
configure > context context_name > cscf ifc-spt-group id group_id
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-cscf-ifc-spt-group)#
```

**Syntax Description**

```
| no | spt-condition id cond_id
```

- **no**
  
  Removes the specified CSCF iFC SPT condition from the iFC SPT group.

- **spt-condition id cond_id**
  
  Specifies the name of an existing iFC SPT condition.
  
  `cond_name` must be an integer from 1 to 200.

**Usage Guidelines**

Use this command to associate individual SPT conditions with an iFC SPT group.

---

**Important**

An iFC SPT group may be associated with multiple SPT conditions.

---

**Examples**

The following command assigns 2 to an iFC SPT group:

```
spt-condition id 2
```
CSCF IFC Trigger Point Mode Commands

The CSCF iFC Trigger Point Configuration Mode is used to associate an Initial Filter Criteria (iFC) Service Point Trigger (SPT) group with an iFC trigger point.

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF IFC Trigger Point Configuration

```
configure > context context_name > cscf ifc-trigger-point id trigger_point_id condition-type { cnf | dnf }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-ifc-trigger-point)#
```

**Important**

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

- end, page 1376
- exit, page 1377
- spt-group, page 1378
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.
**spt-group**

Assigns an existing iFC SPT group to an iFC trigger point.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF IFC Trigger Point Configuration

configure > context context_name > cscf ifc-trigger-point id trigger_point_id condition-type \{ cnf | dnf \}

Entering the above command sequence results in the following prompt:

(context_name)host_name(config-cscf-ifc-trigger-point)#

**Syntax Description**

\[ no \] spt-group id group_id

- **no**
  - Removes the specified CSCF iFC SPT group from the iFC trigger point.

  **spt-group id group_id**
  - Specifies the ID of an existing iFC SPT group.

  *group_id* must be an integer from 1 to 200.

**Important**

An iFC SPT group can be assigned to more than one iFC trigger point.

**Usage Guidelines**

Use this command to associate an iFC SPT group with an iFC trigger point.

**Examples**

The following command assigns iFC SPT group 2 to an iFC trigger point:

spt-group id 2
CSCF ISC Template Configuration Mode

The CSCF ISC Template Configuration Mode is used to configure the IMS Service Control (ISC) interface within the system.

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF ISC Template Configuration

```
configure > context context_name > cscf isc-template id template_id
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-isc-tmpl)#
```

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

- cnsa, page 1380
- end, page 1382
- exit, page 1383
- filter-criteria, page 1384
Core Network Service Authorization (CNSA) related commands used to create media profile and service ids.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF ISC Template Configuration

`configure > context context_name > cscf isc-template id template_id`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-isc-tmpl)#
```

**Syntax Description**

```
cnsa { media-profile-id profile_id [ service-id service_id ] [ service_id ]... [ service_id ] }
no cnsa { media-profile-id [ service-id service_id ] [ service_id ]... [ service_id ] }
```

**media-profile profile_id**

Specifies the cnsa media profile id.

*profile_id* must be an integer from 0 to 10.

The media profile id is assigned to a service policy using the *cnsa-media-profile* command under CSCF Service configuration.

---

**Important**

You can only create one media profile id per ISC template.

```
service-id service_id
```

Specifies the cnsa service id(s). These ids represent URN parameters which are ICSI (IMS Communication Service Identifier) values that are mapped to a service profile through a media profile id.

*service_id* must be from 1 to 79 alpha and/or numeric characters.

```
no cnsa { media-profile-id [ service-id service_id ] [ service_id ]... [ service_id ] }
```

Removes a media profile or service id(s).
Usage Guidelines

Use this command to configure cnsa media profile ids and service ids. Information for core network authorization is received from HSS. It contains a list of service ids and a media profile id. Since the media profile id is an integer value, the S-CSCF needs to have a static database that contains the mapping between the integer value and the subscribed media profile. The media profile id is assigned to this service policy using the `cnsa-media-profile` command under CSCF Service configuration.

The S-CSCF selects the service profile based on the media profile id set and the policies, such as enforce-codec-policy and video-sessions, will be matched with the incoming request. Other policies, if configured, will be ignored in this scenario.

Examples

The following command defines the media profile id as 2:

```
cnsa media-profile-id 2
```

The following command defines several service ids:

```
cnsa service-id xxx:exampletelephony.version1 xxx:abc.com
```
end

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

Product
All

Privilege
Security Administrator, Administrator

Syntax Description
dend

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

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

Product
All

Privilege
Security Administrator, Administrator

Syntax Description
exit

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

Configure the filter criteria to be used by this template.

**Product**

SCM (S-CSCF)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF ISC Template Configuration  
`configure > context context_name > cscf isc-template id template_id`

Entering the above command sequence results in the following prompt:

`(context_name)host_name(config-cscf-isc-tmpl)#`

**Syntax Description**

| no | filter-criteria id criteria_id |

**no**

Removes the specified filter criteria.

**id criteria_id**

Specifies the ID of existing filter criteria to be used by this template. The particular criteria applied to a subscriber will be based on the priority parameter.

*criteria_id* must be an integer from 1 to 200.

**Important**

Filter criteria can be assigned to more than one ISC template.

**Usage Guidelines**

Use this command to configure the filter criteria to be used by this template.

**Examples**

The following command identifies the filter criteria 1:

`filter-criteria id 1`
CSCF Last Route Profile Criteria Configuration Mode Commands

The CSCF Last Route Profile Criteria Configuration Mode is used to configure county names and assign them Last Routing Option (LRO) numbers to be used by the CSCF last route profile. The S-CSCF forwards emergency call packets to the correct Public Safety Answering Point (PSAP) based on this criteria, which it receives from a peer server.

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Last Route Profile Criteria Configuration

configure > context context_name > csf last-route-profile name profile_name criteria { county-name | round-robin }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-criteria_type=lro-profile)#

Important

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

- county-name, page 1386
- end, page 1388
- exit, page 1389
**county-name**

Configure county names and assign them Last Routing Option (LRO) numbers to be used by the CSCF last route profile.

**Product**

SCM (S-CSCF)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Last Route Profile Criteria Configuration
configure > context context_name > csf last-route-profile name profile_name criteria { county-name | round-robin }

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-criteria_type-lro-profile)#
```

**Syntax Description**

```
county-name county_name lro-number value
| no | county-name county_name
```

- **county_name**
  Specifies the county name.
  `county_name` must be from 1 to 79 alpha and/or numeric characters in length.

- **lro-number value**
  Specifies an existing LRO number.
  `value` can be a maximum of ten digits in length.

- **no county-name county_name**
  Removes the specified county name.

**Usage Guidelines**

Use this command to configure county names and assign them LRO numbers.

**Important**

You may configure up to 100 county names.
Examples

The following command creates a county name called *norfolk* and assigns it an LRO number of 8884384357:

```
county-name norfolk lro-number 8884384357
```
**end**

Exits the current 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.
CSCF NPDB Client Configuration Mode

Commands

The NPDB Client Configuration Mode is used to set various commands supporting the role of the NPDB (Number Portability Data Base) client. The NPDB client in a CSCF service performs query for called subscriber number on NPDB server, which returns the Routing Number for the query.

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration > NPDB Client Configuration

`configure > context context_name > csf service service_name > serving-csf > npdb-client client_name`

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-npdb-client)#
```

**Important**

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

- bind, page 1392
- end, page 1394
- exit, page 1395
- npdb-primary-server, page 1396
- npdb-secondary-server, page 1397
- timeout, page 1398
**bind**

Binds the NPDB client to an IP address.

**Product**

SCM (S-CSCF)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration > NPDB Client Configuration

configure > context context_name > escf service service_name > serving-escf > npdb-client client_name

Entering the above command sequence results in the following prompt:

```
=context_name\host_name\(config-npdb-client)#
```

**Syntax Description**

```
bind address IPv4_address system-id system_id id client_id | encrypted | password password
no bind
```

- **address IPv4_address**
  Specifies the NPDB client IP address to establish the TCP connection with NPDB server.
  `IPv4_address` must be expressed in dotted decimal notation for IPv4.

- **system-id system_id**
  Specifies the identifier of the system performing query to NPDB server.
  `system_id` must be an unsigned integer from 0 to 4294962295.

- **id client_id**
  Specifies the ID of the NPDB client.
  `client_id` must be from 1 to 15 alpha and/or numeric characters.

  ```
  | encrypted | password password
  ```
  Specifies the password of the NPDB client and whether it is encrypted.

  - **password password** must be from 1 to 15 alpha and/or numeric characters.
  - **encrypted password password** must be from 1 to 132 alpha and/or numeric characters.
Important Normally, encrypted passwords are only used inside configuration files

no bind
Removes the binding of the NPDB client.

Usage Guidelines
Use this command to establish the NPDB client parameters for TCP connection with NPDB server.

Important This command can be entered multiple times to identify multiple IP addresses.

In connected state, only NPDB client will be able to send query messages to get routing number from NPDB server. When query message is received in non-connected state from core, the NPDB client sends an error message to CSCF core.

Examples
The following command binds the NPDB client to an IP address of 1.2.3.4, system ID of 4294, client ID of asdds, and encrypted password A01h4b5t5rojj205dhrete:

bind address 1.2.3.4 system-id 4294 id asdds encrypted password A01h4b5t5rojj205dhrete
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.
npdb-primary-server

Configure the NPDB primary server.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration > NPDB Client Configuration

configure > context context_name > csf service service_name > serving-cscf > npdb-client client_name

Entering the above command sequence results in the following prompt:

`{context_name}@host_name(config-npdb-client)#`

**Syntax Description**

npdb-primary-server { address IPv4_address | domain domain } port port_number

no npdb-primary-server

- **address IPv4_address | domain domain**
  Specifies the NPDB primary server.
  - **address IPv4_address**: IP addresses must be expressed in dotted decimal notation for IPv4.
  - **domain domain**: Domain name must be entered using from 1 to 255 alpha and/or numeric characters.

- **port port_number**
  Specifies the port at which NPDB primary server listens.
  **port_number** may be an integer from 1024 to 65534.

- no
  Removes the NPDB primary server.

**Usage Guidelines**
Use this command to configure the NPDB primary server.

**Examples**
The following command adds an NPDB primary server with an IP address of 1.2.3.4 and a port number of 3878:

npdb-primary-server address 1.2.3.4 port 3878
npdb-secondary-server

Configure the NPDB secondary server.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration > NPDB Client Configuration

```
configure > context context_name > cscf service service_name > serving-cscf > npdb-client client_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-npdb-client)#
```

**Syntax Description**

```
npdb-secondary-server { address IPv4_address | domain domain } port port_number
no npdb-secondary-server
```

- **address IPv4_address | domain domain**
  Specifies the NPDB secondary server.
  - **address IPv4_address**: IP addresses must be expressed in dotted decimal notation for IPv4.
  - **domain domain**: Domain name must be entered using from 1 to 255 alpha and/or numeric characters.

- **port port_number**
  Specifies the port at which NPDB secondary server listens.
  - **port_number**: may be an integer from 1024 to 65534.

- **no**
  Removes the NPDB secondary server.

**Usage Guidelines**

Use this command to configure the NPDB secondary server.

**Examples**

The following command adds an NPDB secondary server with an IP address of 1.2.3.5 and a port number of 3878:

```
npdb-secondary-server address 1.2.3.5 port 3878
```
timeout

Sets timeout values for NPDB client.

Product
SCM (S-CSCF)

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration > NPDB Client Configuration

configure > context context_name > scf service service_name > serving-cscf > npdb-client client_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-npdb-client)#

Syntax Description

timeout { bind-response sec | error-response sec | idle sec | ping sec | ping-response sec | query-response sec | release-response sec | tcp-retry sec }
[ default | no | timeout { bind-response | error-response | idle | ping | ping-response | query-response | release-response | tcp-retry }

bind-response sec
Default: 30
This timer is used to specify the timeout for connection path creation in seconds. sec must be an integer from 1 to 5000.

error-response sec
Default: 30
This timer is used to specify the timeout for error response in seconds. sec must be an integer from 1 to 5000.

idle sec
Default: 30
This timer is used to specify the timeout interval for retrying failed NPDB BIND in seconds. sec must be an integer from 1 to 5000.
ping sec
Default: 20
This timer is used to specify the timeout to send ping message to make the connection alive in seconds. sec must be an integer from 1 to 5000.

ping-response sec
Default: 30
This timer is used to specify the timeout for ping response in seconds. sec must be an integer from 1 to 5000.

query-response sec
Default: 6
This timer is used to specify the timeout for query response in seconds. sec must be an integer from 1 to 5000.

release-response sec
Default: 30
This timer is used to specify the timeout for release response in seconds. sec must be an integer from 1 to 5000.

tcp-retry sec
Default: 15
This timer is used to specify the timeout interval for retrying failed TCP connection in seconds. sec must be an integer from 1 to 5000.

default
Returns the command to the default settings. See keywords above for specific defaults.

no
Deletes the value configured for the specified timer.

Usage Guidelines
Use this command to configure timeout values for NPDB client.

When CSCF service is started, NPDB client establishes TCP connections with NPDB primary and secondary servers (if configured) and sets the connection path by sending Bind message to server. If NPDB client fails to establish TCP connection to either of the servers, it will retry the connection every TCPRetryTimer interval until it is successful. When the connection is successful, NPDB client will go to the connected state and will start PingTimer. Whenever NPDB client receives service request from CSCF core, it sends the request based on the connected state of the server(s); it should always give higher preference to the primary server. When it fails to send a query message to server, NPDB client returns failure to the core. If both servers are not in connected state, NPDB client will send failure message to CSCF core.
Examples

The following command sets the release response timeout to 64 seconds:

```
timeout release-response 64
```
CSCF PCRF-Policy-Control Configuration Mode Commands

The PCRF-Policy-Control Configuration Mode is used to enable PCRF policy control within the service.

Command Modes

Exec > Global Configuration > Context Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF PCRF-Policy-Control Configuration

```plaintext
configure > context context_name > scsf service service_name > proxy-cscf > pcrf-policy-control
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name (config-pcrf-policy-control) #
```

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

- authorization inactive-media, page 1402
- authorization mediatype, page 1403
- authorization policy-interworking-failure, page 1405
- end, page 1406
- exit, page 1407
- signaling-bearer-loss, page 1408
authorization inactive-media

Enables policy authorization for calls with inactive media.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF PCRF-Policy-Control Configuration

configure > context *context_name* > csf service *service_name* > proxy-cscf > pcrf-policy-control

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-pcrf-policy-control)#

**Syntax Description**

| default | no | authorization inactive-media |

- **default**
  Calls with all media lines in the inactive state are authorized via Rx.

- **no**
  Calls with all media lines in the inactive state will not be authorized via Rx.

**Usage Guidelines**
Use this command to enable or disable policy authorization for calls with inactive media. The media will be considered inactive when all m lines in SDP are in inactive state.

**Examples**
The following command enables policy authorization for calls with inactive media:

authorization inactive-media
authorization mediatype

Enables media authorization, using external PCRF via Rx, of specific media types (present in the SDP of a SIP message) only.

**Product**  
SCM (P-CSCF, A-BG)

**Privilege**  
Administrator

**Command Modes**  
Exec > Global Configuration > Context Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF PCRF-Policy-Control Configuration

```plaintext
configure > context context_name > csf service service_name > proxy-cscf > pcrf-policy-control
```

Entering the above command sequence results in the following prompt:

```
(context_name) host_name (config-pcrf-policy-control)#
```

**Syntax Description**  

```plaintext
[ no ] authorization mediatype { application | audio | control | data | message | others | text | video }
```

mediatype { application | audio | control | data | message | others | text | video }

Enables the external authorization of calls for the following SDP media types:

- application
- audio
- control
- data
- message
- others
- text
- video

```plaintext
no
```

Disables external authorization for the specified media type.

**Usage Guidelines**  

As Per 3GPP 29.214V8.5, P-CSCF/A-BG will authorize VOIP calls only for the media types enabled via this command. The P-CSCF/A-BG sends all media information for all supported media types present in SDP in
AAR message to PCRF via Rx. For the other (unsupported) media types, P-CSCF will not send media information in AAR.

By default, media authorization for all the media types is enabled.

**Examples**

- Enables the P-CSCF to authorize calls for audio media types:
  ```
  authorization mediatype audio
  ```

- Disables the authorization of calls for audio media types:
  ```
  no authorization mediatype audio
  ```
authorization policy-interworking-failure

Allows/rejects a session based on configuration in case of failure from PCRF.

**Product**

SCM (P-CSCF, A-BG)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF PCRF-Policy-Control Configuration

configure > context context_name > csf service service_name > proxy-cscf > pcrf-policy-control

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-pcrf-policy-control)#
```

**Syntax Description**

```
authorization policy-interworking-failure { session-continue | session-reject [ response-code code ] } 

default authorization policy-interworking-failure
```

**session-continue**

P-CSCF continues session in case of failure from PCRF.

**session-reject**

P-CSCF rejects session in case of failure from PCRF.

**response-code code**

Specifies SIP response code for rejected session.

`number` must be an integer from 400 to 699. Default is 500.

**default**

By default, session-reject is activated to reject session with default response code 500.

**Usage Guidelines**

Use this command to configure for policy interworking failure. Allow or reject a session based on configuration in case of failure from PCRF.

**Examples**

The following command rejects session in case of failure from PCRF with SIP response code 450:

```
authorization policy-interworking-failure session-reject response-code 450
```
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.
signaling-bearer-loss

Enables subscription to Notification of Signaling Transmission Path Status, as well as IPCAN Change type notification. This command is enabled by default.

**Product**

SCM (P-CSCF, A-BG)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF PCRF-Policy-Control Configuration

configure > context context_name > csf service service_name > proxy-cscf > pcrf-policy-control

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no ] signaling-bearer-loss subscription
```

**no**

Disables subscription to Notification of Signaling Transmission Path Status, as well as IPCAN Change type notification.

**subscription**

Enables subscription to Notification of Signaling Transmission Path Status, as well as IPCAN Change type notification.

**Usage Guidelines**

Use this command to enable or disable subscription to Notification of Signaling Transmission Path Status, as well as IPCAN Change type notification.

When enabled, the P-CSCF/A-BG sends AAR to the external PCRF via the Rx interface after UE registration. When disabled, the P-CSCF/A-BG will not subscribe to any event during Registration with PCRF and no diameter session will be established.

**Examples**

Enables subscription to Notification of Signaling Transmission Path Status, as well as IPCAN Change type notification:

```
signaling-bearer-loss subscription
```
Disables subscription to Notification of Signaling Transmission Path Status, as well as IPCAN Change type notification:

no signaling-bearer-loss subscription
signaling-bearing-loss
CSCF Peer Servers Configuration Mode Commands

The CSCF Peer Servers Configuration Mode is used to configure peer servers (for next-hop session routes) within the system.

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration

```
configure > context context_name > scsf peer-servers server_name type { bgcf | ibcf | icscf | mgcf | mrcf |
pcsf | sesf | sip-as }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name (config-cscf-peer-servers-group) #
```

**Important**

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

- end, page 1412
- exit, page 1413
- hunting-method, page 1414
- server, page 1415
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.
hunting-method

Configures the method by which server is contacted.

Product
SCM

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration
configure > context context_name > cscf peer-servers server_name type { bgcf | ibcf | icscf | mgcf | mrcf | pcscf | scscf | sip-as }

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

Syntax Description
hunting-method { round-robin | sequence-on-failure | weighed }
default hunting-method

default
Specifies that the server will be used in round-robin fashion.

round-robin | sequence-on-failure | weighed
Specifies the hunting method for the server.

round-robin: Specifies that the server will be used in round-robin fashion. This is the default setting.
sequence-on-failure: Specifies that the server will be used sequentially if a failure occurs on a server (i.e., first peer server is always used, except on failure, during which next peer server in the list will be used).
weighed: Specifies that the peer server has a set "weight" that determines use as compared to the other like-configured peer servers. The actual weight of the peer server is configured in the server command in this mode.

Usage Guidelines
Use this command to configure the method that is used by the system to connect to the peer server.

Examples
The following command sets the hunting method for a server to contact sequentially only when a server fails:
hunting-method sequence-on-failure
**server**

Configures the name, IP address, and port of servers belonging to this peer server and enters the Server Configuration Mode.

**Product**

SCM

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration

```
configure > context context_name > cscf peer-servers server_name type { bgcf | ibcf | icsef | mgcf | mrcf | pcscf | scscf | sip-as }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-peer-servers-group)#
```

**Syntax Description**

```
server name { address ip_address | domain domain_name } | port number ] | transport { tcp | udp } | | weight number ]
no server name

no
```

Removes the specified server from the group.

```
name
```

Specifies a name for the server. *name* must be from 1 to 79 alpha and/or numeric characters in length.

```
address ip_address
```

Specifies the IP address of the server. *ip_address* is expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

```
domain domain_name
```

Specifies the domain name of the peer server. *domain_name* must be from 1 to 255 alpha and/or numeric characters in length.

```
port number
```

Specifies the port number of the server.

*number* must be an integer value from 1 to 65535.
transport \{ tcp | udp \}

Specifies the transport type (TCP or UDP).

weight number

Default: 5

Specifies a weighted number for the specific peer server for load balancing purposes. number must be an integer value from 1 to 10. Higher weight implies larger server capability (and more routed requests).

Important

This keyword is only valid if the weighed keyword is applied to the hunting-method command in this mode.

Usage Guidelines

Use this command to configure servers and enter the Server Configuration Mode.

Entering this command results in the following prompt:

\(\text{context}\_\text{name}\hbox{}\text{hostname}(\text{config}\_\text{server}\_\text{name}\hbox{}\text{peer}\_\text{server})\#\)

Server Configuration Mode commands are defined in the CSCF Peer Server Monitoring Configuration Mode Commands chapter.

Examples

The following command configures a server named scscf5 with an IP address of 1.2.3.4 and a port number of 5060:

server scscf5 address 1.2.3.4 port 5060
CSCF Peer Servers Group Configuration Mode Commands

The CSCF Peer Servers Group Configuration Mode is used to configure peer servers lists within a peer servers group.

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Peer Servers Group Configuration

configure > context context_name > cscf peer-servers-group group_name type sip-as

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-cscf-peer-servers-group)#
```

**Important**

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

- end, page 1418
- exit, page 1419
- peer-servers, page 1420
**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.
peer-servers

Configures peer servers lists in the peer servers group.

Product
SCM

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Peer Servers Group Configuration
<context_name> > cscf peer-servers-group group_name type sip-as

Syntax Description
peer-servers list_name { default | mode { active | standby } }
no peer-servers list_name

list_name
Specifies a name for the peer servers list. list_name must be from 1 to 79 alpha and/or numeric characters in length.

default
Specifies that the peer servers list is default.

mode { active | standby }
Specifies whether the peer servers list is active or standby.

Usage Guidelines
Use this command to manage peer servers lists in a peer servers group.

Important
There can be one active, one standby, and one default peer servers list in a peer servers group.
**Examples**

The following command configures an active peer servers list named *active_as_list*:

```
peer-servers active_as_list mode active
```
CSCFPeerServerMonitoringConfigurationMode

The CSCF Peer Server Monitoring Configuration Mode is used to configure an individual peer server's monitoring parameters and operational mode. It also associates a network session template with the server.

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration > Server Configuration

```
configure > context context_name > cscf peer-servers server_name type { bgcf | ibcf | icscf | mgcf | mrcf | pcscf | sscf | sip-as } > server server_name { address ip_address | domain domain_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-server_name-peer-server)#
```

Important

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

- dummy-as, page 1424
- end, page 1425
- exit, page 1426
- ims-capable, page 1427
- lro-selection-profile, page 1428
- mode, page 1429
- monitor-status, page 1430
- nw-session-template, page 1432
- registration, page 1433
- tps-rate, page 1434
dummy-as

Sets a response code for Dummy-AS peer server.

Product

SCM (S-CSCF)

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration > Server Configuration

configure > context context_name > cscf peer-servers server_name type { bgcf | ibcf | icscf | mgcf | mrcf | pcscf | scscf | sip-as } > server server_name { address ip_address | domain domain_name }

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-server_name-peer-server)#

Syntax Description

dummy-as custom-response-code SIP_response_code
default dummy-as custom-response-code

custom-response-code SIP_response_code

If the peer server is configured as dummy-as and it is chosen as per routing table configured, a UMM response message will be formed with the response code configured and sent as reply to incoming MESSAGE/PUBLISH requests.

SIP_response_code must be an integer from 200 to 699.

Important

The response code can be 2xx/4xx/5xx/6xx; 3xx,401,and 407 are not allowed.

default dummy-as custom-response-code

Sets the response code to 200.

Usage Guidelines

Use this command to configure a response code for Dummy-AS. If this mode is selected, then MESSAGE/PUBLISH requests will be responded to by S-CSCF with configured response code.

Examples

The following command configures AS as Dummy-AS with a corresponding response code of 425:

dummy-as custom-response-code 425
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.
ims-capable

 Indicates whether the peer server belongs to a 3GPP/IMS network or a non-IMS network such as the Internet. This command is used to determine at the S-CSCF whether SIP signaling inter-working is needed when the calls are forwarded to external networks.

**Product**

SCM (S-CSCF)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration > Server Configuration

`configure > context context_name > csf peer-servers server_name type { bgcf | ibcf | icscf | mgcf | mrcf | pcscf | scscf | sip-as } > server server_name { address ip_address | domain domain_name )`

Entering the above command sequence results in the following prompt:

`(context_name)host_name(config-server_name-peer-server)#`

**Syntax Description**

| no | ims-capable

**Usage Guidelines**

Use this command to identify a peer server as IMS capable allowing the S-CSCF to use SIP signalling inter-working when forwarding calls to non-IMS capable networks.
Iro-selection-profile

Binds a CSCF last route profile with the peer server.

Product  
SCM

Privilege  
Administrator

Command Modes  
Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration > Server Configuration

configure > context context_name > cscf peer-servers server_name type { bgcf | ibcf | icsf | mgcf | mrpf | pcscf | scscf | sip-as } > server server_name { address ip_address | domain domain_name }

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-server_name-peer-server)#

Syntax Description  
Iro-selection-profile name profile_name
no Iro-selection-profile

Iro-selection-profile name profile_name

profile_name must be an existing CSCF last route profile and be from 1 to 79 alpha and/or numeric characters.

no Iro-selection-profile

Removes CSCF last route profile from the peer server group.

Usage Guidelines  
Use this command to identify a CSCF last route profile to use for finding the correct Public Safety Answering Point (PSAP) during emergency calls.

Examples  
The following command assigns a CSCF last route profile named lro1 to the peer server group:

Iro-selection-profile name lro1

The following command removes a CSCF last route profile from the peer server group:

no Iro-selection-profile
mode

Sets the peer server mode to either active or standby. By default, peer servers are in active mode.

Product
SCM

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration > Server Configuration

```bash
configure > context context_name > cscf peer-servers server_name type { bgcf | ibcf | icsef | mgcf | mrcf | pcscf | scscf | sip-as } > server server_name { address ip_address | domain domain_name }
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-server_name-peer-server)#
```

Syntax Description
mode { active | standby }

active
Defines the mode of the CSCF peer server as active.

standby
Defines the mode of the CSCF peer server as standby.

Usage Guidelines
Use this command to set the peer server mode to either active or standby.

Examples
The following command sets the peer server's mode to standby:
**mode standby**
**monitor-status**

Sets parameters for monitoring the status of peer servers.

**Product**

SCM

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration > Server Configuration

```bash
configure > context context_name > escf peer-servers server_name type { bgcf | ibcf | icscf | mgcf | mrcf | pcscf | scscf | sip-as } > server server_name { address ip_address | domain domain_name }
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-server_name-peer-server)#
```

**Syntax Description**

```bash
monitor-status { max-response-codes negative max | [ monitor-interval seconds ] | [ monitor-message options | max-forwards max | response-timer seconds ] | [ monitor-response-timer seconds ] | [ response-code { positive SIP_response_code | negative SIP_response_code } | timer | mark-out-of-service seconds ] | [ unavailable-monitor-interval seconds | [ unavailable-notification seconds ] } }

no monitor-status { monitor | response-code [ negative | positive ] [ SIP_response_code ] }
```

**max-response-codes negative max**

Default: 1

Specifies the maximum number of negative response codes to receive to mark server unavailable. `max` must be an integer from 1 to 10.

**monitor-interval seconds**

Default: 30

Specifies the interval that peer server monitoring will occur. `seconds` must be an integer from 1 to 65535.

**monitor-message options | max-forwards max | response-timer seconds |**

Specifies that SIP message (OPTIONS) are to be sent periodically after each monitoring interval.

**max-forwards max**: Max-forwards in number of hops. `max` must be an integer from 0 to 70.

**response-timer seconds**: Response wait timer in seconds. `seconds` must be an integer from 1 to 65535.
**monitor-response-timer seconds**
Default: 180
Specifies the interval that the CSCF will wait for responses from the peer server.
*seconds* must be an integer from 1 to 65535.

**response-code { positive SIP_response_code | negative SIP_response_code }**
Specifies the Options Message response codes.
**negative**: Negative response codes. *SIP_response_code* must be an integer from 300 to 699.
**positive**: Positive response codes. *SIP_response_code* must be an integer from 200 to 299.

**timer mark-out-of-service seconds**
Default: 864000
Timer to mark server out-of-service from unavailable state.
*seconds* must be an integer from 0 to 2147483646.

**timer unavailable-monitor-interval seconds**
Periodic monitor interval to be used when server is marked as unavailable.
*seconds* must be an integer from 0 to 2147483646.

**timer unavailable-notification seconds**
Default: 180
Time after which to send notification to operations administrator.
*seconds* must be an integer from 0 to 2147483646.

**no monitor-status { monitor | response-code [ negative | positive ] | SIP_response_code | }**
Disables peering server status monitoring.

**Usage Guidelines**
Use this command to set parameters for monitoring the status of a peer server.

**Examples**
The following command sets the monitoring interval to three minutes (180 seconds) and the response timer to six minutes (360 seconds):
`monitor-status monitor-interval 180 monitor-response-timer 360`
nw-session-template

Specifies a session template for sessions terminating from the peer server group.

**Product**
SCM

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration > Server Configuration

```
configure > context context_name > cscf peer-servers server_name type { bgcf | ibcf | icscf | mgcf | mrcf | pcscf | scscf | sip-as } > server server_name { address ip_address | domain domain_name }
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-server_name-peer-server)#
```

**Syntax Description**
```
nw-session-template name template_name
no nw-session-template

name template_name
```

*template_name* must be an existing session template created in the Session Template Configuration Mode.

```
no
```

Removes session template from the peer server group.

**Usage Guidelines**
Use this command to identify a session template to use for sessions terminating from the peer server group.

**Examples**
The following command identifies a session template named *template-25* to use for sessions terminating from the peer server group:
```
nw-session-template template-25
```
registration

This command specifies whether the S-CSCF skips third party registration to the Application Server (AS) by a configured time after initial registration.

**Product**

SCM (S-CSCF)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration > Server Configuration

configure > context context_name > cscf peer-servers server_name type { bgcf | ibcf | icscf | mgcf | mrcf | pscef | scscf | sip-as } > server server_name { address ip_address | domain domain_name }

Entering the above command sequence results in the following prompt:

\[(context_name)host_name(config-server_name-peer-server)#\]

**Syntax Description**

registration skip-count count

no registration skip-count

skip-count count

Number of times to skip third party registration.

count must be an integer from 0 (default) to 60.

no registration skip-count

The S-CSCF does not skip third party registration to the AS by a configured time after initial registration.

**Usage Guidelines**

Use this command to specify whether the S-CSCF skips third party registration to the Application Server (AS) by a configured time after initial registration. After skipping the configured number of times, the third party register should be sent again to AS to reduce overload on AS.

**Examples**

The following command sets the number of times to skip third party registration to 25:

registration skip-count 25
tps-rate

Controls the rate of messages based on Transactions Per Second (TPS) from S-CSCF towards the peer server application server (AS).

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration > Server Configuration

```bash
configure > context context_name > cscf peer-servers server_name type { bgcf | ibcf | iccsef | mgcf | mrcf | pcscf | scscf | sip-as } > server server_name { address ip_address | domain domain_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-server_name-peer-server)#
```

**Syntax Description**

```
tps-rate rate [ exclude Register ]
no tps-rate
```

**rate**
TPS from S-CSCF towards the peer server AS.

*rate* must be an integer from 1 to 1000.

**exclude Register**
Specifies that for Register method, TPS rate need not be applied.

**no**
TPS rate not applied from S-CSCF towards the peer server AS.

**Usage Guidelines**
Use this command to control the TPS towards the peer server AS. If TPS rate is exceeded, the incoming requests will be rejected with 500 error response; Retry-After Header specifies the number of seconds before UE should retry.

**Examples**
The following command sets the TPS rate towards the AS to 25:

```bash
tps-rate 25
```
CSCF Policy Configuration Mode Commands

The CSCF Policy Configuration Mode is used to manage AoR policy profiles within the system. User-defined profiles can be managed in this mode.

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration

`configure > context context_name > cscf policy name policy_name`

Entering the above command sequence results in the following prompt:

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

**Important**

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

- aor-policy-rules, page 1436
- end, page 1437
- exit, page 1438
- service-policy-rules, page 1439
**aor-policy-rules**

Specifies that the newly created policy is an AoR policy and enters the AoR Policy Rules Configuration Mode.

**Product**

SCM

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration

```
configure > context context_name > cscf policy name policy_name
```

Entering the above command sequence results in the following prompt:

```
<context_name>host_name>(config-aor-policy)#
```

**Syntax Description**

aor-policy-rules

**Usage Guidelines**

Use this command to create an AoR policy group and enter the AoR Policy Rules Configuration Mode.

Entering this command results in the following prompt:

```
<context_name>hostname>(config-aor-policy)#
```

AoR Policy Configuration Mode commands are defined in the *CSCF AoR Policy Rules Configuration Mode Commands* chapter.
end

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

dend

**Usage Guidelines**

Use this command to return to the Exec mode.
exit

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

exit

Usage Guidelines

Use this command to return to the parent configuration mode.
**service-policy-rules**

Specifies that the newly created policy is a service policy and enters the Service Policy Rules Configuration Mode.

**Product**
SCM

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Policy Configuration
configure > context context_name > cscf policy name policy_name

Entering the above command sequence results in the following prompt:

```
<context_name>@hostname(config-aor-policy)#
```

**Syntax Description**
`service-policy-rules`

**Usage Guidelines**
Use this command to create a service policy group and enter the CSCF Policy Rules Configuration Mode.

Entering this command results in the following prompt:

```
<context_name>@hostname(config-service-policy)#
```

Service Policy Rule Configuration Mode commands are defined in the *CSCF Policy Rules Configuration Mode Commands* chapter.
service-policy-rules
CSCF Policy Rules Configuration Mode

Commands

The CSCF Policy Rules Configuration Mode is used to manage CSCF AoR and service policy profiles within the system.

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration

```
configure > context context_name > cscf policy { default | name policy_name } > service-policy-rules
```

—or—

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Configuration > CSCF Policy Rules Configuration

```
configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules > aor aor_name
```

Entering the above command sequences results in the following prompt:

```
[context_name]host_name(config-policy_name=aor) #
```

Important

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

- allow-noauth, page 1443
- allow-unsecure, page 1444
- authorization, page 1445
- end, page 1447
- enforce-codec-policy, page 1448
- exit, page 1449
- max-cscf-concurrent-sessions, page 1450
• policy, page 1452
• qos, page 1454
• signalling-bearer-loss, page 1456
• video-sessions, page 1457
allow-noauth

Configures the policy to allow unauthenticated access. Default is disabled.

Product
SCM

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration
configure > context context_name > cscf policy { default | name policy_name } > service-policy-rules

-or-

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Configuration > CSCF Policy Rules Configuration
configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules > aor aor_name

Entering the above command sequences results in the following prompt:

{context_name}host_name(config-policy_name-aor)#

Syntax Description
[ default | no ] allow-noauth

default | no
Disables the allow-noauth functionality for this policy.

Usage Guidelines
Use this command to allow access to subscribers without authenticating them.
allow-unsecure

Configures the policy to allow access to the system without a security association. Default is disabled.

Product
SCM

Privilege
Administrator

Command Modes

- Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration
- configure > context context_name > cscf policy { default | name policy_name } > service-policy-rules

- or -
- Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Configuration > CSCF Policy Rules Configuration
- configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules > aor aor_name

Entering the above command sequences results in the following prompt:

{context_name}host_name(config-policy_name-aor)#

Syntax Description

| default | no | allow-unsecure |

default | no

Disables the allow-unsecure functionality for this policy.

Usage Guidelines

Use this command to enable the policy to provide subscriber access to system without a security association.
**authorization**

Configures the policy to allow early bandwidth, emergency, or provisional response authorization. Default is disabled.

**Product**
SCM

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration

```
configure > context context_name > cscfpolicy {default | name policy_name } > service-policy-rules
```

-or-

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Configuration > CSCF Policy Rules Configuration

```
configure > context context_name > cscfpolicy {default | name policy_name } > aor-policy-rules > aor aor_name
```

Entering the above command sequences results in the following prompt:

```
[context_name]host_name(config-policy_name-aor)#
```

**Syntax Description**

```
[ no ] authorization { early-bandwidth | emergency { all | register | session } | prov-response }
```

**early-bandwidth**

Enables early bandwidth policy.

**emergency { all | register | session }**

Enables AA-Request (AAR) for emergency.

- **all**: Enable AAR for emergency Register and Invite.
- **register**: Enable AAR for emergency Register.
- **session**: Enable AAR for emergency Invite.

**prov-response**

Enables AAR for provisional responses like 18X.
no

Disables the early bandwidth, emergency, or provisional response authorization functionality for this policy.

Usage Guidelines

Use this command to enable the policy to provide early bandwidth, emergency, or provisional response authorization.
end

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

**Product**  
All

**Privilege**  
Security Administrator, Administrator

**Syntax Description**  
end

**Usage Guidelines**  
Use this command to return to the Exec mode.
enforce-codec-policy

Enters the Enforce Codec Policy Command Mode where allowed static and dynamic codec lists are managed.

**Product**
SCM

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration

```
configure > context context_name > csf policy { default | name policy_name } > service-policy-rules
```

or

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Configuration > CSCF Policy Rules Configuration

```
configure > context context_name > csf policy { default | name policy_name } > aor-policy-rules > aor
aor_name
```

Entering the above command sequences results in the following prompt:

```
{context_name}@host_name(config-policy_name-aor)#
```

**Syntax Description**

| default | no | enforce-codec-policy |

```
default | no
```

Disables the codec policy.

**Usage Guidelines**

Use this command to enter the Enforce Codec Policy Configuration Mode.

Entering this command results in the following prompt:

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

CSCF Enforce Codec Policy Mode commands are defined in the *Enforce Codec Policy Configuration Mode Commands* chapter in this guide.
exit

Exits the current mode and returns to the 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-cscf-concurrent-sessions

Configures the maximum number of concurrent sessions allowed per subscriber.

**Product**
SCM

**Privilege**
Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration
  ```
  configure > context context_name > cscf policy { default | name policy_name } > service-policy-rules
  ```
- or -
  ```
  Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Configuration > CSCF Policy Rules Configuration
  configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules > aor aor_name
  ```

Entering the above command sequences results in the following prompt:
```
[context_name] host_name (config-policy-name-aor)>
```

**Syntax Description**
```
max-cscf-concurrent-sessions number
default max-cscf-concurrent-sessions
```

- **number**
  
  Default: 5
  
  Specifies the number of concurrent sessions allowed per subscriber for this policy. *number* must be an integer from 1 to 100.

- **default**
  
  Resets defaults for this command.

**Usage Guidelines**

Use this command to set the maximum number of allowed sessions per subscriber for this policy.

If enabled, the `subscriber-policy-override` command in the CSCF Service Configuration Mode overrides the service-level policy.
Examples

The following command sets the maximum number of concurrent sessions for a subscriber using this policy to 7:

```
max-cscf-concurrent-sessions 7
```
**policy**

Configures the overload response for this policy. When the P-CSCF/A-BG becomes congested, this overload policy is used to reject subsequent sessions or redirect them to another server.

**Product**

SCM (P-CSCF, A-BG)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration

```
configure > context context_name > cscf policy { default | name policy_name } > service-policy-rules
```

-or-

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Configuration > CSCF Policy Rules Configuration

```
configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules > aor aor_name
```

Entering the above command sequences results in the following prompt:

```
[context_name]host_name(config-policy_name-aor)#
```

**Syntax Description**

```
policy overload { redirect address1 [ weight weight1 ] [ address2 [ weight weight2 ] ] ... | reject { use-reject-code { admin-prohibited | insufficient-resources } } } defaul

t policy overload
no policy overload redirect address1 [ address2 ] ...
```

**redirect address1 [ weight weight1 ] [ address2 [ weight weight2 ] ] ...**

Specifies that upon policy overload, the system will redirect the session to another CSCF. *address1* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.  

**weight weight1**: Defines the priority of the redirect address.  

*weight1* must be an integer from 1 to 10. Default is 1.

**reject { use-reject-code { admin-prohibited | insufficient-resources } }**

Specifies that upon policy overload, the system will reject the session. This is the default setting.  

**use-reject-code**: Specifies that a reject code will be returned upon policy overload.
• **admin-prohibited**: Specifies that the "admin-prohibited" reject code will be returned upon policy overload.

• **insufficient-resources**: Specifies that the "insufficient resources" reject code will be returned upon policy overload. This is the default reject code.

**default policy overload**

Resets defaults for this command.

**no policy overload redirect address1 [ address2 ] ...**

Removes configured policy overload redirect address(es).

**Usage Guidelines**

Use this command to define the response to an overload condition on the P-CSCF/A-BG using this AoR policy.

**Examples**

The following command configures the policy overload response to redirect to a series of CSCFs with IP address of 1.2.3.4, 1.2.3.5, and 1.2.3.6 with respective priorities (weights) of 1, 3, and 2:

```
policy overload redirect 1.2.3.4 weight 1 1.2.3.5 weight 3 1.2.3.6 weight 2
```
qos

Configures QoS bandwidth settings for uplink and downlink specific to media types.

Product

SCM

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration

configure > context context_name > cscfpolicy { default | name policy_name } > service-policy-rules

-or-

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Configuration > CSCF Policy Rules Configuration

configure > context context_name > cscfpolicy { default | name policy_name } > aor-policy-rules > aor aor_name

Entering the above command sequences results in the following prompt:

<context_name>host_name(config-policy_name-aor)>

Syntax Description

qos bandwidth { media-type { audio | other | video } | { downlink | uplink } } | peak value |

bandwidth { downlink | uplink }

downlink: Configures the downlink bandwidth.

uplink: Configures the uplink bandwidth.

peak value

Peak value of bandwidth in kilobits per second (kbit/s).

value must be an integer from 1 to 99999999.

media-type { audio | other | video }

Configures QoS bandwidth for media types.

• audio: QoS bandwidth for audio media-type.

• other: QoS bandwidth for media-types other than audio and video.

• video: QoS bandwidth for video media-type.
Usage Guidelines

The P-CSCF/A-BG fills the required bandwidth for downlink and uplink from the Session Description Protocol (SDP) in the message when communicating with an external policy server via Rx/Tx/Gq. Use this command to configure the peak uplink and downlink bandwidth to be used when the SDP does not contain bandwidth. Bandwidth configuration can now be specified per media type.

Examples

Set the media type to audio and peak uplink bandwidth to 256 kbit/s:

qos bandwidth media-type audio uplink peak 256
signalling-bearer-loss

This command enables or disables signalling bearer loss.

Product
SCM

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration

configure > context context_name > cscf policy { default | name policy_name } > service-policy-rules

–or–

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Configuration > CSCF Policy Rules Configuration

configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules > aor aor_name

Entering the above command sequences results in the following prompt:

(context_name)host_name(config-policy_name-aor)#

Syntax Description
| no | signalling-bearer-loss de-register

no

Disables signalling bearer loss for this policy.

Usage Guidelines
Use this command to trigger De-register request from P-CSCF to S-CSCF, and clear the entry of subscriber. When P-CSCF gets ASR for Signalling Bearer, it sends ASA response and triggers STR for same session ID.
**video-sessions**

Configures the policy to allow video bearers. Default is disabled.

**Product**
SCM

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration
configure > context context_name > cscf policy { default | name policy_name } > service-policy-rules
-or-
Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Configuration > CSCF Policy Rules Configuration

configure > context context_name > cscf policy { default | name policy_name } > aoR-policy-rules > aor aor_name

Entering the above command sequences results in the following prompt:

<context_name>host_name(config-policy_name-aor)#

**Syntax Description**

| default | no | video-sessions |

**Usage Guidelines**
Use this command to allow video session via this policy.
video-sessions
CSCF Prefix Table Configuration Mode

Commands

The CSCF prefix table is used to configure for each number (or number prefix) whether it is ported and the SIP routing domain. Only one CSCF prefix table can be configured per context.

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Prefix Table Configuration

configure > context context_name > cscf prefix-table

Entering the above command sequence results in the following prompt:

(context_name)host_name(config-cscf-prefix-table)#

Important

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

- end, page 1460
- exit, page 1461
- number, page 1462
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.

<table>
<thead>
<tr>
<th><strong>Product</strong></th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Privilege</strong></td>
<td>Security Administrator, Administrator</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Syntax Description</strong></th>
<th><strong>exit</strong></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>Usage Guidelines</strong></th>
<th>Use this command to return to the parent configuration mode.</th>
</tr>
</thead>
</table>
number

Determines for each number (or number prefix) in a prefix table whether it is ported and the SIP routing domain.

Product

SCM

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Prefix Table Configuration

configure > context context_name > csf prefix-table

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-csf-prefix-table)#

Syntax Description

number

number number [ported] [routing-domain domain_name]

no number number

If the number is a prefix, it should end with "."

ported

The number (or number prefix) is in ported range and NPDB (Number Portability Data Base) has to be contacted.

routing-domain domain_name

Specifies the SIP routing domain for this number (or number prefix). domain_name must be from 1 to 79 alpha and/or numeric characters in length.

no number number

Removes the specified number or number prefix from the prefix table.
Usage Guidelines

Use this command to determine whether each number (or number prefix) in a prefix table is ported and the SIP routing domain. The S-CSCF service will use the prefix table configured in its source context for the lookup.

Examples

The following command specifies a ported number prefix named $821057$ with SIP routing domain `cisco.com`:

```
number 821057$ ported routing-domain cisco.com
```
CSCF Proxy-CSCF Configuration Mode Commands

The Proxy-CSCF Configuration Mode is used to enable Diameter policy control within the service.

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

**configure > context context_name > csf service service_name > proxy-cscf**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cacf-service-proxy-cscf)#
```

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

- allow rfc3261-ua-interworking, page 1467
- atcf-atgw, page 1468
- core-reg-expiry-time, page 1469
- diameter, page 1470
- emergency, page 1474
- emergency-call-mode, page 1476
- end, page 1477
- exit, page 1478
- interrogating-cscf-role, page 1479
- message-max-size, page 1480
- network-id, page 1481
- pcfr-policy-control, page 1482
- peer-sbc, page 1483
- plmn-id, page 1485
• reg-preloaded-route, page 1486
• reg-service-route, page 1487
• reliable-prov-resp, page 1488
• restoration-procedure, page 1489
• security-parameters, page 1490
• sigcomp, page 1491
• sip-header, page 1492
• sip-param, page 1494
• store-session-path, page 1496
allow rfc3261-ua-interworking

Enables the function to allow IMS interworking with RFC3261 SIP User Agents.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration
configure > context context_name > csf service service_name > proxy-cscf

Entering the above command sequence results in the following prompt:

\[(context_name)host_name(config-cscf-service-proxy-cscf)\#

Syntax Description
|no | allow rfc3261-ua-interworking

no
Disables the interworking capability.

Usage Guidelines
Use this command to enable the P-CSCF/A-BG to allow IMS interworking with RFC3261 SIP User Agents.
**atcf-atgw**

This command enables ATCF functionality for the P-CSCF.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

```
configure > context context_name > csf service service_name > proxy-cscf
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-cscf-service-proxy-cscf)#
```

**Syntax Description**

```
| no | atcf-atgw
```

- **no**
  Disables ATCF support for P-CSCF.

**Usage Guidelines**

Use this command to enable or disable ATCF functionality for the P-CSCF. This command is disabled by default.

On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-cscf-atcf-atgw)#
```

Refer to the *CSCF ATCF-ATGW Configuration Mode Commands* chapter for additional information.
core-reg-expiry-time

Configures Registration Expiry Timer Handling in P-CSCF/A-BG to keep pin holes open in B2BUA mode.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

```shell
configure > context context_name > csf service service_name > proxy-cscf
```

Entering the above command sequence results in the following prompt:

```
/context_name)/host_name(config-cscf-service-proxy-cscf)#
```

**Syntax Description**
```
core-reg-expiry-time [default | no] core-reg-expiry-time
```

- **default**
  Sets the core-reg-expiry-time to 3600 seconds.

- **no**
  Disables the timer.

- **sec**
  Expiry age should be less than or equal to the maximum in seconds. Must be an integer from 300 to 86400.

**Usage Guidelines**
Use this command to configure Registration Expiry Timer Handling in P-CSCF/A-BG to keep pin holes open in B2BUA mode.

**Examples**
The following sets the core-reg-expiry-time to 4000 seconds:
```
core-reg-expiry-time 4000
```
diameter

This command:

- configures the Diameter dictionary used in this function.
- enables the selection of a Diameter host-select-template for PCRF server selection.
- configures the policy control origin endpoint used in this function.
- enables the selection of a Diameter policy control peer server providing Rx/Tx/Gq applications for this service.
- configures the Diameter requested timeout value used in this function.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

configure > context context_name > cscf service service_name > proxy-cscf

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-cscf-service-proxy-cscf) #

Syntax Description

diameter location-info { dictionary { e2custom01 | e2custom02 | e2custom03 | e2custom04 | e2custom05 | e2custom06 | e2custom07 | e2custom08 | e2custom09 | e2standard } | origin endpoint endpoint_name | peer-select peer peer_name | peer-realm realm_name | secondary-peer peer_name | sec-peer-realm realm_name | request-timeout sec }

In StarOS v12.0 and earlier:

diameter policy-control { dictionary { Gq-custom | Gq-standard | Rq-custom | Rx-rel8 | Rx-standard | Tx-standard | custom01 | custom02 | custom03 | custom04 | custom05 | custom06 | custom07 | custom08 | custom09 } | origin endpoint endpoint_name | peer-select peer peer_name | peer-realm realm_name | secondary-peer peer_name | sec-peer-realm realm_name | request-timeout sec }

In StarOS v12.2 and later:

diameter policy-control { dictionary { dynamic-load | gq-custom | gq-standard | rq-custom | rx-custom01 | rx-custom02 | rx-custom03 | rx-custom04 | rx-custom05 | rx-rel8 | rx-standard | tx-standard } | host-select-template template_name | origin endpoint endpoint_name | peer-select peer peer_name | peer-realm realm_name | secondary-peer peer_name | sec-peer-realm realm_name | request-timeout sec }

default diameter { location-info | policy-control } { dictionary | request-timeout }

no diameter { location-info | policy-control } { host-select-template | origin endpoint | peer-select }
**default**
Sets the Diameter's location-info or policy control dictionary or requested timeout value as the default.

**no**
Removes the Diameter location-info or policy control origin endpoint or Diameter peer from the service.

**location-info**
Defines the E2 interface for location information.

**dictionary** { e2custom01...e2custom09 | e2standard }

- **custom01...custom09**: Specifies that a customer-specific (custom) dictionary is to be used for expansion and behaviors.
- **e2standard**: Specifies that the E2-Standard-Dictionary is to be used.

---

**Important**
If this keyword is not configured, the system defaults to the default dictionary (e2standard). In the Proxy-CSCF configuration, at any time, the location-info dictionary can either be an explicitly configured dictionary or the default dictionary. Hence, there is no corresponding "no" CLI to disable the location-info dictionary setting.

**policy-control**
Defines external policy control.

**dictionary** { Gq-custom | Gq-standard | Rq-custom | Rx-rel8 | Rx-standard | Tx-standard | custom01...custom09 }

- **Gq-custom**: Specifies that the Gq Operax dictionary is to be used for Operax-specific behavior.
- **Gq-standard**: Specifies that the Gq standard dictionary is to be used.
- **Rq-custom**: Specifies that the Rq custom dictionary is to be used.
- **Rx-rel8**: Specifies that the Rx Release 8 dictionary is to be used.
- **Rx-standard**: Specifies that the Rx standard dictionary is to be used.
- **Tx-standard**: Specifies that the Tx standard dictionary is to be used.
- **custom01...custom09**: Specifies that a customer-specific (custom) dictionary, for customer-specific expansion and behaviors, is to be used.

**dictionary** { dynamic-load | gq-custom | gq-standard | rq-custom | rx-custom01 | rx-custom02 | rx-custom03 | rx-custom04 | rx-custom05 | rx-rel8 | rx-standard | tx-standard }

- **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.
- **gq-custom**: Specifies that the Gq Operax dictionary is to be used for Operax-specific behavior.
- **gq-standard**: Specifies that the Gq standard dictionary is to be used.
**rq-custom**: Specifies that the Rq custom dictionary is to be used.

**rx-custom01...rx-custom05**: Specifies that a customer-specific (custom) dictionary, for customer-specific expansion and behaviors, is to be used.

**rx-rel8**: Specifies that the Rx Release 8 dictionary is to be used.

**rx-standard**: Specifies that the Rx standard dictionary is to be used.

**tx-standard**: Specifies that the Tx standard dictionary is to be used.

**host-select-template name template_name**

Specifies the Diameter host-select-template. The host-select-template has a table of prefix and PCRF peers. When configured, PCRF server is selected using a lookup based on subscriber IMSI prefix from this table. 

`template_name` must be the template's name and an alpha and/or numeric string of 1 through 63 characters in length.

**origin endpoint endpoint_name**

Specifies the Diameter location-info or policy control endpoint name. 

`endpoint_name` must be the endpoint's name and an alpha and/or numeric string of 1 through 63 characters in length.

**peer-select peer peer_name**

Specifies the name of the Diameter location-info or policy control peer server. 

`peer_name` must be from 1 to 63 alpha and/or numeric characters in length.

Diameter peer servers are configured through the **diameter endpoint** command in the Context Configuration Mode. The **diameter endpoint** command is a generic command and can be found in the Cisco ASR 5000 Series Command Line Interface Reference.

**peer-realm realm_name**

Specifies the realm name for which the Diameter location-info or policy control peer server has responsibility. 

`realm_name` must be from 1 to 63 alpha and/or numeric characters in length.

*Important* If this keyword is not configured, the system defaults to the realm name configured for the selected peer server.

**secondary-peer peer_name**

Specifies the name of the secondary Diameter location-info or policy control peer server. 

`peer_name` must be from 1 to 63 alpha and/or numeric characters in length.

**sec-peer-realm realm_name**

Specifies the realm name for which the secondary Diameter location-info or policy control peer server has responsibility. 

`realm_name` must be from 1 to 63 alpha and/or numeric characters in length.
If this keyword is not configured, the system defaults to the realm name configured for the selected peer server.

The "diameter location-info peer-select peer <primary_peer> peer-realm <primary_peer_realm> secondary-peer <secondary_peer> sec-peer-realm <secondary_peer_realm>" CLI configures Peer Switching—selecting which peers the Diameter messages are routed to. When the secondary peer is configured, in case the primary fails, request messages are rerouted to the secondary. Note that the "no diameter location-info peer-select" CLI command will remove the entire Peer Switching CLI from the configuration.

request-timeout sec

Specifies the Diameter location-info or policy control requested timeout value in seconds.

sec must be an integer from 1 to 300.

Default: 10

If this keyword is not configured, the system defaults to the default setting (10 seconds). In the Proxy-CSCF configuration, at any time, the request-timeout setting can either be an explicitly configured value or the default value. Hence, there is no corresponding "no" CLI to disable the request-timeout setting.

Usage Guidelines

Use this command to:

- define the Diameter dictionary to use for the service.
- specify the Diameter origin endpoint.
- specify a Diameter location-info or policy control peer server to support Rx/Tx/Gq applications.
- specify the Diameter requested timeout value for this service.

Examples

The following command configures the system to use the Tx standard Diameter dictionary for this service:

diameter policy-control dictionary Tx-standard

The following command sets the Diameter location-info origin endpoint to test:

diameter location-info origin endpoint test

The following command selects a Diameter policy control peer server with a name of diam-2 and a realm name of realm-6:

diameter policy-control peer-select peer diam-2 peer-realm realm-6
**emergency**

Configures the function to allow or disallow the emergency-session or emergency-registration of a particular type.

**Product**

SCM (P-CSCF, A-BG, SIP Proxy)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

`configure > context context_name > cscf service service_name > proxy-cscf`

Entering the above command sequence results in the following prompt:

`{context_name}@host_name(config-cscf-service-proxy-cscf)#`

**Syntax Description**

`[default | no] emergency { registration [ visited-ue ] | session [ 3gpp-ims-xml-body | anonymous | non-emergency-registered | sdp-cs-media | visited-ue ] }`

- **default**
  
  Specifies that the emergency-session or emergency-registration of a particular type can be allowed.

- **no**
  
  Disallows the emergency-session or emergency-registration of a particular type.

- **registration [ visited-ue ]**
  
  Allow emergency-registration. By default, it's allowed.

  **visited-ue**: Allow emergency-registration from a visited UE. By default, it's allowed.

- **session [ 3gpp-ims-xml-body | anonymous | non-emergency-registered | sdp-cs-media | visited-ue ]**
  
  Specifies the type of emergency-session to be allowed or disallowed. By default, all are allowed.

  **3gpp-ims-xml-body**: Allow 3GPP IM CN XML body to be added in 380 response messages.

  **anonymous**: Allow anonymous subscribers (unregistered UEs) to initiate emergency sessions.

  **non-emergency-registered**: Allow non-emergency registered subscribers to initiate emergency sessions.

  **sdp-cs-media**: Allow emergency calls with SDP CS Media.

  **visited-ue**: Allow emergency calls from visited UE.
Usage Guidelines

Use this command to configure the function to allow or disallow the emergency-session or emergency-registration of a particular type.

Examples

The following command configures the function to allow non-emergency registered subscribers to initiate emergency sessions:

`emergency session non-emergency-registered`
emergency-call-mode

Enables the P-CSCF/A-BG service to add "P-Emergency-Call-Mode-Preference" header in 200OK to REGISTER message. By default, this command is disabled.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

```
configure > context context_name > cscf service service_name > proxy-cscf
```

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

**Syntax Description**
```
emergency-call-mode { 3gpp-cs | 3gpp-ims }
[ default | no ] emergency-call-mode
```

- **default**
  Specifies 3GPP IMS access preference in header.

- **no**
  Disables "P-Emergency-Call-Mode-Preference" header insertion for the P-CSCF/A-BG service.

- **3gpp-cs | 3gpp-ims**
  - **3gpp-cs**: Specifies 3GPP CS access preference in header.
  - **3gpp-ims** (default): Specifies 3GPP IMS access preference in header.

**Usage Guidelines**
Enabling this command allows the P-CSCF or A-BG to add a "P-Emergency-Call-Mode-Preference" header in 200OK to REGISTER message.

**Examples**
The following command enables "P-Emergency-Call-Mode-Preference" header insertion with a 3GPP CS access preference defined:
```
emergency-call-mode 3gpp-cs
```
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.
interrogating-cscf-role

Enables the function to also perform as an Interrogating-CSCF.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

```bash
configure > context context_name > cscf service service_name > proxy-cscf
```

Entering the above command sequence results in the following prompt:

```bash
<context_name>@host_name(config-cscf-service-proxy-cscf)>
```

**Syntax Description**

```
| no | interrogating-cscf-role
```

- **no**
  Disables the Interrogating-CSCF role in this function.

**Usage Guidelines**

Use this command to enable the P-CSCF/A-BG to also perform as an Interrogating-CSCF.

---

**Important**

All Interrogating-CSCF functions have been moved to the Serving-CSCF exclusively in v10.0 and beyond.
message-max-size

Configures the maximum message body size in MESSAGE method.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

configure > context context_name > csf service service_name > proxy-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-proxy-cscf)#

Syntax Description

message-max-size limit
| default | no | message-max-size

default | no

Returns/sets the maximum SIP message size to 1024 bytes.

limit

Default: 1024

Configures the maximum SIP message size limit in bytes for any SIP message buffer.

limit must be an integer from 512 to 65535.

Important

Message body size should be less than the max-sipmsg-size set in the CSCF Service Configuration Mode.

Usage Guidelines

Use this command to configure the maximum SIP message size for any SIP message buffer.

Examples

The following command limits the SIP message size to 4000 bytes:

message-max-size 4000
network-id

Configures the Network Identifier.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

```
configure > context context_name > cscf service service_name > proxy-cscf
```

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-cscf-service-proxy-cscf)#
```

**Syntax Description**

```
[ no ] network-id id
```

- **no**
  Removes the configured Network Identifier of the entity.

- **id**
  The Network Identifier of the entity.
  *id* must be from 1 to 79 alpha and/or numeric characters in length.

**Usage Guidelines**
The Network Identifier is used by the P-CSCF or A-BG to fill the P-Visited-Network-ID header.

**Examples**
Sets the Network Identifier to *pcscf01.company.com*:
```
network-id pcscf01.company.com
```
pcrf-policy-control

Enables external policy control via PCRF through the Rx Diameter interface and enters the PCRF-Policy-Control Configuration Mode. Default is disabled.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

configure > context context_name > cscf service service_name > proxy-cscf

Entering the above command sequence results in the following prompt:

{context_name}@hostname(config-cscf-service-proxy-cscf)#

Syntax Description

[ no ] pcrf-policy-control

no

Disables external policy control via PCRF for this service. P-CSCF/A-BG will not establish any Diameter session with PCRF, even though the PCRF is configured. This option disables both authorization and subscription to PCRF during Registration and VOIP call.

Usage Guidelines

Use this command to enable PCRF policy control and enter the PCRF-Policy-Control Configuration Mode. It enables authorization and subscription to PCRF during Registration and VOIP calls. If the P-CSCF cannot connect to the PCRF server (due to wrong configuration in CSCF or PCRF unavailability), then P-CSCF/A-BG does not authorize media and VOIP calls will be rejected due to auth failure. Registrations will be handled normally.

Entering this command results in the following prompt:

{context_name}@hostname(config-pcrf-policy-control)#

PCRF-Policy-Control Configuration Mode commands are defined in the CSCF PCRF-Policy-Control Configuration Mode Commands chapter in this guide.
peer-sbc

Configures peer Session Border Controller (SBC) addresses from where the P-CSCF/A-BG service can receive requests.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

`configure > context context_name > cscf service service_name > proxy-cscf`

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-cscf-service-proxy-cscf)#
```

**Syntax Description**
```
[ no ] peer-sbc ip_address
```

- **no**
Remove the IP address of a peer SBC from this P-CSCF/A-BG service.

- **ip_address**
Specify the IP address of a peer SBC for this P-CSCF/A-BG service.
`ip_address` is expressed in standard dotted decimal notation for IPv4 or colon notation for IPv6.

**Usage Guidelines**
Use this command to specify peer Session Border Controller (SBC) addresses from where the P-CSCF/A-BG service can receive requests.

**Important**
This command must be entered multiple times if more than one SBC is present.

**Examples**
The following commands identify three peer SBCs for a single P-CSCF/A-BG service:

```
peer-sbc 200.6.2.3
peer-sbc 200.6.2.10
peer-sbc 200.6.2.11
```
The following command removes the peer SBC with IP address 200.6.2.10 from the P-CSCF/A-BG service:
no peer-sbc 200.6.2.10
plmn-id

Configures location specific mobile network identifiers used to help translate local emergency and service-related numbers. Default is disabled.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

configure > context context_name > cscf service service_name > proxy-cscf

Entering the above command sequence results in the following prompt:

(host_name) (config-cscf-service-proxy-cscf) #

Syntax Description

plmn-id mcc code mnc code

no plmn-id

no

Removes the access network configuration for this P-CSCF/A-BG service.

mcc code

Specifies the Mobile Country Code for the mobile access network. code must be a three-digit integer from 200 to 999.

mnc code

Specifies the Mobile Network Code for the mobile access network. code must be a two or three-digit integer from 00 to 999.

Usage Guidelines

Use this command to help match location specific emergency/service numbers when configuring translations. The mcc and mnc values are compared against those received in p-access-network-info headers as per 3GPP TS 24.229. If mnc is not provided in the criteria only mcc is compared.

Examples

The following command identifies the mobile network with a MCC of 123 and a MNC of 12:

plmn-id mcc 123 mnc 12
**reg-preloaded-route**

Enables the function to use the preloaded-route-headers received in REGISTER for routing at P-CSCF.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

`configure > context context_name > csf service service_name > proxy-cscf`

Entering the above command sequence results in the following prompt:

`{context_name}@host_name(config-cscf-service-proxy-cscf) #`

**Syntax Description**
| default | no | reg-preloaded-route

- **default | no**
  Enables the ability to use preloaded-route-headers for routing REGISTER.

**Usage Guidelines**
Use this command to enable or disable usage of preloaded-route-headers for routing REGISTER.
reg-service-route

Enables the function to use service routes when routing re-registrations.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

```plaintext
configure > context context_name > cscf service service_name > proxy-cscf
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-cscf-service-proxy-cscf)#
```

**Syntax Description**

```
| no | reg-service-route
```

**no**

Disables the ability to use service routes for re-registration.

**Usage Guidelines**
Use this command to enable the P-CSCF/A-BG service to use service routes when routing re-registrations.
reliable-prov-resp

Enables/disables the reliability of provisional responses feature.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

**Syntax Description**

```
reliable-prov-resp { mandatory | optional }
[ no ] reliable-prov-resp
```

- **no**
  Disables the reliability of provisional responses feature.

- **mandatory | optional**
  - **mandatory**: Both inbound and outbound will request reliability.
  - **optional** *(default)*: Reliability is imposed by inbound side. Only if inbound call requests reliability will outbound also request reliability.

**Usage Guidelines**
Use this command to enable/disable the reliability of provisional responses feature.

**Examples**
The following command sets the reliability of provisional responses feature to mandatory:
```
reliable-prov-resp mandatory
```

The following command disables the reliability of provisional responses feature:
```
no reliable-prov-resp
```
**restoration-procedure**

Enables the P-CSCF/A-BG service to reject with a 504 response when it receives 3xx, 480, or "no response" to service request. This feature is disabled by default.

**Product**

SCM (P-CSCF, A-BG)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

```plaintext
configure > context context_name > csf service service_name > proxy-cscf
```

Entering the above command sequence results in the following prompt:

```plaintext
<context_name>@host_name(config-cscf-service-proxy-cscf) #
```

**Syntax Description**

[ no ] restoration-procedure

no

Disables restoration procedure on the P-CSCF/A-BG service.

**Usage Guidelines**

Restoration procedure is intended to handle unreachability of service-route header content. Enabling this command allows the P-CSCF/A-BG service to reject with a 504 response when it receives 3xx, 480, or "no response" to service request.

**Examples**

Enables restoration procedure on the P-CSCF/A-BG service:

```plaintext
restoration-procedure
```

Disables restoration procedure on the P-CSCF/A-BG service:

```plaintext
no restoration-procedure
```
**security-parameters**

Enters the Security Configuration Mode in which Denial of Service (DOS) prevention commands can be configured.

**Product**

SCM (P-CSCF, A-BG)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

`configure > context context_name > cscf service service_name > proxy-cscf`

Entering the above command sequence results in the following prompt:

`{context_name}@hostname(config-cscf-service-proxy-cscf)#`

**Syntax Description**

`security-parameters`

**Usage Guidelines**

Use this command to enter the Security Configuration Mode.

Entering this command results in the following prompt:

`{context_name}@hostname(config-security-parameters)#`

Security Configuration Mode commands are defined in the *CSCF Security Configuration Mode Commands* chapter in this guide.
**sigcomp**

Enables signaling compression for the P-CSCF/A-BG service and enters the Signaling Compression Configuration Mode.

**Product**

SCM (P-CSCF, A-BG)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

```plaintext
configure > context context_name > cscf service service_name > proxy-cscf
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-cscf-service-proxy-cscf)#
```

**Syntax Description**

```
[ no ] sigcomp
```

**no**

Disables signaling compression for the P-CSCF/A-BG service.

**Usage Guidelines**

Use this command to enable signaling compression for the P-CSCF/A-BG service and enter the CSCF Signaling Compression Configuration Mode.

Entering this command results in the following prompt:

```
(context_name)hostname(config-sigcomp)#
```

Signaling Compression Configuration Mode commands are defined in the *CSCF Signaling Compression Configuration Mode Commands* chapter in this guide.
**sip-header**

Enable SIP header insertion for the P-CSCF/A-BG service. SIP header insertion is disabled by default.

**Product**

SCM (P-CSCF, A-BG)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

```plaintext
configure > context context_name > csf service service_name > proxy-cscf
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-cscf-service-proxy-csf)#
```

**Syntax Description**

| **no** | sip-header insert { p-access-network-info | p-cust1-prid-info | p-user-database } |

**no**

Disables SIP header insertion for the P-CSCF/A-BG service.

```
sip-header insert { p-access-network-info | p-cust1-prid-info | p-user-database }
```

**p-access-network-info**: Inserts P-Access-Network-Info (PANI) header in received request/response.

**p-cust1-prid-info**: Inserts a custom header, P-LGUPlus-PRID-Info, which contains the private user id of the user sending any dialogue creating request or any standalone requests, to be added in the message toward nexthop. Addition of the header will be done when P-CSCF forwards this message.

**p-user-database**: Inserts P-User-Database (PUD) header in SIP (REGISTER) message and Invite from I-CSCF to S-CSCF.

**Usage Guidelines**

Enabling this command allows SIP header insertion on the P-CSCF or A-BG.

**Important**

Use the `access-type` command to configure a ue-ip-address-range per access type. CSCF Service Configuration Mode commands are defined in the `CSCF Service Configuration Mode Commands` chapter in this guide.
Examples

Enables SIP PANI header insertion for the P-CSCF/A-BG service:

```
sip-header insert p-access-network-info
```
sip-param

Enable the addition of "integrity-protected" parameter in the authorization header of a SIP (REGISTER) message for the P-CSCF/A-BG service.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

configure > context context_name > cscf service service_name > proxy-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-proxy-cscf)#

Syntax Description

[ no ] sip-param insert integrity-protected | custom-logic | transparent |

no

Disables the addition of "integrity-protected" parameter in the authorization header of a SIP (REGISTER) message for the P-CSCF/A-BG service.

insert integrity-protected

Inserts "integrity-protected" parameter in the authorization header of a SIP (REGISTER) message for the P-CSCF/A-BG service.

custom-logic

Insert "integrity-protected" parameter for custom-logic in Authorization header.

transparent

Pass the "integrity-protected" parameter received from the previous node unmodified.

Usage Guidelines

Enabling this command allows the P-CSCF or A-BG to add the "integrity-protected" parameter in the authorization header of a SIP (REGISTER) message. The parameter will be used by the S-CSCF to decide which authentication mode to use to authenticate the user.
Examples

Enables the addition of integrity-protected parameter:
sip-param insert integrity-protected

Disables the addition of integrity-protected parameter:
no sip-param insert integrity-protected
store-session-path

Enables the P-CSCF or A-BG to store and process the session path information, which includes the Route list, Record-Route list, Service-Route list, and ViaList.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

configure > context context_name > cscf service service_name > proxy-cscf

Entering the above command sequence results in the following prompt:

(context_name)host_name(config-cscf-service-proxy-cscf)#

Syntax Description
[ no ] store-session-path

no

Disables the storing of session path information by the P-CSCF or A-BG. In addition, the P-CSCF/A-BG will not overwrite the Route list, Record-Route list, Service-Route list, or ViaList in the in-dialog request and responses.

Usage Guidelines
Enabling this command allows the P-CSCF or A-BG to store and process the session path information.

Examples
Enables the storage and processing of session path information:
store-session-path

Disables the storage and processing of session path information:
no store-session-path
CSCF Routes Configuration Mode Commands

The CSCF Routes Configuration Mode is used to configure session forwarding within the system.

Command Modes

Exec > Global Configuration > Context Configuration > Routes Configuration

configure > context context_name > cscf routes { default | name list_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-route)#

Important

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

- after, page 1498
- before, page 1499
- end, page 1500
- exit, page 1501
- route, page 1502
after

Places the CSCF route entry at the bottom or end of the route list. Use this command in conjunction with the route command.

Product

SCM (P-CSCF, S-CSCF, SIP Proxy)

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Routes Configuration

configure > context context_name > scf routes { default | name list_name }

Entering the above command sequence results in the following prompt:

(context_name)host_name(config-cscf-route)#

Syntax Description

after

Usage Guidelines

Add this command before the route command to place the entry at the end of the route list.
before

Places the CSCF route entry at the top or beginning of the route list. Use this command in conjunction with the `route` command.

**Product**
SCM (P-CSCF, S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > Routes Configuration

```
configure > context context_name > cscfroutes { default | name list_name }
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-cscf-route)#
```

**Syntax Description**
before

**Usage Guidelines**
Add this command before the `route` command to place the entry at the beginning of the route list.
end

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

end

**Usage Guidelines**

Use this command to return to the Exec mode.
exit

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

Product
All

Privilege
Security Administrator, Administrator

Syntax Description
exit

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

Configure the routing parameters for the context.

Product

SCM (P-CSCF, S-CSCF, SIP Proxy)

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Routes Configuration

configure > context context_name > csf routes { default | name list_name }

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-cscf-route)#

Syntax Description

route { domain name | local { icscf | pcsf | scscf } | nexthop-address address | peer-servers server_name | peer-servers-group group_name | route-list group_name | vpn name } | [ mod-req-uri | base-criteria criteria | filter-criteria1 criteria | filter-criteria2 criteria | log ]

no route { domain name | local { icscf | pcsf | scscf } | nexthop-address address | peer-servers server_name | peer-servers-group group_name | route-list group_name | vpn name } base-criteria criteria | filter-criteria1 criteria | filter-criteria2 criteria |

no

Removes the specified routing parameters for the CSCF service.

domain name

Specifies a valid next-hop domain name. name must be from 1 to 79 alpha and/or numeric characters in length.

local { icscf | pcsf | scscf }

Specifies a local interrogating, serving, or proxy call/session control function to which all calls processed by the context will be routed.

nexthop-address ip_address

Specifies a next-hop address.

ip_address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

peer-servers server_name

Specifies a configured peer server.
server_name must be the name of a configured peer server on this system.

peer-servers-group group_name
Specifies a configured peer servers group.
group_name must be the name of a configured peer servers group on this system.

route-list group_name
Specifies a configured route list group.
group_name must be the name of a configured route list group on this system.

vpn name
Specifies a configured VPN context on the system.
nname must be a configured context name.

mod-req-uri
Specifies that a route lookup should be performed and the request URI modified.

base-criteria criteria
Specifies the base criteria that packets will be compared against. The following criteria is supported:

- access-type type: Filters sessions based on a specific access-type used by the subscriber. Possible access types are:
  - 3gpp-geran: 3GPP Access Type
  - 3gpp-utran-fdd: 3GPP Access Type
  - 3gpp-utran-tdd: 3GPP Access type
  - 3gpp2-1x: 3GPP2 Access Type
  - 3gpp2-1x-hrpd: 3GPP2 Access Type
  - 3gpp2-cdma-cs: 3GPP2-CDMA-CS
  - 3gpp2-umb: 3GPP2-UMB
  - adsl: FixedLine Access Type
  - adsl2: FixedLine Access Type
  - adsl2p: FixedLine Access Type ADSL2+
  - docsis: DOCSIS
  - gshdsl: Fixed Line Access Type G.SHDSL
  - hdsl: Fixed Line Access Type
  - hdsl2: Fixed Line Access Type
  - idsl: Fixed Line Access Type
  - ieee-80211: WLAN Access Type
• ieee-80211a: WLAN Access Type
• ieee-80211b: WLAN Access Type
• ieee-80211g: WLAN Access Type
• ieee-80216e: Wireless MAN Access Type
• radsl: Fixed Line Access Type
• sdsl: Fixed Line Access Type
• vdsl: Fixed Line Access Type

• any: Filters all CSCF sessions.

• carrier-id name: Filters sessions based on the carrier's ID. name must be from 1 to 79 alpha and/or numeric characters in length.

• destination aor aor: Filters sessions based on the destination AoR. aor must be an existing AoR from 1 to 79 characters in length.

> Important The destination aor and carried-id criteria cannot occur in the same route rule.

• nexthop-uri name: Filters sessions based on Address of Record. name must be from 1 to 79 alpha and/or numeric characters in length.

• plmn-id mcc mcc_code mnc mnc_code: Filters sessions based on the mobile country and network codes. mcc_code must be a three-digit integer from 200 to 999. mnc_code must be a two or three-digit integer from 00 to 999.

• source address ip_address: Filters sessions based on source IP address. ip_address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

• source aor aor: Filters sessions based on the source AoR. aor must be an existing AoR from 1 to 79 characters in length.

• subscriber-capability capability_type: Filters sessions based on capability of the subscriber. Possible capability types are:

• at - Custom AT Type
• audio - Audio Capability Type
• chat - Custom CHAT Type
• cs - Custom CS Type
• ft - Custom FT Type
• im - Custom IM Type
• lte-voip - Custom LTE-VOIP Type
• lte-vt - Custom LTE-VT Type
• mms - Custom MMS Type
• msg - Custom MSG Type
- **oma-sip-im** - Custom OMA SIP-IM Type
- **rcs-dp** - Custom RCS-DP Type
- **rcs-e** - Custom RCS-E Type
- **rcs-ft** - Custom RCS-FT Type
- **rcs-im** - Custom RCS-IM Type
- **rcs-is** - Custom RCS-IS Type
- **rcs-sp** - Custom RCS-SP Type
- **rcs-vs** - Custom RCS-VS Type
- **smart-edu** - Custom SMART-EDU Type
- **text** - Text Capability Type
- **video** - Video Capability Type
- **vt** - Custom VT Type
- **vt-ft** - Custom VT-FT Type
- **vt-is** - Custom VT-IS Type
- **vt-loc** - Custom VT-LOC Type
- **vt-memo** - Custom VT-MEMO Type

- **subscriber-ip-type** { **v4** | **v6** } : Filters sessions based on IP type of the subscriber. Possible IP types are:
  - **v4** - IPV4 Type
  - **v6** - IPV6 Type

- **time-of-day** : Filters sessions based on the time of the day. Additional filter criteria for **time-of-day** is as follows:
  - **day-of-month** *day*: Filters session based on the day of the month. *day* must be an integer from 1 to 31.
  - **day-of-week** *day*: Filters session based on the day of the week. *day* must be an integer from 1 to 7 with 1 signifying Sunday and 7 signifying Saturday.
  - **start** date/time [ **end** date/time ]: Filters sessions based on a start time to, optionally, an end time during the day. *date/time* must be integers in either of the following formats: YYYY:MM:DD:HH:mm or YYYY:MM:DD:mm:ss. YYYY: year range 2005 to 2099 MM: months (integer range 1 to 12) DD: days (integer range 1 to 31) HH: hours (integer range 0 to 23) mm: minutes (integer range 0 to 59) ss: seconds (integer range 0 to 59)
  - **week-of-month** *week*: Filters sessions based on the week of the month. *week* must be an integer from 1 to 5.
AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

**filter-criteria**

Specifies the filter criteria that packets that have passed the base criteria will be compared against. The following criteria is supported:

- **access-type** *type*: Filters sessions based on a specific access-type used by the subscriber. Possible access types are:
  - 3gpp-geran: 3GPP Access Type
  - 3gpp-utran-fdd: 3GPP Access Type
  - 3gpp-utran-tdd: 3GPP Access Type
  - 3gpp2-1x: 3GPP2 Access Type
  - 3gpp2-1x-hrpd: 3GPP2 Access Type
  - 3gpp2-cdma-cs: 3GPP2-CDMA-CS
  - 3gpp2-umb: 3GPP2-UMB
  - adsl: FixedLine Access Type
  - adsl2: FixedLine Access Type
  - adsl2p: FixedLine Access Type ADSL2+
  - docsis: DOCSIS
  - gshdsl: Fixed Line Access Type G.SHDSL
  - hdsl: Fixed Line Access Type
  - hdsl2: Fixed Line Access Type
  - idsl: Fixed Line Access Type
  - iee-80211: WLAN Access Type
  - iee-80211a: WLAN Access Type
  - iee-80211b: WLAN Access Type
  - iee-80211g: WLAN Access Type
  - iee-80216e: Wireless MAN Access Type
  - rads: Fixed Line Access Type
  - sdsl: Fixed Line Access Type
  - vdsl: Fixed Line Access Type
  - any: Filters all CSCF sessions.
- **carrier-id name**: Filters sessions based on the carrier's ID. *name* must be from 1 to 79 alpha and/or numeric characters in length.

- **destination aor aor**: Filters sessions based on the destination AoR. *aor* must be an existing AoR from 1 to 79 characters in length.

  **Important** The destination aor and carried-id criteria cannot occur in the same route rule.

- **nexthop-uri name**: Filters sessions based on Address of Record. *name* must be from 1 to 79 alpha and/or numeric characters in length.

- **plmn-id mcc mcc_code mnc mnc_code**: Filters sessions based on the mobile country and network codes. *mcc_code* must be a three-digit integer from 200 to 999. *mnc_code* must be a two or three-digit integer from 00 to 999.

- **source address ip_address**: Filters sessions based on source IP address. *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

- **source aor aor**: Filters sessions based on the source AoR. *aor* must be an existing AoR from 1 to 79 characters in length.

- **subscriber-capability capability_type**: Filters sessions based on capability of the subscriber. Possible capability types are:
  - **at** - Custom AT Type
  - **audio** - Audio Capability Type
  - **chat** - Custom CHAT Type
  - **cs** - Custom CS Type
  - **ft** - Custom FT Type
  - **im** - Custom IM Type
  - **lte-voip** - Custom LTE-VOIP Type
  - **lte-vt** - Custom LTE-VT Type
  - **mms** - Custom MMS Type
  - **msg** - Custom MSG Type
  - **oma-sip-im** - Custom OMA SIP-IM Type
  - **rcs-dp** - Custom RCS-DP Type
  - **rcs-e** - Custom RCS-E Type
  - **rcs-ft** - Custom RCS-FT Type
  - **rcs-im** - Custom RCS-IM Type
  - **rcs-is** - Custom RCS-IS Type
  - **rcs-sp** - Custom RCS-SP Type
  - **rcs-vs** - Custom RCS-VS Type
- **smart-edu** - Custom SMART-EDU Type
- **text** - Text Capability Type
- **video** - Video Capability Type
- **vt** - Custom VT Type
- **vt-ft** - Custom VT-FT Type
- **vt-is** - Custom VT-IS Type
- **vt-loc** - Custom VT-LOC Type
- **vt-memo** - Custom VT-MEMO Type

- **subscriber-ip-type { v4 | v6 }**: Filters sessions based on IP type of the subscriber. Possible IP types are:
  - **v4** - IPV4 Type
  - **v6** - IPV6 Type

- **time-of-day**: Filters sessions based on the time of the day. Additional filter criteria for **time-of-day** is as follows:
  - **day-of-month** *day*: Filters session based on the day of the month. *day* must be an integer from 1 to 31.
  - **day-of-week** *day*: Filters session based on the day of the week. *day* must be an integer from 1 to 7 with 1 signifying Sunday and 7 signifying Saturday.
  - **start date/time [ end date/time ]**: Filters sessions based on a start time to, optionally, an end time during the day. *date/time* must be integers in either of the following formats: YYYY:MM:DD:HH:mm or YYYY:MM:DD:mm:ss. YYYY: year range 2005 to 2099 MM: months (integer range 1 to 12) DD: days (integer range 1 to 31) HH: hours (integer range 0 to 23) mm: minutes (integer range 0 to 59) ss: seconds (integer range 0 to 59)
  - **week-of-month** *week*: Filters sessions based on the week of the month. *week* must be an integer from 1 to 5.

**Important**
AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

**filter-criteria2 criteria**
Specifies the filter criteria that packets that have passed the base criteria and filter-criteria1 will be compared against. The following criteria is supported:

- **access-type** *type*: Filters sessions based on a specific access-type used by the subscriber. Possible access types are:
  - **3gpp-geran**: 3GPP Access Type
  - **3gpp-utran-fdd**: 3GPP Access Type
- **3gpp-utran-tdd**: 3GPP Access type
- **3gpp2-1x**: 3GPP2 Access Type
- **3gpp2-1x-hrp**: 3GPP2 Access Type
- **3gpp2-cdma-cs**: 3GPP2-CDMA-CS
- **3gpp2-umb**: 3GPP2-UMB
- **adsl**: Fixed Line Access Type
- **adsl2**: Fixed Line Access Type
- **adsl2p**: Fixed Line Access Type ADSL2+
- **docsis**: DOCSIS
- **gshdsl**: Fixed Line Access Type G.SHDSL
- **hdsi**: Fixed Line Access Type
- **hdsi2**: Fixed Line Access Type
- **idsi**: Fixed Line Access Type
- **ieee-80211**: WLAN Access Type
- **ieee-80211a**: WLAN Access Type
- **ieee-80211b**: WLAN Access Type
- **ieee-80211g**: WLAN Access Type
- **ieee-80216e**: Wireless MAN Access Type
- **radsi**: Fixed Line Access Type
- **sdsl**: Fixed Line Access Type
- **vdsl**: Fixed Line Access Type

- **any**: Filters all CSCF sessions.
- **carrier-id name**: Filters sessions based on the carrier's ID. name must be from 1 to 79 alpha and/or numeric characters in length.
- **destination aor aor**: Filters sessions based on the destination AoR. aor must be an existing AoR from 1 to 79 characters in length.

  __Important__  
  The destination aor and carried-id criteria cannot occur in the same route rule.

- **nexthop-uri name**: Filters sessions based on Address of Record. name must be from 1 to 79 alpha and/or numeric characters in length.
- **plmn-id mcc mcc_code mcc mcc_code**: Filters sessions based on the mobile country and network codes. mcc code must be a three-digit integer from 200 to 999. mcc_code must be a two or three-digit integer from 00 to 999.
• **source address** `ip_address`: Filters sessions based on source IP address. `ip_address` must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

• **source aor aor**: Filters sessions based on the source AoR. `aor` must be an existing AoR from 1 to 79 characters in length.

• **subscriber-capability** `capability_type`: Filters sessions based on capability of the subscriber. Possible capability types are:
  - `at` - Custom AT Type
  - `audio` - Audio Capability Type
  - `chat` - Custom CHAT Type
  - `cs` - Custom CS Type
  - `ft` - Custom FT Type
  - `im` - Custom IM Type
  - `lte-voip` - Custom LTE-VOIP Type
  - `lte-vt` - Custom LTE-VT Type
  - `mms` - Custom MMS Type
  - `msg` - Custom MSG Type
  - `oma-sip-im` - Custom OMA SIP-IM Type
  - `rcs-dp` - Custom RCS-DP Type
  - `rcs-e` - Custom RCS-E Type
  - `rcs-ft` - Custom RCS-FT Type
  - `rcs-im` - Custom RCS-IM Type
  - `rcs-is` - Custom RCS-IS Type
  - `rcs-sp` - Custom RCS-SP Type
  - `smart-edu` - Custom SMART-EDU Type
  - `rcs-vs` - Custom RCS-VS Type
  - `text` - Text Capability Type
  - `video` - Video Capability Type
  - `vt` - Custom VT Type
  - `vt-ft` - Custom VT-FT Type
  - `vt-is` - Custom VT-IS Type
  - `vt-loc` - Custom VT-LOC Type
  - `vt-memo` - Custom VT-MEMO Type

• **subscriber-ip-type** `{ v4 | v6 }`: Filters sessions based on IP type of the subscriber. Possible IP types are:
  - `v4` - IPV4 Type
- **v6** - IPV6 Type

- **time-of-day**: Filters sessions based on the time of the day. Additional filter criteria for **time-of-day** is as follows:
  - **day-of-month** `day`: Filters session based on the day of the month. `day` must be an integer from 1 to 31.
  - **day-of-week** `day`: Filters session based on the day of the week. `day` must be an integer from 1 to 7 with 1 signifying Sunday and 7 signifying Saturday.
  - **start date/time [ end date/time ]**: Filters sessions based on a start time to, optionally, an end time during the day. `date/time` must be integers in either of the following formats: YYYY:MM:DD:HH:mm or YYYY:MM:DD:mm:ss. YYYY: year range 2005 to 2099 MM: months (integer range 1 to 12) DD: days (integer range 1 to 31) HH: hours (integer range 0 to 23) mm: minutes (integer range 0 to 59) ss: seconds (integer range 0 to 59)
  - **week-of-month** `week`: Filters sessions based on the week of the month. `week` must be an integer from 1 to 5.

---

**Important**

AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

---

**log**

Enables logging for CSCF sessions meeting the criteria specified in the ACL. The logs can be viewed by executing the **logging filter active facility cscf-acl-log** command in the Exec mode.

---

**Usage Guidelines**

Use this command to configure routing parameters for the service.

---

**Important**

Use the **before** or **after** command to place the route entry in the route list.

---

**Examples**

The following command is placed at the end of the route list and routes sessions to a peer server group named `icscf_peer5`, filters sessions with a base criteria of the source address (1.2.3.4) and a filter criteria of the destination AoR ($@test.com):

```
after route peer-servers icscf_peer5 base-criteria source address 1.2.3.4 filter-criteria1 destination aor $@test.com
```
CSCF Service Configuration Mode Commands

The CSCF Service Configuration Mode is used to create and manage CSCF services within the current context.

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```plaintext
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name@host_name(config-cscf-service)]#
```

**Important**

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

- RetryAfter-header-value, page 1516
- access-service, page 1517
- access-type, page 1519
- allow-dereg, page 1522
- bind, page 1523
- caller-preference, page 1526
- charging, page 1527
- cnsa-media-profile, page 1528
- core-service, page 1530
- custom cdf-selection, page 1531
- custom reason-header-cause, page 1532
- custom reg-binding, page 1534
- custom response, page 1535
• custom volte, page 1538
• default-aor-domain, page 1539
• emergency-cscf, page 1540
• end, page 1541
• exit, page 1542
• history-info, page 1543
• interface statistics sip, page 1544
• interrogating-cscf, page 1545
• ipv4-ipv6-interworking, page 1546
• keepalive, page 1547
• lawful-intercept, page 1549
• li-packet-cable, page 1550
• max-reqmsg-size, page 1551
• max-sipmsg-size, page 1552
• media-bridging, page 1553
• monitoring, page 1554
• multiple-reg same-private-id, page 1555
• nat-policy, page 1556
• nat-pool, page 1558
• policy, page 1560
• policy-name, page 1563
• proxy-cscf, page 1564
• proxy-serving-cscf, page 1565
• recurse-on-redirect-resp, page 1566
• reject-on-cnlsa-failure, page 1567
• release-call-on-media-loss, page 1568
• rfc3261-proxy, page 1569
• server-header, page 1570
• server-name, page 1572
• serving-cscf, page 1573
• serving-cscf-list, page 1574
• session-timer, page 1576
• strict-check configured-aor-domain, page 1578
- strict-outbound, page 1579
- subscriber-policy-override, page 1580
- subscription, page 1581
- support-content-type any, page 1583
- tcp-proxy, page 1584
- threshold, page 1585
- timeout, page 1587
- transport-switching, page 1590
- trusted-domain-entity, page 1591
RetryAfter-header-value

Sets the minimum and maximum value in seconds for Retry-After Header.

Product
SCM (S-CSCF)

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Service Configuration
configure > context context_name > csf service service_name

Entering the above command sequence results in the following prompt:
<context_name>host_name(config-cscf-service)#

Syntax Description
RetryAfter-header-value min-value sec max-value sec
default RetryAfter-header-value

default
Returns the command to the default settings.

min-value sec max-value sec

min-value sec: Specifies the minimum amount of time for Retry-After Header. sec must be an integer from 2 to 3600. Default is 2 seconds.

max-value sec: Specifies the maximum amount of time for Retry-After Header. sec must be an integer from 3 to 3601. Default is 10 seconds.

Important
Maximum value should be greater than minimum value.

Usage Guidelines
Use this command to set the minimum and maximum value in seconds for Retry-After Header. If Transactions Per Second (TPS) rate towards the peer-server application server (AS) is exceeded, the incoming requests will be rejected with 500 error response; Retry-After Header specifies the number of seconds before UE should retry.

Examples
The following command configures the minimum value to 3 and maximum value to 12 for Retry-After Header:
RetryAfter-header-value min-value 3 max-value 12
access-service

Configures the name of the P-CSCF/A-BG access service from which the system receives requests and sends responses. The access service lets the core service know where a packet needs to be routed.

**Product**  
SCM (P-CSCF, A-BG)

**Privilege**  
Administrator

**Command Modes**  
Exec > Global Configuration > Context Configuration > CSCF Service Configuration  
`configure > context context_name > csf service service_name`

Entering the above command sequence results in the following prompt:  
`(context_name)host_name(config-cscf-service)#`

**Syntax Description**  
`access-service name name`
`no access-service [ name name ]`

- **no**  
Remove the access service.

- **name name**  
Specifies the name of the P-CSCF/A-BG access service from which the system receives requests and sends responses.  
`name` must be from 1 to 63 alpha and/or numeric characters.

**Important**  
This command should only be issued in the core service configuration, however, multiple access services may be configured per core service.

**Usage Guidelines**  
Use this command to identify the name of the P-CSCF/A-BG access service from which the system receives requests and sends responses from/to the UEs. This command is used in systems that deploy two P-CSCF/A-BG services in bridging (Back-to-Back User Agent) mode configurations where an access service P-CSCF/A-BG faces the UE network and a core P-CSCF/A-BG faces the public network.
The following command identifies the P-CSCF/A-BG access service named to the CSCF/A-BG core service:

```
access-service name HA3
```
**access-type**

Specifies the access types for IMS core.

**Product**

SCM (P-CSCF, A-BG)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax Description**

```
access-type { type } access-profile { default | name access_profile_name } | ue-ip-address-range name
ue_ip_name { address ip_address_mask | range start_ip_address end_ip_address }
no access-type { type } | access-profile | ue-ip-address-range { name ue_ip_name } |
```

```
no
```

Removes the specified access type from a CSCF access profile or UE IP address/range.

```
access-type { type }
3gpp-e-utran-fdd: 3GPP Access Type
3gpp-e-utran-tdd: 3GPP Access Type
3gpp-geran: 3GPP Access Type
3gpp-utran-fdd: 3GPP Access Type
3gpp-utran-tdd: 3GPP Access type
3gpp2-1x: 3GPP2 Access Type
3gpp2-1x-hrp: 3GPP2 Access Type
3gpp2-cdma-cs: 3GPP2-CDMA-CS
3gpp2-umb: 3GPP2-UMB
adsl: FixedLine Access Type
adsl2: FixedLine Access Type
adsl2p: FixedLine Access Type ADSL2+
docsis: DOCSIS

gshdsl: FixedLine Access Type G.SHDSL

hdsl: FixedLine Access Type

hdsl2: FixedLine Access Type

idsl: FixedLine Access Type

ieee-80211: WLAN Access Type

ieee-80211a: WLAN Access Type

ieee-80211b: WLAN Access Type

ieee-80211g: WLAN Access Type

ieee-80211n: WLAN Access Type

ieee-80216e: Wireless MAN Access Type

ieee-8023: Ethernet Access Type

ieee-8023a: Ethernet Access Type

ieee-8023ab: Ethernet Access Type

ieee-8023ae: Ethernet Access Type

ieee-8023ak: Ethernet Access Type

ieee-8023an: Ethernet Access Type

ieee-8023aq: Ethernet Access Type

ieee-8023e: Ethernet Access Type

ieee-8023i: Ethernet Access Type

ieee-8023j: Ethernet Access Type

ieee-8023u: Ethernet Access Type

ieee-8023y: Ethernet Access Type

ieee-8023z: Ethernet Access Type

radsl: FixedLine Access Type

sdsl: FixedLine Access Type

vdsl: FixedLine Access Type

access-profile { default | name access_profile_name }
Associates an access type with a CSCF access profile. Different access types can refer to the same access profile.

ue-ip-address-range name ue_ip_name { address ip_address_mask | range start_ip_address end_ip_address }
Configures UE IP address/range for a specific access type.

ue_ip_name must be from 1 to 79 alpha and/or numeric characters.

address ip_address_mask: Specifies a combined IP address subnet mask bits to indicate what IP addresses the specific access-type applies to. ip_address_mask must be specified using the form "IP Address/Mask Bits"
where the IP address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6, and the mask bits are a numeric value, which is the number of bits in the subnet mask.

**range start_ip_address end_ip_address:** Configure UE IP range for specific access-type.

- `start_ip_address` specifies the beginning of the range of addresses.
- `end_ip_address` specifies the end of the range of addresses.
- `ip_address` must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

**Usage Guidelines**

Use this command to associated the access types for a specified CSCF access profile or UE IP address/range name.

**Important**

Use the `sip-header` command to enable SIP P-Access-Network-Info (PANI) header insertion. CSCF Proxy-CSCF Configuration Mode commands are defined in the *CSCF Proxy-CSCF Configuration Mode Commands* chapter in this guide.

**Examples**

The following command identifies the access type adsl and assigns it to access profile *ap1*:

```
access-type adsl access-profile name ap1
```
**allow-dereg**

Allows the CSCF to send de-registration requests. Feature is disabled by default.

**Product**
SCM

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration
configure > context context_name > csf service service_name

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-cscf-service)#
```

**Syntax Description**

```
| no | allow-dereg
```

**no**
Disables the feature.

**Usage Guidelines**

Use this command to allow the CSCF service to send de-registration requests.

If the UE stops sending keepalive packets, which ends the connection between the UE and the proxy, UE information is cleared from the Proxy-CSCF (P-CSCF) or Access Border Gateway (A-BG). If de-registration requests are enabled, any UE-related information that is shared with the Serving-CSCF (S-CSCF) will also be cleared.
**bind**

Binds the CSCF service to a logical IP interface and specifies the maximum number of sessions that can access this service over the specified interface.

**Product**

SCM (P-CSCF, A-BG)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

\[(context_name)host_name(config-cscf-service)\]

**Syntax Description**

bind address ip_address | cscf-hostname host_name | [ ipsec-crypto-template template ] | [ max-sessions max# ] | [ port number ] | [ reserved-call-capacity percentage ] | [ tls-crypto-template template ] | [ tls-port number ] | [ transport tcp ] | [ use-serviceport-towards-network ]

no bind address

no

Removes the binding of the service to a specified interface.

**address ip_address**

Specifies the IP address of the interface to which the service is being bound.

*ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

**cscf-hostname host_name**

Specifies the local host name of the CSCF service.

*host_name* must be an existing CSCF service name and be from 1 to 127 alpha and/or numeric characters.

Configuring this keyword associates the CSCF service with the AOR domain configured in the **default-aor-domain** command and uses the domain name in SIP headers.

**Important**

If this keyword is not configured, SIP headers will contain the IP address of the CSCF service instead of the domain name.
ipsec-crypto-template template

Specifies the name of an existing IPSec CSCF crypto template to be used for accessing CSCF service by user equipment. Valid only for P-CSCF or A-BG.

*template* must be an existing IPSec CSCF crypto template and be from 1 to 127 alpha and/or numeric characters.

---

**Important**
The IPSec CSCF crypto template should be configured in the same context in which the P-CSCF is configured.

---

max-sessions max#

Default: 500,000

Specifies the maximum number of sessions managed by this service on this interface.

*max#* must be configured to any integer value from 0 to 500,000.

---

**Important**
The total session capacity of the system is 500,000. **max-sessions** is also limited by the capacity in the license generated for the service. If licenses for PDSN/GGSN/HA are generated for `x` number of sessions, then the license for the CSCF service will be generated at 500,000-`x`. Hardware configuration and installed features can also affect the maximum number of sessions that can be supported.

---

port number

Default: 5060

Specifies the UDP port number.

*number* must be an integer value from 1 to 65534.

---

reserved-call-capacity percentage

Default: 10

Specifies the call capacity percentage per session manager (sessmgr).

*percentage* must be an integer value from 1 to 50.

---

tls-crypto-template template [ tls-port number ]

Specifies the name of an existing Transport Layer Security (TLS) crypto template to enable TLS functionality. Valid only for P-CSCF or A-BG.

*template* must be an existing TLS crypto template and be from 1 to 127 alpha and/or numeric characters.

Default: 5061

Specifies the TLS port number.

*number* must be an integer value from 1 to 65534.
When the `tls-crypto-template` is configured, TCP transport must be enabled, otherwise this command will throw an error. The configured `tls-crypto-template` should be configured in the same context in which the P-CSCF service is configured and must be complete with all certificate and cipher suite configuration. If the `tls-crypto-template` is not present or not completely configured, the P-CSCF service will not be started.

**Important**

<table>
<thead>
<tr>
<th>transport tcp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables TCP transport for the address.</td>
</tr>
</tbody>
</table>

**use-serviceport-towards-network**

| Enables use of service port for sending and receiving UDP messages from network elements. |

**Usage Guidelines**

Use this command to associated the service with a specific logical IP address. This command also configures the identity of the CSCF in SIP headers as either the domain name of the CSCF service or the IP address.

**Important**

| Multiple keywords can be used per bind command. |

**Examples**

The following command binds the CSCF service to a logical interface with an IP address of 1.2.3.4 and sets the maximum number of supported sessions for this interface at 250000:

```
bind address 1.2.3.4 max-sessions 250000
```
**caller-preference**

Enables custom SIP caller preferences; standards-based caller preference will not be applied.

**Product**
SCM

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-cscf-service)#
```

**Syntax Description**

```
caller-preference custom
| default | no | caller-preference
```

default

Enables standards-based caller preference.

no

Disables custom caller preference processing; contact will be selected without considering caller preference.

**Usage Guidelines**

Use this command to enable or disable custom SIP caller preferences.
charging

Enables Rf charging in this CSCF service for SIP messages.

**Product**  
SCM

**Privilege**  
Administrator

**Command Modes**  
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```plaintext
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax Description**

```plaintext
[ default | no ] charging
```

- **default | no**
- Enables Rf charging in this CSCF service for SIP messages.
- Disables Rf charging in this CSCF service for SIP messages.

**Usage Guidelines**

Use this command to enable the RF charging feature in this service and enter the CSCF Charging Configuration Mode.

Entering this command results in the following prompt:

```
[context_name]host_name(config-cscf-charging)#
```

CSCF Charging Configuration Mode commands are defined in the *CSCF Charging Configuration Mode Commands* chapter in this guide.
cnsa-media-profile

Configures the media profile id to be set for a previously created service policy.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-cscf-service)#
```

**Syntax Description**

- `no cnsa-media-profile profile_id cscf-service-policy policy_name content-type {application-3gpp-ims-xml | application-pidf-diff-xml | application-pidf-partial-xml | application-pidf-xml | application-reginfo-xml | application-sdp | application-xml | message-sipfrag | multipart-mixed | multipart-related | text-plain}

  - **no**
    - Removes the media profile from the service policy.

  - **cnsa-media-profile profile_id**
    - Specifies the media profile id.
    - `profile_id` must be an integer from 0 to 10 and be an existing media profile id in the system. CNSA media profile ids are created and maintained in the CSCF ISCTemplate Configuration Mode.

  - **cscf-service-policy policy_name**
    - Assigns the media profile id to a service policy.
    - `policy_name` must be from 1 to 63 alpha and/or numeric characters and be an existing policy name in the system. Service policies are created and maintained in the CSCF Policy Configuration Mode.

  - **content-type {application-3gpp-ims-xml | application-pidf-diff-xml | application-pidf-partial-xml | application-pidf-xml | application-reginfo-xml | application-sdp | application-xml | message-sipfrag | multipart-mixed | multipart-related | text-plain}

    - Specifies the content type(s).
**application-3gpp-ims-xml** - format for exchanging information in SIP Requests and Responses as used within the 3GPP IM CN Subsystem

**application-pidf-diff-xml** - contains changed presence elements. Contains full presence document when there are many changes

**application-pidf-partial-xml** - contains only changed parts of PIDF-based presence information

**application-pidf-xml** - XML MIME entity that contains presence information

**application-reginfo-xml** - used in Notifications to SIP user agents about registration expiry

**application-sdp** - SDP session description

**application-xml** - content type for generic xml documents

**message-sipfrag** - contains subsets of well formed SIP messages

**multipart-mixed** - intended for use when the body parts are independent and need to be bundled in a particular order

**multipart-related** - intended for compound objects consisting of several inter-related body parts

**text-plain** - plain text

---

**Important** You may specify multiple types of content.

---

**Usage Guidelines**

Use this command to assign a media profile id to a service policy. The policies defined in the service policy apply to all subscribers using this service.

CNSA media profile ids are created and maintained in the CSCF ISC Template Configuration Mode. Service policies are created and maintained in the CSCF Policy Configuration Mode.

**Examples**

The following command defines the media profile id as 2 and assigns it to `serv_policy3` with plain text content type.

```
cnsa-media-profile 2 cscf-service-policy serv_policy3 content-type text-plain
```
core-service

Configures a core service if:

- CSCF services are run in bridging (Back-to-Back User Agent) mode
- A-BG is an Application-level Gateway (ALG) for Network Address Translation (NAT)

By default, no core-service name will be present.

Product
SCM (CSCF, A-BG)

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Service Configuration
configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-cscf-service)#

Syntax Description

| no | core-service name service_name |

no
Removes the core service.

name service_name
Specifies the name of the core service.

service_name must be from 1 to 80 alpha and/or numeric characters.

Usage Guidelines
Use this command to assign a core service to the CSCF/A-BG service.

Examples
The following command identifies the core service:

core-service name service1
custom cdf-selection

Enables using the CDF selected during registration for "VT" calls. For other calls, the CDF in default AAA-Group is used. Default is disabled.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration
configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

\[context_name\] host_name(config-cscf-service)#

**Syntax Description**

```
[ no ] custom cdf-selection
```

**no**
When disabled, the CDF selected during registration shall be used for all calls.

**Usage Guidelines**
Use this command to apply prefix-based CDF selection logic for VT calls only. For non-VT calls, CDF in default AAA Group is used.
When disabled, prefix-based CDF selection logic is applied for all calls.
custom reason-header-cause

This command configures SIP Reason header cause value.

Product
SCM (S-CSCF)

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Service Configuration
configure > context context_name > csf service service_name

Entering the above command sequence results in the following prompt:
 contexto_name host_name (config-cscf-service)#

Syntax Description

custom reason-header-cause node-type node_type node-number node_num base-cause-code cause_code
no custom reason-header-cause node-type

no
Disables SIP reason header cause configuration.

node-type node_type
Specifies the node type and indicates P-CSCF or S-CSCF.
node_type must be an integer from 1 to 9.

node-number node_num
Specifies the node number assigned to the node.
node_num must be an integer from 1 to 99.

base-cause-code cause_code
Specifies the base number to be added to internal cause code.
cause_code must be an integer from 1 to 65536.
Default: 999

Usage Guidelines
Use this command to configure parameters which will be used for building the SIP Reason header's cause value.
Examples

The following command sets the node type to 1, node number to 5 and base cause code value to 7000:

```
custom reason-header-cause node-type 1 node-number 5 base-cause-code 7000
```
custom reg-binding

Enables the S-CSCF to return only one binding (latest contact) for each registration without including other bindings, if any. Default is disabled.

Product: SCM (S-CSCF)

Privilege: Administrator

Command Modes: Exec > Global Configuration > Context Configuration > CSCF Service Configuration
configure > context context_name > scf service service_name

Entering the above command sequence results in the following prompt:

[context_name]\host_name\(config-cscf-service)>

Syntax Description:

| no | custom reg-binding |

no

S-CSCF returns all the bindings for AOR in 200 OK REGISTER response.

Usage Guidelines:

Use this command to control whether the S-CSCF returns only one or all bindings for AOR in 200 OK REGISTER response.
**custom response**

Configures reject with specific response code for UE capability failure or UE status. Feature is disabled by default.

**Product**

SCM (S-CSCF)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

`configure > context context_name > cscf service service_name`

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-cscf-service)#
```

**Syntax Description**

```
custom response { ue-capability-failure capability_type | ue-status status } reject response-code response_code
no custom response { ue-capability-failure capability_type | ue-status status }
```

**no**

Removes customer-specific UE capability failure or UE status configuration, if present, and uses default RFC/3GPP specification behavior.

**ue-capability-failure capability_type**

Specifies UE capability failure type:

- `all` - UE capability all
- `at` - UE capability AT
- `audio` - UE capability audio
- `chat` - UE capability CHAT
- `cs` - UE capability CS
- `ft` - UE capability FT
- `im` - UE capability IM
- `lte-voip` - UE capability LTE-VOIP
- `lte-vt` - UE capability LTE-VT
- **mms** - UE capability MMS
- **msg** - UE capability MSG
- **oma-sip-im** - UE capability OMA SIP-IM
- **rcs-dp** - UE capability RCS-e DP
- **rcs-e** - UE capability RCS-E
- **rcs-ft** - UE capability RCS-e FT
- **rcs-im** - UE capability RCS-e IM
- **rcs-is** - UE capability RCS-e IS
- **rcs-sp** - UE capability RCS-e SP
- **rcs-vs** - UE capability RCS-e VS
- **smart-edu** - UE capability SMART-EDU
- **text** - UE capability text
- **video** - UE capability video
- **vt** - UE capability VT
- **vt-ft** - UE capability VT-FT
- **vt-is** - UE capability VT-IS
- **vt-loc** - UE capability VT-LOC
- **vt-memo** - UE capability VT-MEMO

**ue-status status**

Specifies UE status:

- **1x-busy** - UE status 1x-busy
- **all** - UE status all
- **idle** - UE status idle
- **power-off** - UE status power-off
- **unreg** - UE status unreg
- **vt-busy** - UE status vt-busy

**reject response-code response_code**

Specifies reject for UE capability failure with specific response code. 

*response_code* must be an integer from 400 to 699.

**Usage Guidelines**

As per RFC/3GPP specifications, S-CSCF rejects with 480 response code for UE capability failure (caller preference) or UE status. Use this command to configure the S-CSCF to reject with specific response code based on UE capability failure or UE status.
Examples

The following command configures S-CSCF reject with response code 455 for a UE capability audio failure.

custom-response ue-capability-failure audio reject response-code 455
custom volte

Enables custom Voice over LTE (VoLTE) features.

**Product**

SCM

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```plaintext
configure > context context_name > csf service service_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-cscf-service)#
```

**Syntax Description**

<table>
<thead>
<tr>
<th>default</th>
<th>no</th>
<th>custom volte</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>no</td>
<td></td>
</tr>
</tbody>
</table>

Disables custom features.

**Usage Guidelines**

Use this command to enable or disable custom VoLTE features.
**default-aor-domain**

Configures the domain name of the service.

**Product**

SCM

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

`configure > context context_name > cs cf service service_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-cscf-service)#`

**Syntax Description**

| no | default-aor-domain alias |

no

Removes the domain name from the service.

**Usage Guidelines**

Use this command to define the domain name of the service.

**Examples**

The following command defines the domain name of the CSCF service as `business.com`:

`default-aor-domain business.com`
emergency-cscf

Enables the Emergency-CSCF for the service and enters the Emergency-CSCF Configuration Mode. Default is disabled.

**Product**  
SCM

**Privilege**  
Administrator

**Command Modes**  
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
configure > context context_name > csf service service_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}@hostname(config-cscf-service)#
```

**Syntax Description**  

```
no | emergency-cscf
```

**Usage Guidelines**  
Use this command to enable the Emergency-CSCF feature and enter the Emergency-CSCF Configuration Mode.

Entering this command results in the following prompt:

```
{context_name}@hostname(config-cscf-service-emergency-cscf)#
```

Emergency-CSCF Configuration Mode commands are defined in the *CSCF Emergency-CSCF Configuration Mode Commands* chapter in this guide.

---

**Important**  
Only one function (P-CSCF, S-CSCF, E-CSCF, SIP Proxy, or A-BG) can be enabled per service.
end

Ends 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.
history-info

Enables the addition of the history-info header to SIP requests in order to capture request URI information. By default, this command is disabled.

Product
SCM

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Service Configuration
configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

(context_name)host_name(config-cscf-service)#

Syntax Description
| default | no | history-info

default | no
Disables the inclusion of the history-info header.

Usage Guidelines
Use this command to include the history-info header in SIP requests to capture the request URI information for routing or translation.
interface statistics sip

Enables interface SIP statistic collection in this CSCF service.

Product: SCM

Privilege: Administrator

Command Modes: Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-cscf-service)#

Syntax Description:

| default | no | interface statistics sip

default | no

Disables interface SIP statistic collection for this service.

Usage Guidelines: Use this command to enable or disable the collection of interface SIP statistics in this service.
interrogating-cscf

This command is not supported in this release.
ipv4-ipv6-interworking

Allows the P-CSCF to provide IPv4-IPv6 interworking when UEs are IPv6-only and the IMS core network is IPv4-only. Feature is disabled by default.

Product
SCM (P-CSCF)

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-cscf-service)#

Syntax Description
| no | ipv4-ipv6-interworking

no
Disables the feature.

Usage Guidelines
Use this command to allow IPv4-IPv6 interworking functionality.
keepalive

Configures the CSCF to receive and respond to different types of keep-alive requests.

**Product**
SCM

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax Description**

```
keepalive [ expire-timer sec | max-retry num ] | max-retry num | expire-timer sec | method { crlf | stun }
| expire-timer sec | max-retry num | max-retry num | expire-timer sec |
| default keepalive | expire-timer | max-retry | expire-timer | method | expire-timer | max-retry |
no keepalive | method { crlf | stun }
```

**default**

Returns the command to the default settings. All methods are enabled by default. See keywords above for specific defaults.

**no**

Disables the specified method of keepalive messages.

**expire-timer sec**

Default: 29

This value is used according to timed-keepalives parameter present in Path header. UEs are expected to send keepalive messages according to this time interval.

`sec` must be an integer from 24 to 150.

**max-retry num**

Default: 3

Specifies the maximum number of times the CSCF waits for the UE to send a keepalive request before it deletes the user information.

`num` must be an integer from 1 to 10.
method { crlf | stun }

Default: both methods enabled.
Specifies the method of keepalive messages supported by the CSCF.

crlf: "\r\n" string (CRLF packets) sent by UE
stun: STUN protocol messages (rfc3489-bis)

Usage Guidelines
Use this command to configure how the CSCF manages keepalive requests.

Examples
The following example sets the expire timer to 40 and the maximum retry parameter to 5:
keepalive expire-timer 40 max-retry 5
lawful-intercept

Enables Lawful Intercept (LI) in this CSCF service. Feature is disabled by default.

**Product**

SCM

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

`configure > context context_name > cscf service service_name`

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-cscf-service)#
```

**Syntax Description**

```
[ no ] lawful-intercept
```

*no*

Disables the feature.

**Usage Guidelines**

Refer to the *Lawful Intercept Configuration Guide* for more information on LI.
li-packet-cable

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.
**max-reqmsg-size**

Configures the maximum SIP Request processing size.

**Product**
SCM

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

`configure > context context_name > cscf service service_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-cscf-service)#`

**Syntax Description**

```
[ no ] max-reqmsg-size sipreq_size
```

- **no**
  - Disables the SIP processing configuration.
  - If disabled, then P-CSCF will not reject the message with 513 and the old functionality of message drop based on `max-sipmsg-size` will only apply.

- **sipreq_size**
  - Configures the SIP request processing size limit in bytes.
  - `sipreq_size` must be an integer from 1024 to 65535.

**Usage Guidelines**

Use this command to configure the maximum SIP Request processing size.

The configured value for `max-reqmsg-size` must always be lesser than the configured value for `max-sipmsg-size` in the same CSCF service for the new implementation to take effect.

**Examples**

The following command limits the SIP request processing size to **1024** bytes:

```
max-reqmsg-size 1024
```
max-sipmsg-size

Configures the maximum SIP message size.

Product
SCM

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-cscf-service)#

Syntax Description
max-sipmsg-size limit
| default | no | max-sipmsg-size

default | no
Returns/sets the maximum SIP message size to 4096 bytes.

limit
Default: 4096
Configures the SIP message size limit in bytes.

limit must be an integer from 1024 to 65535.

Important
Maximum SIP message size should be more than the message-max-size set in the CSCF Proxy-CSCF Configuration Mode.

Usage Guidelines
Use this command to configure the maximum SIP message size.

Examples
The following command limits the SIP message size to 4500 bytes:

max-sipmsg-size 4500
media-bridging

Enables SDP modification that terminate media on CSCF. Feature is disabled by default.

**Product**
SCM (P-CSCF)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration
counte r > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax Description**

```
media-bridging [v6port-range start_port end_port]
nomedia-bridging
```

- **no**
  Disables the feature.

- **v6port-range start_port end_port**
  Specifies port ranges to be used with IPv6 addresses. Only selected ports from the range specified should be used for media bridging.
  - **start_port**: Start of port range; must be an integer from 1024 to 65535.
  - **end_port**: End of port range; must be an integer from 1025 to 65535.

**Usage Guidelines**
Use this command to allow termination of media on CSCF.

**Examples**
The following command allows media bridging on ports 2000 to 4000 for IPv6 addresses:
```
media-bridging v6port-range 2000 4000
```
monitoring

Enables thresholds alerting for this CSCF service.

Product

SCM

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-cscf-service)#

Syntax Description

monitoring

Usage Guidelines

Use this command to enable thresholds alerting for this CSCF service.
multiple-reg same-private-id

This command allows multiple registrations for the same private user-id from different devices.

**Product**
SCM (P-CSCF, A-BG, S-CSCF)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax Description**

| default | no | multiple-reg same-private-id |

**Usage Guidelines**

Use this command to allow or disallow multiple registrations for the same private user-id from different devices.

**Examples**

The following command allows multiple registrations for the same private user-id from different devices:

```
multiple-reg same-private-id
```
**nat-policy**

Configures a NAT (Network Address Translation) policy for the service if the CSCF service is performing one of the following functions:

- CSCF services are run in bridging (Back-to-Back User Agent) mode
- A-BG is an Application-level Gateway (ALG) for NAT

**Product**

SCM (CSCF A-BG)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-cscf-service)#

**Syntax Description**

```
nat-policy policy_name { private-address ( address ip_address_mask | default | range start_ip_address end_ip_address ) | bridge-network { address ip_address_mask | range start_ip_address end_ip_address } }
no nat-policy policy_name
```

no

Removes the specified NAT policy from the service.

**policy_name**

Specifies a name for the NAT policy.

`policy_name` must be from 1 to 79 alpha and/or numeric characters.

**private-address { address ip_address_mask | default | range start_ip_address end_ip_address }**

Specifies the private-address policy type for nat-pool.

`address ip_address_mask`: Address for nat-policy policy type for nat-pool. Specifies a combined IP address subnet mask bits to indicate what IP addresses the specific policy type applies to. `ip_address_mask` must be specified using the form "IP Address/Mask Bits" where the IP address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6, and the mask bits are a numeric value, which is the number of bits in the subnet mask.
default: Default for nat-policy policy type for nat-pool. Default is defined as the address range specified by rfc1918.

- 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

range start_ip_address end_ip_address: Range for nat-policy policy type for nat-pool.

- start_ip_address specifies the beginning of the range of addresses.
- end_ip_address specifies the end of the range of addresses.
- ip_address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

bridge-network { address ip_address_mask | range start_ip_address end_ip_address }

Specifies the bridge-network policy type for S-CSCF bridging.

address ip_address_mask: Address for bridge-network policy type for S-CSCF bridging. Specifies a combined IP address subnet mask bits to indicate what IP addresses the specific policy type applies to. ip_address_mask must be specified using the form "IPAddress/MaskBits" here the IP address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6, and the mask bits are a numeric value, which is the number of bits in the subnet mask.

range start_ip_address end_ip_address: Range for bridge-network policy type for S-CSCF bridging.

- start_ip_address specifies the beginning of the range of addresses.
- end_ip_address specifies the end of the range of addresses.
- ip_address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

Usage Guidelines

Generally, if a SIP packet has a VIA address (physical address that identifies where the service is located) different from the Source address, ALG functionality is invoked. Even if the VIA and Source addresses are the same, however, this command allows the ALG functionality to be started. For ALG to start, the VIA address should belong to one of the nat-policy address ranges.

Examples

The following command identifies the NAT policy named policy1 with a private-address policy type of 10.10.10.10 255.255.255.0:

```
nat-policy policy1 private-address address 10.10.10.10 255.255.255.0
```

The following command identifies the NAT policy named policy2 with a private-address range policy type of 172.162.23.23 172.162.23.230:

```
nat-policy policy2 private-address address 172.162.23.23 172.162.23.230
```

The following command identifies the NAT policy named policy3 with a default policy type:

```
nat-policy policy3 private-address default
```
nat-pool

Configures a NAT (Network Address Translation) pool for the service if the CSCF service is performing one of the following functions:

- P-CSCF services are run in bridging (Back-to-Back User Agent) mode
- A-BG is an Application-level Gateway (ALG) for NAT

By default, no nat-pool name will be present.

Product

SCM (P-CSCF A-BG)

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-cscf-service)#

Syntax Description

nat-pool name pool_name [ signalling-pool signalling_pool_name ]

no nat-pool name pool_name

no

Removes the NAT pool from the service.

name pool_name

Specifies the name of an existing NAT pool.

pool_name must be from 1 to 32 alpha and/or numeric characters.

Important

NAT pools are created in Context Configuration Mode with the ip pool command.

signalling-pool signalling_pool_name

Specifies the name of an existing IP pool from where IP addresses will be used to fill in signalling headers only.

signalling_pool_name must be from 1 to 32 alpha and/or numeric characters.
Important If signalling-pool is not specified, service IP:port will be filled in signalling headers.

**Usage Guidelines**
Use this command to assign a NAT pool to the P-CSCF/A-BG service.

**Examples**
The following command identifies the NAT pool:
```
nat-pool name pool2
```
**policy**

Enables or disables early media support and IBCF capability in P-CSCF/A-BG. In addition, configures Interim-Interval value for CSCF accounting sessions, overload response, and the congestion control threshold and tolerance values that are to be monitored on this CSCF service.

**Product**

SCM (P-CSCF, A-BG)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
configure context context_name cscfservice service_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-cscf-service)>
```

**Syntax Description**

```
policy { accounting interim-interval value | allow-early-media | ibcf-capability domain domain/name | overload | drop | redirect IPv4_address1 | weight weight1 | IPv4_address2 | weight weight2 | ... | reject | | threshold congestion-control { system-cpu-utilization percent | tolerance percent } | default policy { allow-early-media | overload | threshold congestion-control { system-cpu-utilization | tolerance } } | no policy { accounting interim-interval | allow-early-media | ibcf-capability domain domain/name | overload | redirect IPv4_address1 | IPv4_address2 | ... | threshold congestion-control { system-cpu-utilization | tolerance } } | default
```

**default**

Returns the command to the default settings. See keywords above for specific defaults.

**no**

Disables the specified functionality.

**accounting interim-interval value**

Default: Disabled

Used to configure Interim-Interval value for CSCF accounting sessions.

*value* can be configured to any integer value from 50 to 7200. This value is sent in the "Act-Interim-Interval" AVP of the accounting message. Based on the response message from accounting server, Interim-Interval timer is started.
**allow-early-media**
Default: Enabled
Allows early media by doing QoS commit during QoS Authorization (with PCRF) in P-CSCF.

**ibcf-capability domain** *domain/name*
Enables IBCF capability to support Mx reference point in CSCF.
IBCF capability domain name must be entered using from 1 to 80 alpha and/or numeric characters.

---

**Important**
This CLI can be repeated to add/delete multiple entities to/from the ibcf-capability domain table. An ibcf-capability domain can be removed by using the **no** keyword; using the **no** keyword without giving any domain name will delete all entries from the list.

---

**overload** [drop | redirect] *IPv4_address1* [weight *weight1*] [IPv4_address2 [weight *weight2*]] ... [reject]
Configures the overload response for this policy. When the P-CSCF/A-BG becomes congested, this overload policy is used to drop/reject subsequent sessions or redirect them to another server.

- **drop:** Specifies that upon policy overload, the system will drop the session.
- **redirect:** Specifies that upon policy overload, the system will redirect the session to another CSCF.
  
  - *IPv4_address1* must be expressed in dotted decimal notation.
  
  - **weight** *weight1:* Defines the priority of the redirect address.
    
    *weight1* must be an integer from 1 to 10. Default is 1.

- **reject:** Specifies that upon policy overload, the system will reject the session with 503 (Service Unavailable) SIP error response. This is the default setting.

**threshold congestion-control** { system-cpu-utilization *percent* | tolerance *percent* }
Enables congestion control. CSCF performs congestion control based on the memory usage inside every sessmgr at two levels.

- **Level 1:** For every new call/event received, the system checks if sessmgr memory-usage is above a threshold value (such as 95 percent). If it is, memory-congestion is triggered and new call messages are rejected with 500 SIP response. Memory congestion is disabled when memory usage drops by a tolerance value (default is 10 percent).

- **Level 2:** If the sessmgr usage reaches 100 percent, all newly received SIP messages are dropped at the socket layer in that sessmgr except for the BYE message. The new SIP messages are not processed until the memory reaches the threshold value (95 percent).

A trap is also generated whenever sessmgr is in congestion state

**system-cpu-utilization** *percent:* The average percent utilization of a CPU in a PSC/PSC2/PSC3 running the CSCF service as measured in 10 second intervals.

*percent* can be configured to any integer value from 0 to 100. This value becomes the upper threshold for triggering the CPU-based congestion for CSCF services. Default is 80.
tolerance percent: The percentage under a configured threshold that dictates the point at which the condition is cleared.

percent is an integer value from 1 to 25. Default is 5

Usage Guidelines

Use this command to set the following policy for this CSCF service:

- Configure Interim-Interval value for CSCF accounting sessions.
- Set QoS support during either the initial SDP response or the 200OK response to the INVITE. When allow-early-media is enabled, QoS commit is done during initial SDP answer. When disabled, QoS commit is done during 200OK INVITE. By default, this command is enabled.
- Enable or disable IBCF capability.
- Define the response to an overload condition.
- Set thresholds to dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the CSCF service (congested or clear). The tolerance parameter establishes the threshold at which the condition is cleared.

Important: When congestion is triggered, new CSCF calls are not rejected.

Examples

The following command sets the upper threshold for CPU utilization for triggering congestion control at 90%.

```
policy threshold congestion-control system-cpu-utilization 90
```

The following command sets the tolerance to its default value of 5.

```
default policy threshold congestion-control tolerance
```
policy-name

Assigns a previously created service policy to this service.

**Product**
SCM

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

`configure > context context_name > cscf service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax Description**

```
policy-name name
no policy-name
```

- **no**
  Remove the assigned service policy from this service.

- **name**
  Specifies the name of the service policy being assigned to this service.

  *name* must be from 1 to 79 alpha and/or numeric characters and be an existing policy name in the system. Service policies are created and maintained in the CSCF Policy Configuration Mode.

**Usage Guidelines**

Use this command to assign a service policy to this service. The policies defined in the service policy apply to all subscribers using this service. Service policies are created and maintained in the CSCF Policy Configuration Mode.

**Examples**

The following command assigns a service policy named `serv_policy3` to this service:

```
policy-name serv_policy3
```
proxy-cscf

Enables the Proxy-CSCF for the service and enters the Proxy-CSCF Configuration Mode. Default is disabled.

Product
SCM (P-CSCF)

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Service Configuration
configure > context context_name > cscf service service_name

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

Syntax Description
| no | proxy-cscf

no
Disables the P-CSCF for the service.

Usage Guidelines
Use this command to enable the Proxy-CSCF feature and enter the Proxy-CSCF Configuration Mode.

Entering this command results in the following prompt:
{context_name}hostname(config-cscf-service-proxy-cscf)#

Proxy-CSCF Configuration Mode commands are defined in the CSCF Proxy-CSCF Configuration Mode Commands chapter in this guide.

Important
The Proxy-CSCF is a license-enabled function of the Session Control Manager. Only one function (P-CSCF, S-CSCF, E-CSCF, SIP Proxy, or A-BG) can be enabled per service.
proxy-serving-cscf

This command is not supported in this release.
recurse-on-redirect-resp

Enables the 3xx recursion feature. If enabled, the service will send further invites to the contacts specified upon receiving a 3xx redirect response. Default is disabled.

**Product**
SCM

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration
`configure > context context_name > cscf service service_name`

Entering the above command sequence results in the following prompt:
`(context_name)host_name(config-cscf-service)#`

**Syntax Description**

`| no | recurse-on-redirect-resp`

`no`
Disables the 3xx recursion feature.

**Usage Guidelines**
When enabled and on receipt of a 3xx response, the service will collect the SIP URIs present in the Contact header(s) of 3xx and recursively contact each one of them until the call succeeds. The contacts are tried serially. There is a maximum implementation limit of 50 URIs. Each contact, in turn, can send a 3xx response. The service will honor them and append the new contacts. When disabled, the service treats a 3xx response as the final failure response and declares the call attempt "failed". By default, this feature is disabled.

**Examples**
Enable recursion on 3xx:
`recurse-on-redirect-resp`

Disable recursion on 3xx:
`no recurse-on-redirect-resp`


**reject-on-cnsa-failure**

Enables rejection of messages on Core Network Service Authorization failure. Default is disabled.

**Product**
SCM

**Privilege**
Administrator

**Command Modes**
Exec &gt; Global Configuration &gt; Context Configuration &gt; CSCF Service Configuration

```
configure &gt; context context_name &gt; cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax Description**

| no | reject-on-cnsa-failure |

**no**

Disables the rejection of messages on Core Network Service Authorization failure.

**Usage Guidelines**

Enables rejection of messages on Core Network Service Authorization failure. By default, this feature is disabled.

In a mobile originating case, S-CSCF checks for the presence of P-Preferred-Service (PPS) header. If the header is present, media profile authentication is successful and if the incoming ICSI (IMS Communication Service Identifier) value also matches with one of the values in the service_id list, then the request will be forwarded after replacing the PPS header with PAS (P-Asserted-Service). If media profile authentication fails, S-CSCF will check reject-on-cnsa-failure. If enabled, then call is rejected with 403 message. If disabled, a default ICSI is selected from the service_id list and will be put into PAS while forwarding the request by the S-CSCF on service authentication failure.

In PPS is not received by the S-CSCF and media profile authentication is successful, an ICSI from the service_id list, if present, is selected and will be added in PAS header. If media profile authentication fails, reject-on-cnsa-failure is checked. If enabled, call is rejected with 403 message. If disabled, PAS header is added if service_id list is present with an ICSI value.

**Examples**

Enable rejection of messages on Core Network Service Authorization failure:
```
reject-on-cnsa-failure
```

Disable rejection of messages on Core Network Service Authorization failure:
```
no reject-on-cnsa-failure
```
release-call-on-media-loss

Release call on detection of media loss.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
configure > context context_name > cscf service service_name
```

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

**Syntax Description**
```
release-call-on-media-loss media-type audio [ timeout seconds ]
no release-call-on-media-loss
```

- **no**
  Disables the release of SIP calls upon the detection of media loss.

- **media-type audio**
  Enables the release of SIP calls upon the detection of media loss on media-type audio.

- **timeout seconds**
  Specifies the media loss timeout value; media loss after timeout value results in call release.
  *seconds* must be an integer from 5 to 3600.
  If timeout value is not configured, media loss after 5 seconds results in call release.

**Usage Guidelines**
Use this command to enable the release of SIP calls upon the detection of media loss.

**Examples**
- Enables the release of SIP calls upon the detection of media loss:
  ```
  release-call-on-media-loss media-type audio
  ```
- Enables the release of SIP calls upon the detection of media loss:
  ```
  no release-call-on-media-loss
  ```
rfc3261-proxy

Enables RFC3261 proxy (SIP Proxy) for this service and enters the SIP Proxy Configuration Mode. Default is disabled.

**Product**

SCM (SIP Proxy)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

`configure > context context_name > cscf service service_name`

Entering the above command sequence results in the following prompt:

`{context_name}@host_name(config-cscf-service)#`

**Syntax Description**

| default | no | rfc3261-proxy |

*default | no*  
Disables RFC3261 proxy in this service.

**Usage Guidelines**

Use this command to enable the SIP Proxy feature and enter the SIP Proxy Configuration Mode.

Entering this command results in the following prompt:

`{context_name}@hostname(config-cscf-service-rfc3261-proxy)#`

SIP Proxy Configuration Mode commands are defined in the *CSCF SIP Proxy Configuration Mode Commands* chapter in this guide.

**Important**

The SIP Proxy is a license-enabled function of the Session Control Manager. Only one function (P-CSCF, S-CSCF, E-CSCF, SIP Proxy, or A-BG) can be enabled per service.
server-header

This command determines the handling of the server header. This is applicable for B2BUA mode only; Proxy mode will forward the message as it is.

Product

SCM (P-CSCF, A-BG, S-CSCF, SIP Proxy)

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Service Configuration
configure > context context_name > scf service service_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-cscf-service)#

Syntax Description

server-header { name header_name | pass-through }
| default | no | server-header

default

Sets the server header to the default server header. The default server name is "Cisco".

no

Suppresses server header; no server header is forwarded or added.

name header_name

Sets the server header to the value specified by header_name.

header_name must be from 1 to 63 alpha and/or numeric characters.

pass-through

S-CSCF forwards the server header received without any modification. If no server header is received, no server header is added.

Usage Guidelines

Use this command to determine the handling of the server header, including forwarding, modifying, adding, or suppressing.
Examples

The following command forwards the server header received without any modification:

`server-header pass-through`
server-name

Enables/disables filling the server name AVP in MAR and SAR for Cx interface, and the From header in third party register request, with configured server name. In addition, it can be used by other CSCF service to fill From header while performing peer server monitoring using OPTIONS request. This command is disabled by default.

Product
SCM (S-CSCF)

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

{context_name}\host_name{(config-cscf-service)#

Syntax Description
server-name server_name
no server-name

no
S-CSCF uses configured cscf-hostname or bind IP address to fill the server name AVP in MAR and SAR for Cx interface. This is the default CSCF behavior.

server_name
Configures the name that will be used to fill the server name AVP in MAR and SAR for Cx interface, and the From header in third party register request. In addition, it can be used by other CSCF service to fill From header while performing peer server monitoring using OPTIONS request.
name must be from 1 to 63 alpha and/or numeric characters.

Usage Guidelines
Use this command to enable/disable filling the server name AVP in MAR and SAR for Cx interface, and the From header in third party register request, with configured server name. In addition, it can be used by other CSCF service to fill From header while performing peer server monitoring using OPTIONS request.

Examples
The following command configures the CSCF server name as stp-c-scsf1.cisco.co.kr:

server-name stp-c-scsf1.cisco.co.kr
serving-cscf

Enables Serving-CSCF for the service and enters the Serving-CSCF Command Mode. Default is disabled.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

\[context_name\]host_name(config-cscf-service)#

**Syntax Description**

\[ no \] serving-cscf

no

Disables S-CSCF for the service.

**Usage Guidelines**

Use this command to enable the Serving-CSCF feature and enter the Serving-CSCF Configuration Mode. Entering this command results in the following prompt:

\[context_name\]hostname(config-cscf-service-serving-cscf)#

Serving-CSCF Configuration Mode commands are defined in the CSCF Serving-CSCF Configuration Mode Commands chapter in this guide.

**Important**
The Serving-CSCF is a license-enabled function of the Session Control Manager. Only one function (P-CSCF, S-CSCF, E-CSCF, SIP Proxy, or A-BG) can be enabled per service.
serving-cscf-list

Configure a list of Serving CSCFs and their capabilities.

Product
SCM

Privilege
Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-cscf-service)#

Syntax Description

| no | serving-cscf-list server { address address | domain domain } { capability value | port num } { capability value } |

no
Removes an entry from this list.

server { address address | domain domain }
Specifies the S-CSCF server.

address address: IP addresses must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

domain domain: Domain names must be entered using from 1 to 80 alpha and/or numeric characters.

capability value
Specifies the capability of the S-CSCF server. value is assigned by the Service Provider and may be an integer from 1 to 999999.

port num
Specifies the port at which service is provided by the S-CSCF server. num may be an integer from 1 to 65535.

Usage Guidelines
Use this command to configure a list of Serving CSCFs and their capabilities.
This command can be entered multiple times to identify multiple Serving CSCFs.

**Examples**

The following command adds a S-CSCF with an IP address of 1.2.3.4 and a capability value of 75 to this service's list:

```
serve-cscf-list server address 1.2.3.4 capability 75
```
session-timer

Configures the session expiry for sessions (Session will expire at the configured value unless refreshed.) and the minimum number of seconds in a session timer (session-expires) value the system will allow.

Product
SCM

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Syntax Description
session-timer { min-se sec | session-expires sec | session-expires sec | min-se sec } } default session-timer [ min-se | session-expires ]
no session-timer

default
Returns the command to the default settings.

no
Disables the session timer.

min-se sec
Default: 90
Specifies the minimum number of seconds the system will allow a session-expires value in a session request. sec must be an integer value between 90 and the value of the session-expires command.

session-expires sec
Default: 1800 (30 minutes)
Specifies the number of seconds a session is allowed exist before it expires. sec must be an integer value between 90 and 18000.
Usage Guidelines

Use this command to set a session expiry value for all invites generated by the SCM and a minimum value for a session request session timer the system will allow. If a session is requested with a timer of less than this command's value, the system will reject the request with a "422 Session Interval Too Small" response code.

Examples

The following command sets the session expiry for all sessions generated by the SCM to 60 minutes:

```
session-timer session-expires 3600
```
strict-check configured-aor-domain

Enables strict checking on default-aor-domain so S-CSCF will reject registration and invite if there is a mismatch between AoR in To/From and the configured default-aor-domain.

**Product**

SCM (S-CSCF)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

*configure* > context *context_name* > cscf service *service_name*

Entering the above command sequence results in the following prompt:

*(context_name)*host_name* (config-cscf-service)*#

**Syntax Description**

| default | no | strict-check configured-aor-domain |

**Usage Guidelines**

Use this command to enable or disable strict checking on default-aor-domain. This allows support for registration of subscribers from multiple domains.

**Usage Guidelines**

default | no

Disables strict checking on default-aor-domain. This is the default behavior.
strict-outbound

When enabled, the CSCF rejects registration without outbound parameters from an already registered AoR (the AoR would have included outbound parameters in a previous registration). When disabled, the CSCF allows registration without outbound parameters from the previously registered AoR.

Product

SCM

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service)#

Syntax Description

[ no ] strict-outbound

no

Disables the feature. This is the default behavior.

Usage Guidelines

Use this command to reject registration from a previously registered AoR if the AoR fails to register with outbound parameters but included them in the previous registration.
subscriber-policy-override

Configures the system to allow the subscriber-based policy to override the service-based policy. Default is disabled.

**Product**
SCM

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

`configure > context context_name > cscf service service_name`

Entering the above command sequence results in the following prompt:

`{context_name}@host_name(config-cscf-service)#`

**Syntax Description**

<table>
<thead>
<tr>
<th>default</th>
<th>no</th>
<th>subscriber-policy-override</th>
</tr>
</thead>
</table>

**Usage Guidelines**
By default, if a conflict occurs between the subscriber-based policy and the service-based policy, the service policy takes precedence. Use this command to override the default behavior of the system and allow the subscriber-based policy to overrule the service policy.
subscription

Enables the registration event package for the service and configures a system-wide subscription lifetime for all subscribers to the service.

**Product**

SCM

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

`configure > context context_name > csf service service_name`

Entering the above command sequence results in the following prompt:

`{context_name}@host_name(config-cscf-service)#`

**Syntax Description**

`subscription package reg [ lifetime { default sec | max sec | default sec | min sec | max sec | default sec } ]

| default | no | subscription package reg

default

Returns the command to the default settings.

no

Disables the registration event package for the service.

`package reg [ lifetime { default sec | max sec | min sec }]

default sec`: Specifies the default amount of time that a subscription can exist on the system. `sec` must be an integer from 60 to max sec -1.

Default: 3761

---

**Important**

`default sec` must be < or = to max sec and > or = to min sec.

The following keywords are specific to the S-CSCF functionality:

max sec: Specifies the maximum amount of time that a subscription can exist on the system.

`sec` must be an integer from 60 to 2147483646.

Default: 86400
Important max sec must be > or = to min sec.

\textbf{min sec}: Specifies the minimum amount of time that a subscription can exist on the system.

\textit{sec} must be an integer from 60 to max sec -1.

Default: 60

Important min sec must be < or = to max sec.

**Usage Guidelines**

Use this command to enable the registration event package for the service and control the amount of time subscriptions are allowed to exist on this service.

The system responds to subscriptions in the following manner:

Using default values:

- If a subscription with an expiration value lower than the service's minimum (60) is received, the service will respond with a 423 Interval Too Small message.
- If a subscription with an expiration value higher than the service's maximum (2147483646) is received, the service will automatically reduce the expiration value to the default value.

If a subscription is received missing the "Expires" value, or the value is malformed, the service will automatically respond with 3761 in the 200OK message.

**Examples**

The following command configures the maximum subscription lifetime to \textit{43200} (12 hours):

\texttt{subscription package reg lifetime max 43200}
support-content-type any

Validates Content-Type in this CSCF service.

**Product**
SCM

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax Description**

```
[ no ] support-content-type any
```

- **no**
  Disables the feature. If disabled, CSCF service rejects unsupported Content-Type with "415 Unsupported Media Type".

**Usage Guidelines**

Use this command to either allow any type of Content-Type or reject unsupported Content-Type.

**Examples**

- Allows any type of Content-Type for the CSCF service:
  ```
support-content-type any
  ```
- Rejects unsupported Content-Type for the CSCF service:
  ```
no support-content-type any
  ```
tcp-proxy

Enables SIP TCP proxy for the CSCF service.

**Product**
SCM

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

cfg> context context_name > csf service service_name

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-cscf-service)#
```

**Syntax Description**
tcp-proxy | port port_number | 
no tcp-proxy

- **no**
  Disables SIP TCP proxy for the CSCF service

- **port port_number**
  Default: 5062
  Specifies the port used for SIP TCP proxy connections.
  *port_number* must be an integer from 1 to 65534.

**Usage Guidelines**
Use this command to enable SIP TCP proxy for the CSCF service.

**Examples**
Enables SIP TCP proxy for the CSCF service on port 5062:

tcp-proxy port 5062

Disables SIP TCP proxy for the CSCF service:

no tcp-proxy
threshold

Enables thresholds alerting and configuration of thresholds for CSCF Service.

**Product**  
SCM

**Privilege**  
Administrator

**Command Modes**  
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax Description**

```
threshold { { call-setup-failures | call-total-active | error-no-resource | error-presence | error-reg-auth | error-tcp | invite-rcvd-rate | monitoring | reg-rcvd-rate | reg-total-active | route-failures } high_thresh |
{ clear low_thresh } | monitoring |
} default | no | threshold monitoring

default

Returns the command to the default settings.

**no**

Disables thresholds alerting for CSCF Service.

```
{ call-setup-failures | call-total-active | error-no-resource | error-presence | error-reg-auth | error-tcp | invite-rcvd-rate | reg-rcvd-rate | reg-total-active | route-failures } high_thresh clear low_thresh
```

**call-setup-failures**: Number of CSCF call setup failures.

Default: 0

**call-total-active**: Number of total active CSCF calls.

Default: 0

**error-no-resource**: Number of CSCF call setup failures due to no-resource.

Default: 0

**error-presence**: Number of CSCF Presence errors.

Default: 0

**error-reg-auth**: Number of CSCF Registration Authentication failures.
Default: 0

**error-tcp**: Number of CSCF call setup failures due to TCP error.
Default: 0

**invite-rcvd-rate**: Number of CSCF calls per polling interval.
Default: 0

**reg-rcvd-rate**: Number of CSCF registrations per polling interval.
Default: 0

**reg-total-active**: Number of total CSCF active registrations.
Default: 0

**route-failures**: Maximum number of route-failures, after which the alarm/alert will be raised. Default: 5

*high_thresh*: The high threshold number that must be met or exceeded within the polling interval to generate an alert or alarm. Can be configured to any integer value between 0 and 2000000 (0 and 60000 for route-failures).

*clear low_thresh*: The low threshold number that must be met or exceeded within the polling interval to clear an alert or alarm. Can be configured to any integer value between 0 and 2000000 (0 and 60000 for route-failures).

---

**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.

---

**monitoring**

Enables thresholds alerting for CSCF Service.

---

**Usage Guidelines**

Use this command to:

- enable/disable thresholds alerting for CSCF Service
- set an alert or an alarm when a threshold exceeds the configured level

Alerts or alarms are triggered for the number of registration reply errors on the following rules:

- Enter condition: Actual number > High Threshold
- Clear condition: Actual number < Low Threshold

---

**Examples**

The following command configures a route failures threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

```
threshold route-failures 1000 clear 500
```
**timeout**

Sets timeout values for CSCF and SIP transactions.

**Product**

SCM

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```plaintext
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax Description**

```plaintext
timeout { hss-wait sec | map-slr-response sec | no-answer sec | policy-interface sec | sip { 3gpp-d sec | 3gpp-t1 msec | 3gpp-t2 sec | 3gpp-t4 sec | c sec | d sec | idle-tcp-connection msec | cleanup-timer msec | invite-expiry sec | t1 msec | t2 sec | t4 sec } }
```

**default timeout**

Returns the command to the default settings. See keywords above for specific defaults.

- **hss-wait sec**
  
  Default: 5
  
  This timer is used by S-CSCF with HSS interface for timeout.
  
  `sec` must be an integer from 0 to 2147483646.

- **map-slr-response sec**
  
  Default: 15
  
  This timer is used by the E-CSCF for MAP SLR response timeout.
  
  `sec` must be an integer from 15 to 30.

- **no-answer sec**
  
  Default: 100
This timer is specially used for No-Answer Call Feature executed by S-CSCF. The timer will be started as soon as 180 Ringing response is received and No-Answer call feature is enabled. The value of this timer should be always less than INVITE Timeout used by DC-SIP.

\( sec \) must be an integer from 0 to 2147483646.

**policy-interface sec**

Default: 5

This timer is used by the P-CSCF/A-BG with Policy interface for timeout.

\( sec \) must be an integer from 0 to 2147483646.

**sip { 3gpp-d sec | 3gpp-t1 msec | 3gpp-t2 sec | 3gpp-t4 sec | c sec | d sec | idle-tcp-connection msec | cleanup-timer msec } | invite-expiry sec | t1 msec | t2 sec | t4 sec }**

Sets transaction and expiry timers for SIP.

- **3gpp-d sec**: This timer is used to control the retransmission of 200OK messages to INVITEs after an ACK is sent. The ACK transaction is cleared after this period. This timer is applicable only for unreliable transport. \( sec \) must be an integer from 0 to 2147483646.
  
  Default: 64*T1 (128 seconds, recommended minimum)

- **3gpp-t1 msec**: This timer is used to control the time interval between each retransmission. The interval doubles after each retransmission. This is used by P-CSCF/A-BG only when it sending message toward the UE. Example: T1, 2T1, 4T2, etc. This timer is applicable only for unreliable transport. \( msec \) must be an integer from 0 to 4294967294.
  
  Default: 2000 ms (2 secs, recommended minimum).

- **3gpp-t2 sec**: This timer is used to control the period for which the request continues to get retransmitted. This is used by P-CSCF/A-BG only when it sending message toward the UE. This timer is applicable both for reliable and unreliable transport. \( sec \) must be an integer from 0 to 2147483646.
  
  Default: 16 seconds (recommended minimum).

- **3gpp-t4 sec**: This timer is used to control the period for which the final response to non-invite transaction should be buffered. The buffered response for the retransmitted non-invite request should be sent within that interval. This timer is applicable only for unreliable transport. \( sec \) must be an integer from 0 to 2147483646.
  
  Default: 17 seconds (recommended minimum).

- **c sec**: This timer is used for an INVITE transaction; if the response is a provisional response with status codes 101 to 199 inclusive (anything but 100), the proxy must reset timer C for that client transaction. The timer may be reset to a different value, but this value must be greater than 3 minutes (180 seconds). When timer C in S-CSCF fires first, S-CSCF will send CANCEL request to Terminating P-CSCF and Terminating P-CSCF will send CANCEL request to UAS. \( sec \) must be an integer from 180 to 2147483646.
  
  Default: 180 seconds

- **d sec**: This timer is used to control the retransmission of 200OK to INVITE after ACK is sent. The ACK transaction will be cleared after this interval. This timer is applicable only for unreliable transport. \( sec \) must be an integer from 0 to 2147483646.
  
  Default: 64*T1 (32 seconds, recommended minimum)
• **idle-tcp-connection msec**: This timer is used for closing idle TCP connections. If there is not activity in the TCP connection for the configuration duration, then the connection will be closed. `msec` must be an integer from 1000 (recommended minimum) to 4294967294.
  
  Default: 42000 milliseconds.

• **cleanup-timer msec**: This timer is used to control how often to check for idle TCP connections. `msec` must be an integer from 2000 to 2147483646.
  

• **invite-expiry sec**: This timer is used by SIP while acting as UA Role and no final response is received for the INVITE request sent. This timer is applicable for both reliable and unreliable transport. `sec` must be an integer from 0 to 2147483646.
  
  Default: 100 seconds (recommended minimum).

• **t1 msec**: Specifies the time interval (in microseconds) between each retransmission. The interval doubles after each retransmission, for example: T1, 2T1, 4T2, etc. This timer is applicable only for unreliable transport. `msec` must be an integer from 0 to 2147483646.
  
  Default: 500 milliseconds (recommended minimum).

• **t2 sec**: This timer is used to control the period for which the request keeps getting retransmitted. This timer is applicable both for reliable and unreliable transport. `sec` must be an integer from 0 to 2147483646. The recommended minimum value for this parameter is 4 seconds.
  
  Default: 64*T1 (32 seconds)

• **t4 sec**: This timer is used to control the period for which the final response to non-invite transaction should be buffered so as to send the buffered response for the retransmitted non-invite request within that interval. This timer is applicable only for unreliable transport. `sec` must be an integer from 0 to 2147483646.
  
  Default: 5 seconds (recommended minimum).

**Usage Guidelines**

Use this command to configure SIP Stack timers and CSCF service specific timers.

**Examples**

The following command sets the SIP d timer to 64 seconds:

```
timeout sip d 64
```
**transport-switching**

Sets the message size that triggers a transport protocol switch.

**Product**

SCM

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-cscf-service)#
```

**Syntax Description**

```
transport-switching policy protocol tcp trigger msg-size size
default transport-switching policy protocol tcp trigger msg-size
```

**default**

Returns the size of the SIP message beyond which transport changes to TCP to 1300 bytes.

**policy protocol tcp trigger msg-size size**

Default: 1300

Specifies the size of the SIP message beyond which transport changes to TCP.

size can be configured to any integer value between 1300 and 65535.

**Usage Guidelines**

Use this command to configure the size of the SIP message beyond which transport changes to TCP.

**Examples**

Switch to TCP transport protocol when the SIP message size is 4000 bytes or more:

```
transport-switching policy protocol tcp trigger msg-size 4000
```
trusted-domain-entity

Adds trusted network nodes (or entities) to a table used by this service to identify those nodes that can be trusted with subscriber information.

Product

SCM (S-CSCF)

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-cscf-service)#

Syntax Description

trusted-domain-entity address [ foreign-network ] [ private-network ]

no trusted-domain-entity address

no

Removes an entry from this service's trusted domain table.

address

Specifies the IP address of the network node identified as a trusted entity by this service. address must be either an IP address or a domain name. IP addresses must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6. Domain names must be entered using from 1 to 80 alpha and/or numeric characters.

foreign-network

Entity belongs to Foreign Network.

private-network

Entity belongs to Private Network.

Usage Guidelines

Use this command to identify to the service the network entities that can be trusted with subscriber information by this service.
This command can be entered multiple times to identify multiple trusted network entities. In StarOS v12.x and earlier, a maximum of 50 entries can be configured per CSCF service. In StarOS v14.0 and later, a maximum of 256 entries can be configured per CSCF service.

**Examples**

The following command adds a network node with an IP address of 1.2.3.4 to this service's trusted domain table:

```
trusted-domain-entity 1.2.3.4
```
CSCF Security Configuration Mode Commands

The CSCF Security Configuration Mode is used to configure Denial of Service (DOS) prevention commands.

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF Security Configuration

`configure > context context_name > cscf service service_name > proxy-cscf > security-parameters`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-security-parameters)#
```

**Important**

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

- `auth-failure-weight`, page 1594
- `bad-request-weight`, page 1596
- `dos-prevention`, page 1598
- `end`, page 1599
- `exit`, page 1600
- `forking-contact-limit`, page 1601
- `greylist-duration`, page 1602
- `per-aor-failure-limit`, page 1604
- `per-ip-failure-limit`, page 1606
- `threshold-rate`, page 1608
auth-failure-weight

Sets a severity number for authorization failures used in calculating a value for determining when to suspend registration attempts.

Important

The system will ignore the configuration of this command unless the dos-prevention command has been enabled.

Product

SCM (P-CSCF, A-BG)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF Security Configuration

configure > context context_name > escf service service_name > proxy-cscf > security-parameters

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-security-parameters)#

Syntax Description

auth-failure-weight weight
default auth-failure-weight

default

Sets/restore the default value assigned to the specified command.

weight

Default: 1

Assigns a weight to an authorization failure. Defines the severity of a single authorization failure.

weight must be an integer from 1 to 5.

Usage Guidelines

Use this command to define the severity of an authorization failure. This parameter is used in calculating the current number of authorization failures to compare to the per-aor-failure-limit and the per-ip-failure-limit. Configuring this command with a lower number causes the system to suspend registration attempts with repeated authorization failures much sooner than when configured with a higher number.
Examples

The following command assigns a weight of 3 to an authorization failure:

```
auth-failure-weight 3
```
bad-request-weight

Sets a severity number for bad registration requests used in calculating a value for determining when to suspend registration attempts.

Important

The system will ignore the configuration of this commandunless the dos-prevention command has been enabled.

Product

SCM (P-CSCF, A-BG)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF Security Configuration

configure > context context_name > cscf service service_name > proxy-cscf > security-parameters

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-security-parameters)#

Syntax Description

bad-request-weight weight
default bad-request-weight

default

Sets/restores the default value assigned to the specified command.

weight

Default: 2

Assigns a weight to a bad registration request. Defines the severity of a single bad request.

weight must be an integer from 1 to 5.

Usage Guidelines

Use this command to define the severity of bad registration request. This parameter is used in calculating the current number of request failures to compare to the per-aor-failure-limit and the per-ip-failure-limit.

Configuring this command with a lower number causes the system to suspend registration attempts with repeated request failures much sooner than when configured with a higher number.
Examples

The following command assigns a weight of 3 to a bad registration request:

```
bad-request-weight 3
```
do-prevention

Enables the denial of service (DoS) attack prevention feature.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF Security Configuration

```plaintext
configure > context context_name > csf service service_name > proxy-cscf > security-parameters
```

Entering the above command sequence results in the following prompt:

```plaintext
{context_name}host_name(config-security-parameters)#
```

**Syntax Description**

```
[ default | no ] dos-prevention
```

Disables the DoS attack prevention feature.

**Usage Guidelines**
Use this command to enable the DoS attack prevention feature. The default value for this command is disabled. When this command is enabled, the commands in this mode are enabled with default values configured.

**Important**
This command must be enabled before configuring other commands in this mode.
end

Exits the current 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.
forking-contact-limit

Sets a limit on the number of contacts a user ID can register with the system.

---

**Important**
The system will ignore the configuration of this command unless the `dos-prevention` command has been enabled.

---

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF Security Configuration

```
configure > context context_name > cscf service service_name > proxy-cscf > security-parameters
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-security-parameters)#
```

---

**Syntax Description**

```
forking-contact-limit limit
default forking-contact-limit
```

- **default**
  
  Sets/restores the default value assigned to the specified command.

- **limit**
  
  Default: 0
  
  Sets the maximum number of contacts a user ID can register with the system. 0 specifies that unlimited contacts can be registered per user ID.

  `limit` must be an integer from 0 to 10.

---

**Usage Guidelines**

Use this command to limit the number of contacts a user ID can register with the system.

**Examples**

The following command limits all users to 2 registered contacts on the system:

```
forking-contact-limit 2
```
greylist-duration

Configures the amount of time an AoR or IP address remains on a "grey list" after having crossed the registration authorization limit or the bad registration request limit.

**Important**
The system will ignore the configuration of this command unless the dos-prevention command has been enabled.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF Security Configuration

configure > context context_name > escf service service_name > proxy-cscf > security-parameters

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-security-parameters)#

**Syntax Description**
greylist-duration time
default greylist-duration

default
Sets/restores the default value assigned to the specified command.

time
Default: 10
Defines the time, in minutes, that an AoR or IP address remains on a "grey list".
time must be an integer from 5 to 1,440.

**Usage Guidelines**
Use this command to specify the amount of time AoRs or IP addresses remain on a "grey list" after having crossed the registration authorization limit or the bad registration request limit. Limits are described in the per-aor-failure-limit command and the per-ip-failure-limit command.
Examples

The following command sets the duration AoRs or IP addresses remain on a "grey list" to 30 minutes:

`greylist-duration 30`
**per-aor-failure-limit**

Sets a failure limit that, when exceeded, causes the suspension of registration attempts for the offending AoR.

---

**Important**

The system will ignore the configuration of this command unless the **dos-prevention** command has been enabled.

---

**Product**

SCM (P-CSCF, A-BG)

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF Security Configuration

`configure > context context_name > csf service service_name > proxy-cscf > security-parameters`

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-security-parameters)#
```

**Syntax Description**

`per-aor-failure-limit limit`

default `per-aor-failure-limit`

`default`

Sets/restores the default value assigned to the specified command.

`limit`

Default: 200

Defines the threshold for registration failures based on a calculation using weighted multipliers defined in `auth-failure-weight` and `bad-request-weight`. `limit` must be an integer from 5 to 10,000.

**Usage Guidelines**

Use this command to set a failure limit for registration attempts from an identified AoR. The following calculation determines when this threshold is reached for a specific AoR:

Current authorization failures ÷ **auth-failure-weight** = current failures per AoR

or

Total bad registration requests ÷ **bad-request-weight** = current failures per AoR
If `auth-failure-weight = 2` and `bad-request-weight = 1`, and the `per-aor-failure-limit = 100`, then the tolerance for registration authentication failures = 50 per AoR and the tolerance for bad registration requests = 100 per AoR.

When an AoR reaches the failure limit, it is added to a "grey list" for a period of time as defined by the `greylist-duration` command.

**Examples**

The following command sets the AoR failure limit to 300:

```
per-aor-failure-limit 300
```
per-ip-failure-limit

Sets a failure limit that, when exceeded, causes the suspension of registration attempts for the offending IP address.

Important

The system will ignore the configuration of this command unless the dos-prevention command has been enabled.

Product

SCM (P-CSCF, A-BG)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF Security Configuration

configure > context context_name > csf service service_name > proxy-cscf > security-parameters

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-security-parameters)#

Syntax Description

per-ip-failure-limit limit
default per-ip-failure-limit

default

Sets/restores the default value assigned to the specified command.

limit

Default: 100

Defines the threshold for registration failures based on a calculation using weighted multipliers defined in auth-failure-weight and bad-request-weight.

limit must be an integer from 5 to 10,000.

Usage Guidelines

Use this command to set a failure limit for registration attempts from an identified IP address. The following calculation determines when this threshold is reached for any IP address:

Current authorization failures ÷ auth-failure-weight = current failures per AoR

or
Total bad registration requests $\div$ **bad-request-weight** = current failures per AoR

If **auth-failure-weight** = 2 and **bad-request-weight** = 1, and the **per-ip-failure-limit** = 200, then the tolerance for registration authentication failures = 100 per each IP address and the tolerance for bad registration requests = 200 per each IP address.

When an IP address reaches the failure limit, it is added to a "grey list" for a period of time as defined by the **greylist-duration** command.

**Examples**

The following command sets the IP address registration failure limit to 200:

```
per-ip-failure-limit 200
```
threshold-rate

Configures the rate per second at which the system must receive authorization failures or bad registration requests before it considers the failures/requests a DoS attack.

---

**Important**
The system will ignore the configuration of this command unless the `dos-prevention` command has been enabled.

---

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF Security Configuration

`configure > context context_name > escf service service_name > proxy-cscf > security-parameters`

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-security-parameters)#
```

**Syntax Description**

```
threshold-rate rate
default threshold-rate
```

**default**
Sets/restores the default value assigned to the specified command.

**rate**
Default: 1
Specifies the rate per second that the system must receive authorization failures or bad registration requests to determine that it is under a DoS attack.

*rate* must be an integer from 1 to 1,000.

**Usage Guidelines**
Use this command to specify the threshold rate for authorization failures or bad registration requests. For example, if a malicious user sends bad registration requests at a rate of 5 per second and this parameter is set to 10, the system will not consider itself under a DoS attack.
Examples

The following command sets the threshold rate to 5 authorization failures or bad registration requests per second:

```
threshold-rate 5
```
CSCF Serving-CSCF Configuration Mode Commands

The Serving-CSCF Configuration Mode is used to set various commands supporting the role of the CSCF service as a Serving CSCF.

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

```
configure > context context_name > cscf service service_name > serving-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-cscf-service-serving-cscf)#
```

**Important**

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

- 3gpp, page 1613
- allow rfc3261-ua-interworking, page 1615
- as-call invite-request-uri update, page 1616
- authentication, page 1617
- bgcf-proxy, page 1620
- diversion-info, page 1622
- end, page 1623
- exit, page 1624
- forking, page 1625
- interrogating-cscf-role, page 1627
- lir-failure, page 1628
• local-call-features, page 1629
• network-id, page 1630
• npdb-client, page 1631
• policy, page 1633
• registration lifetime, page 1634
• reliable-prov-resp, page 1636
• server-name, page 1637
• sife, page 1638
• sip-header insert, page 1639
• sip-request, page 1640
• tas, page 1642
• tas-service, page 1643
• user-authorization, page 1644
3gpp

Enables/disables functionality related to 3GPP Release 8 support. This command is disabled by default.

Product

SCM (S-CSCF)

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

configure > context context_name > cscf service service_name > serving-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-serving-cscf)#

Syntax Description

3gpp Rel8 Cx { alias-indication | dynamic-password-change | ims-restoration | num-auth-vectors value
}
[ default | no ] 3gpp Rel8 Cx { alias-indication | dynamic-password-change | ims-restoration | num-auth-vectors }

default | no
Disables specified 3GPP Release 8 support feature.

Rel8 Cx
Specifies functionality related to 3GPP Release 8 support.

alias-indication
Enables alias indication functionality, a collaborative information exchange between the S-CSCF and HSS. Use this command to display alias information from the HSS.
If both the HSS and the S-CSCF support this feature, Alias Group IDs will be displayed in the output of the show subscribers cscf-only full command.

dynamic-password-change
Enables dynamic password change support on the S-CSCF service, as per 3GPP 33.203 release 8 version 8.8.0.
ims-restoration
Enables IMS restoration procedures on the S-CSCF service. Use this command to enable IMS REGISTER and INVITE restoration procedures defined in 3GPP TS 23.820.

num-auth-vectors value
Enables configurable value for SIP-Number-Auth-Items in MAR.
value must be an integer from 1 to 3. Default is 1.
SCSCF can retrieve multiple authentication vectors from HSS by setting SIP-Number-Auth-Items to an appropriate value. Previously, S-CSCF always set this value to "1". Using higher values helps to reduce MAR-MAA transactions.

Usage Guidelines
Use this command to configure the S-CSCF to support 3GPP Release 8 functionality.

Examples
The following command enables 3GPP Release 8 alias indication functionality on this service:
3gpp Rel8 Cx alias-indication
The following command disables 3GPP Release 8 dynamic password change support on this service:
no 3gpp Rel8 Cx dynamic-password-change
**allow rfc3261-ua-interworking**

Enables the function to allow IMS interworking with RFC3261 SIP User Agents.

**Product**  
SCM (S-CSCF)

**Privilege**  
Administrator

**Command Modes**  
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

```bash
configure > context context_name > csf service service_name > serving-cscf
```

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-cscf-service-serving-cscf)#
```

**Syntax Description**  
```bash
[ no ] allow rfc3261-ua-interworking
```

`no`

Disables the interworking capability.

**Usage Guidelines**  
Use this command to enable the S-CSCF to allow IMS interworking with RFC3261 SIP User Agents.
**as-call invite-request-uri update**

Enabling this command causes request-URIs in INVITE messages to be updated with the result of the translation before being passed to an Application Server (AS). This command is disabled by default.

**Product**

SCM (S-CSCF, SIP Proxy)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

```
configure > context context_name > cscf service service_name > serving-cscf
```

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-cscf-service-serving-cscf)#
```

**Syntax Description**

- `default | no` as-call invite-request-uri update

- `default` | `no`

  The translation result is ignored.

**Usage Guidelines**

Use this command to update the request-URI in INVITE messages with the result of the translation before passing it to an AS.
**authentication**

Configures the authentication method used by the S-CSCF service.

**Product**

SCM (S-CSCF, SIP Proxy)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

```bash
configure > context context_name > csf service service_name > serving-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-csf-service-serving-cscf)#
```

**Syntax Description**

```
authentication { aka-v1 value | allow-auth-rsp-failure re-register | allow-hss-failure re-register | allow-noauth [ invite | re-register | register ] | allow-noipauth [ invite | re-register | register ] | allow-skip-sar re-register | allow-unsecure | aor-auth | custom-md5 value | md5 value }
no authentication { aka-v1 | allow-auth-rsp-failure re-register | allow-hss-failure re-register | allow-noauth [ invite | re-register | register ] | allow-noipauth [ invite | re-register | register ] | allow-skip-sar re-register | allow-unsecure | aor-auth | custom-md5 | md5 }
```

**no**

Disables the specified authentication method for the S-CSCF service.

**aka-v1 value**

Specifies that AKA-v1 algorithm is used as the authentication type when accessing the CSCF service. `value` specifies a preference - the lower the value, the higher the preference. `value` must be an integer from 1 to 1000.

**Important**

In order to change a priority level, you must remove the original value and configure a new one.

**allow-auth-rsp-failure re-register**

Specifies that S-CSCF will not validate authorization received from UE for challenge re-register. If enabled, S-CSCF will send SAR without validating authentication; after receiving SAA, it will send 200 OK for register.
allow-hss-failurere-register
SpecifiesthatS-CSCFshouldsend200OKforre-registerincaseofHSSfailure.
WhenS-CSCFreceivesregister,itisendsMAR/SARtoHSSauthenticate theuserwhenauthenticationis
enabledandtogetthesubscriberprofile.WhenS-CSCFfailstoreceiveresponseMAA/SAAfromHSS,itis
sends500erroresponsetoUE.Whenallow-hss-failureisenabled,S-CSCFsendsa200OKforregisterinstead
of500response.

allow-noauth[invite|re-register|register]
Specifiesthataccess to the S-CSCF service is allowed if authentication fails.

invite: Specifiesthat access to the S-CSCF service is allowed if authentication fails on INVITERequests only.

re-register: Specifiesthat access to the S-CSCF service is allowed if authentication fails on RE-REGISTER
requestswhentherequestisintegrity-protectedonly.

registration: Specifiesthat access to the S-CSCF service is allowed if authentication fails on REGISTER
requests only.

allow-noipauth[invite|re-register|register]
Specifiesthataccess to the S-CSCF service is allowed if early IMS-based IP authentication fails.

invite: Specifiesthat access to the S-CSCF service is allowed if early IMS-based IP authentication fails on
INVITERequests only.

re-register: Specifiesthat access to the S-CSCF service is allowed if authentication fails on RE-REGISTER
requestswhentherequestisintegrity-protectedonly.

registration: Specifiesthat access to the S-CSCF service is allowed if early IMS-based IP authentication fails
onREGISTERrequests only.

allow-skip-sarre-register
SpecifiesthatS-CSCFshouldskipsar toHSSforre-register.
WhenS-CSCFreceivesre-register/challengeforre-register,itsendsSARtoHSSgetthesubscriberprofile.
ToavoidoverloadingHSS,enablingallow-skip-sarallowsS-CSCFtoskipSARforre-register.

allow-unsecure
Specifiesthatun-secureaccess is allowed to the S-CSCF service.

aor-auth
SpecifiesthatauthenticationisbasedontheAoRwhentheS-CSCFservice.

custom-md5value
SpecifiesthatcustomalgorithmHTTP-Digest-MD5isusedastheauthenticationtypeforaccessingtheS-CSCF
service.value specifierates thelowerthevalue, the higherthepreference.value mustbean integer
from1to1000.

Important
Inordertochangepriority level,youmustremovetheoriginalvalueandconfigureanewone.
md5 value

Specifies that the MD5 algorithm is used as the authentication type for accessing the S-CSCF service. Value specifies a preference - the lower the value, the higher the preference. Value must be an integer from 1 to 1000.

Important
In order to change a priority level, you must remove the original value and configure a new one.

Usage Guidelines
Use this command to configure the authentication method used by the S-CSCF service.

Important
The S-CSCF supports multiple authorization schemes, but this requires disabling all authorization configured in the S-CSCF service so that it will send "Unknown" in the Sip-Authorization-Scheme AVP. This allows the HSS to dictate authorization. The following commands disable all authorization configured in the S-CSCF service to allow HSS to control authorization:

- authentication allow-noipauth
- allow rfc3261-ua-interworking
- no authentication aka-v1
- no authentication md5

Examples
The following command configures the authentication method used by the S-CSCF service to MD5 with a preference of 3:

- authentication md5 3
**bgcf-proxy**

Enables SIP BGCF proxy for the service.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

```
configure > context context_name > scsf service service_name > serving-cscf
```

Entering the above command sequence results in the following prompt:

```
<context_name>@host_name(config-cscf-service-serving-cscf)#
```

**Syntax Description**

```
bgcf-proxy [port value | transport { tcp | udp } port value ] | default | no ] bgcf-proxy
```

- **default | no**
  Disables SIP BGCF proxy for the service.

- **port value**
  Configures port value for SIP BGCF proxy.
  *value* must be an integer from 1 to 65534.

- **transport**
  Enables the specific transport protocol for BGCF proxy.
  - **tcp**: Enables TCP transport protocol for BGCF proxy.
  - **udp**: Enables UDP transport protocol for BGCF proxy.

**Usage Guidelines**
Use this command to enable or disable SIP BGCF proxy for the service.

**Examples**
The following command enables a SIP BGCF proxy on port 561 for this service:

```
bgcf-proxy port 561
```
The following command disables SIP BGCF proxy for this service:
no bgcf-proxy
**diversion-info**

Enabling this command prompts the service to add a diversion header (draft-levy-sip-diversion-08) when the call is diverted to a different endpoint due to a call feature. By default, diversion-info is disabled.

**Product**

SCM (S-CSCF, SIP Proxy)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

`configure > context context_name > cscf service service_name > serving-cscf`

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-cscf-service-serving-cscf)#
```

**Syntax Description**

`[default | no] diversion-info`

- **default**
- **no**

The service will not add a diversion header.

**Usage Guidelines**

Use this command to enable the service to add a diversion header to call setup packets when calls are diverted due to the application of call features.
end

Exits the current 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.
# forking

Controls the default-request forking-type in S-CSCF.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

```
configure > context context_name > cscf service service_name > serving-cscf
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-cscf-service-serving-cscf)#
```

**Syntax Description**

```
forking { parallel | serial }
| default | no | forking
```

- **default**
  Perform parallel forking of request.

- **no**
  Do not perform any forking of request.

- **parallel | serial**
  Defines the fork type for request forking.
  - **parallel**: Perform parallel forking of request.
  - **serial**: Perform serial forking of request.

**Usage Guidelines**
Use this command to control the default-request forking-type in S-CSCF. This configuration will be effective in the absence of "Request-Disposition" header in the message.

**Examples**
The following command enables serial forking of request:

```
forking serial
```
The following command disables any forking of request:

no forking
interrogating-cscf-role

Enables the function to also perform as an Interrogating-CSCF.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

```
configure > context context_name > cscf service service_name > serving-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-serving-cscf)#
```

**Syntax Description**

```
[no ]interrogating-cscf-role
```

**no**

Disables the Interrogating-CSCF role in this function.

**Usage Guidelines**

Use this command to enable the S-CSCF to also perform as an Interrogating-CSCF.
**lir-failure**

This command allows you to define routes towards the target server for LIR failure case.

**Product**

SCM (S-CSCF)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

```plaintext
configure > context context_name > scf service service_name > serving-cscf
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-cscf-service-serving-cscf)#
```

**Syntax Description**

- `lir-failure route-list route_list_name`
- `no lir-failure route-list`

**Usage Guidelines**

Use this command to route register messages based on the route table if LIR-LIA fails during HSS interaction.
**local-call-features**

Enables/disables local call features. This command is disabled by default.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

```configure > context context_name > cs cf service service_name > serving-cscf```

Entering the above command sequence results in the following prompt:

```
{context_name} host_name(config-cscf-service-serving-cscf)#
```

**Syntax Description**
`| default | no | local-call-features`

**Usage Guidelines**
Use this command to enable local call features.
network-id

Configures the Network Identifier.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

`configure > context context_name > cscf service service_name > serving-cscf`

Entering the above command sequence results in the following prompt:

`{context_name}@host_name(config-cscf-service-serving-cscf)#`

**Syntax Description**

- `network-id id`
- `no network-id`

  **no**
  Removes the configured Network Identifier of the entity.

  **id**
  The Network Identifier of the entity.
  
  - `id` must be from 1 to 79 alpha and/or numeric characters in length.

**Usage Guidelines**

The Network Identifier is used to compare with the P-Visited-Network-ID header received from P-CSCF to decide home or roaming subscriber at S-CSCF service.

**Examples**

Sets the Network Identifier to `pcscf01.company.com`:

```
network-id pcscf01.company.com
```
**npdb-client**

Creates an NPDB (Number Portability Data Base) client under CSCF and enters the CSCF NPDB Client Configuration Mode.

**Product**

SCM (S-CSCF)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

`configure > context context_name > cscf service service_name > serving-cscf`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-cscf-service-serving-cscf)#`

**Syntax Description**

npdb-client client_name [-noconfirm ]

no npdb-client

no

Deletes NPDB client under CSCF.

**client_name**

Specifies the name of the NPDB client.

`client_name` must be from 1 to 79 alpha and/or numeric characters.

**-noconfirm**

Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage Guidelines**

Use this command to enable the NPDB client feature and enter the NPDB Client Configuration Mode. Entering this command results in the following prompt:

`[context_name]host_name(config-npdb-client)#`

NPDB Client Configuration Mode commands are defined in the **CSCF NPDB Client Configuration Mode Commands** chapter in this guide.
Examples

The following command creates an NPDB client named `npdb1` and enters NPDB Client Configuration Mode:

```
npdb-client npdb1
```
policy

Configures the policy for Served User Routing in this S-CSCF service.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

`configure > context context_name > cscf service service_name > serving-cscf`

Entering the above command sequence results in the following prompt:

`{context_name}host_name(config-cscf-service-serving-cscf)#`

**Syntax Description**

| default | no | policy allow p-served-user-routing |

- **default** | no
Disables Served User Routing functionality for this S-CSCF.

- **allow p-served-user-routing**
Enables Served User Routing functionality for this S-CSCF.

**Usage Guidelines**
Use this command to enable/disable the policy for Served User Routing.

**Examples**
The following command enables Served User Routing on this service:

`policy allow p-served-user-routing`

The following command disables Served User Routing on this service:

`no policy allow p-served-user-routing`
registration lifetime

Configures a registration lifetime for all subscribers to the service.

**Product**  
SCM (S-CSCF, SIP Proxy)

**Privilege**  
Administrator

**Command Modes**  
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

```
configure > context context_name > csf service service_name > serving-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-serving-cscf)#
```

**Syntax Description**

```
registration lifetime { default sec | implicit sec | max sec | min sec }
```

**default registration lifetime**

- **default**

  Returns the command to the default settings.

  ```
  default sec | implicit sec | max sec | min sec
  ```

  **default sec | implicit sec | max sec | min sec**

  **default sec**: Specifies the default amount of time that a registration can exist on the system.

  - **sec** must be an integer from 60 to **max sec** -1.
  - Default: 3600

  **Important**

  - **default sec** must be < or = to **max sec** and > or = to **min sec**.

  **implicit sec**: Specifies the implicit amount of time that a registration can exist on the system. **sec** must be an integer from 60 to 1209600.

  - Default: 0

  **max sec**: Specifies the maximum amount of time that a registration can exist on the system.

  - **sec** must be an integer from 60 to 1209600.
  - Default: 86400
**Important**  
\( \text{max sec must be} \geq \text{or} = \text{to min sec}. \)

**min sec**: Specifies the minimum amount of time that a registration can exist on the system.  
\( \text{sec must be an integer from} 60 \text{ to} \text{max sec} - 1. \)

Default: 60

**Important**  
\( \text{min sec must be} \leq \text{or} = \text{to max sec}. \)

---

**Usage Guidelines**

Use this command to control the amount of time registrations are allowed to exist on this service.  
The system responds to registrations in the following manner:

If implicit-timer is configured (>0), and if UE expires time < min expires time, respond with 200 OK with Expires-header set to configured implicit-expire time.

If implicit timer is not configured (=0), the service will respond with a 423 Interval Too Small message.

Using default values:

- If a registration with an expiration value lower than the service's minimum (60) is received, the service will respond with a 423 Interval Too Small message.
- If a registration with an expiration value higher than the service's maximum (2147483646) is received, the service will automatically reduce the expiration value to the default value.
- If a registration is received missing the "Expires" value, or the value is malformed, the service will automatically respond with 3761 in the 200 OK message.

**Examples**

The following command configures the maximum registration lifetime to 43200 (12 hours):

```
registration lifetime max 43200
```
reliable-prov-resp

Enables/disables the reliability of provisional responses feature.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

configure > context context_name > csf service service_name > serving-cscf

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-cscf-service-serving-cscf)#

Syntax Description
reliable-prov-resp { mandatory | optional }
no reliable-prov-resp

no
Disables the reliability of provisional responses feature.

mandatory | optional
mandatory: Both inbound and outbound will request reliability.
optional (default): Reliability is imposed by inbound side. Only if inbound call requests reliability will outbound also request reliability.

Usage Guidelines
Use this command to enable/disable the reliability of provisional responses feature.

Examples
The following command sets the reliability of provisional responses feature to mandatory:
reliable-prov-resp mandatory
server-name

Enables/disables filling the server name AVP in MAR and SAR for Cx interface with configured server name. This command is disabled by default.

Important

The server-name command has been moved to CSCF Service Configuration Mode in StarOS release 14.0 and later.

Product

SCM (S-CSCF)

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

configure > context context_name > csf service service_name > serving-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-serving-cscf)#

Syntax Description

server-name server_name
no server-name

no

S-CSCF uses configured cscf-hostname or bind IP address to fill the server name AVP in MAR and SAR for Cx interface. This is the default CSCF behavior.

server_name

Configures the name that will be used to fill the server name AVP in MAR and SAR for Cx interface. name must be from 1 to 63 alpha and/or numeric characters.

Usage Guidelines

Use this command to enable/disable filling the server name AVP in MAR and SAR for Cx interface with configured server name.

Examples

The following command configures the CSCF server name as stp-c-scscf1.cisco.co.kr:

server-name stp-c-scscf1.cisco.co.kr
**sifc**

Enables Shared Initial Filter Criteria (SiFC) functionality. This command is disabled by default.

**Product**

SCM (S-CSCF, SIP Proxy)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

```
configure > context context_name > csf service service_name > serving-cscf
```

Entering the above command sequence results in the following prompt:

```
(context_name|host_name(config-cscf-service-serving-cscf)#
```

**Syntax Description**

```
| default | no | sifc
```

**Usage Guidelines**

Use this command to configure the S-CSCF to share iFC functionality.

---

48 SiFC IDs are supported per subscriber.

If both the HSS and the S-CSCF support this feature, subsets of iFC may be shared by several service profiles. The HSS downloads the unique identifiers of the shared iFC sets to the S-CSCF. The S-CSCF uses a locally administered database to map the downloaded identifiers onto the shared iFC sets.

If the S-CSCF does not support this feature, the HSS will not download identifiers of shared iFC sets.

---

When using this feature option, the network operator is responsible for keeping the local databases in the S-CSCFs and HSSs consistent.
sip-header insert

Enable SIP header insertion for the S-CSCF service. SIP header insertion is disabled by default.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Command Modes**
Exec
Global Configuration
Context Configuration
CSCF Service Configuration
Serving-CSCF Configuration

configure
context context_name
cscf service service_name
serving-cscf

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-serving-cscf)>
```

**Syntax Description**

```
[no] sip-header insert { p-cust1-prid-info | p-user-database }
```

**no**
Disables specific SIP header insertion for the S-CSCF service.

**p-cust1-prid-info**
Inserts a custom header, P-LGUPlus-PRID-Info, which contains the private user id of the user sending the REGISTER request, to be added in the REGISTER message toward AS during third party registration.

**p-user-database**
Inserts PUD header in SIP (REGISTER) message and Invite from I-CSCF to S-CSCF.

**Usage Guidelines**

Enabling this command allows header insertion in SIP (REGISTER) message.

**Examples**
The following command disables insertion of custom header, P-LGUPlus-PRID-Info, in SIP (REGISTER) message:

```
no sip-header insert p-cust1-prid-info 5
```

The following command enables insertion of PUD header in SIP (REGISTER) message and Invite from I-CSCF to S-CSCF:

```
sip-header insert p-user-database 5
```
sip-request

Configures SIP Request-related configuration in this S-CSCF service.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration  
configure > context context_name > csf service service_name > serving-cscf

Entering the above command sequence results in the following prompt:

(context_name|host_name)(config-cscf-service-serving-cscf)#

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip-request re-route { max-attempts attempts</td>
<td>response-code code }</td>
</tr>
<tr>
<td>default sip-request re-route max-attempts</td>
<td></td>
</tr>
<tr>
<td>no sip-request re-route response-code code</td>
<td></td>
</tr>
</tbody>
</table>

**default**

Specifies a maximum number of two re-route attempts that a S-CSCF should allow for a given call before passing the negative response upstream.

**no**

Disables the specified Response code.

**re-route**

Specify SIP Request re-route related configuration.

**max-attempts attempts**

Specifies the maximum number of re-route attempts that a S-CSCF should allow for a given call before passing the negative response upstream.

*attempts* must be an integer from 1 to 10.

Default: 2

**response-code code**

Specifies the list of Response codes that will be considered as re-routable responses to a call attempt.
code must be a three-digit integer from 400 to 699.

### Important
You may configure a maximum of five response code values per S-CSCF service.

### Usage Guidelines
Use this command to configure:

- list of Response codes that will be considered as re-routable responses to a call attempt.
- the maximum number of re-route attempts that a S-CSCF should allow for a given call before passing the negative response upstream.

### Examples
The following command configures the maximum number of re-route attempts to 5:

```
sip-request re-route max-attempts 5
```
tas

Configures the S-CSCF to perform Telephony Application Server (TAS) functions.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

```
configure > context context_name > csf service service_name > serving-cscf
```

Entering the above command sequence results in the following prompt:

```
<context_name>@host_name(config-cscf-service-serving-cscf)#
```

**Syntax Description**
```
| default | no | tas
```

**Usage Guidelines**
Use this command to configure the S-CSCF to perform TAS functions.

<table>
<thead>
<tr>
<th>default</th>
<th>no</th>
</tr>
</thead>
</table>

Disables the TAS feature for this S-CSCF.
**tas-service**

Identifies the name of the service configured on the system performing Telephony Application Server (TAS) functions.

**Product**

SCM (S-CSCF, SIP Proxy)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

```
configure > context context_name > cscf service service_name > serving-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-serving-cscf)#
```

**Syntax Description**

- `tas-service name`
- `no tas-service`

- `no`

Removes the TAS name from the S-CSCF configuration.

- `name`

Specifies the name of the service configured on the system performing TAS functions.

`name` must be from 1 to 63 alpha and/or numeric characters and be an existing service.

**Usage Guidelines**

Use this command to identify the name of the service configured on the system performing TAS functions.

**Examples**

The following command identifies the TAS service name as `scsf3`:

```
tas-service scsf3
```
**user-authorization**

Enables sending user-authorization to HSS. User-authorization is disabled by default.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

```
configure > context context_name > csf service service_name > serving-cscf
```

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-cscf-service-serving-cscf)#
```

**Syntax Description**

```
| default | no | user-authorization
```

```
default | no
```
Disables sending user-authorization to HSS.

**Usage Guidelines**
If this command is enabled, and I-CSCF role is enabled in S-CSCF, I-CSCF will send UAR/UAA diameter message to HSS.
CSCF Session Template Configuration Mode Commands

The CSCF Session Template Configuration Mode is used to classify users and/or domains (AoRs) within the system.

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Session Template Configuration

`configure > context context_name > cscf session-template { default | name template_name }`

Entering the above command sequence results in the following prompt:

`{context_name}host_name(config-cscf-session-template)#`

---

Important

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

- end, page 1646
- exit, page 1647
- inbound-cscf-acl, page 1648
- outbound-cscf-acl, page 1649
- policy-profile, page 1650
- route-list, page 1651
- translation-list, page 1652
- urn-service-list, page 1653
end

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

end

**Usage Guidelines**

Use this command to return to the Exec mode.
exit

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

Product
All

Privilege
Security Administrator, Administrator

Syntax Description
exit

Usage Guidelines
Use this command to return to the parent configuration mode.
**inbound-cscf-acl**

Configures the ACL to use for inbound sessions using this template.

**Product**

SCM

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Session Template Configuration

```plaintext
configure > context context_name > cscf session-template { default | name template_name }
```

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-cscf-session-template)#
```

**Syntax Description**

```plaintext
inbound-cscf-acl { default | name acl_name }

no inbound-cscf-acl name acl_name
```

- **default | name acl_name**
  
  default: Specifies that the default ACL should be used for inbound sessions using this template.
  
  name acl_name: Specifies an existing ACL to use for inbound sessions using this template. acl_name must be the name of an existing ACL.

- **no inbound-cscf-acl name acl_name**
  
  Removes the ACL from this template.

**Usage Guidelines**

Use this command to identify an ACL to use on inbound sessions using this template.

**Examples**

The following command sets the inbound ACL for this template to an ACL named acl_in22:

```plaintext
inbound-cscf-acl name acl_in22
```
outbound-cscf-acl

Configures the ACL to use for outbound sessions using this template.

**Product**
SCM

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Session Template Configuration

```
configure > context context_name > cscf session-template { default | name template_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-session-template)#
```

**Syntax Description**

```
outbound-cscf-acl { default | name acl_name }

no outbound-cscf-acl name acl_name
```

- **default** | **name acl_name**
  - default: Specifies that the default ACL should be used for outbound sessions using this template.
  - name acl_name: Specifies an existing ACL to use for outbound sessions using this template. acl_name must be the name of an existing ACL.

- **no outbound-cscf-acl name acl_name**
  - Removes the ACL from this template.

**Usage Guidelines**
Use this command to identify an ACL to use on outbound sessions using this template.

**Examples**
The following command sets the outbound ACL for this template to an ACL named acl_out22:

```
outbound-cscf-acl name acl_out22
```
policy-profile

Configures an AoR policy group to be used for sessions using this template.

**Product**
SCM

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Session Template Configuration
`configure > context context_name > cscf session-template { default | name template_name }`

Entering the above command sequence results in the following prompt:
`{context_name}host_name(config-cscf-session-template)#`

**Syntax Description**

```
policy-profile { default | name profile_name }
no policy-profile name profile_name

default | name profile_name
```

default: Specifies that the default policy group will be used for sessions using this template.
name `profile_name`: Specifies an existing policy group. `profile_name` must be an existing CSCF policy group.

```
no policy-profile name profile_name
```

Removes the policy group from the template.

**Usage Guidelines**
Use this command to specify a policy group for the template.

**Examples**
The following command specifies that a policy group called `aor_grp1` will be used for sessions using this template:
`policy-profile name aor_grp1`
route-list

Configures a route group to be used for sessions using this template.

**Product**    SCM

**Privilege**  Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Session Template Configuration

configure > context context_name > cscf session-template { default | name template_name }

Entering the above command sequence results in the following prompt:

<context_name>host_name(config-cscf-session-template)#

**Syntax Description**

- **route-list { default | name group_name }
- no route-list name group_name**

- **default | name group_name**
  - default: Specifies that the default route group will be used for sessions using this template.
  - name group_name: Specifies an existing route group. group_name must be an existing peer server group.

- **no route-list name group_name**
  - Removes the route group from this template.

**Usage Guidelines**

Use this command to specify a route group for the template.

**Examples**

The following command specifies an accounting server group called route_grp2 that will be used for sessions using this template:

```
route-list name route_grp2
```
**translation-list**

Configures a translation list to be used for sessions using this template.

**Product**  
SCM

**Privilege**  
Administrator

**Command Modes**  
Exec > Global Configuration > Context Configuration > CSCF Session Template Configuration  
```
configure > context context_name > cscf session-template { default | name template_name }
```

Entering the above command sequence results in the following prompt:
```
{context_name}host_name(config-cscf-session-template)#
```

**Syntax Description**
```
translation-list { default | name list_name }
no translation-list name list_name
```

- **default | name list_name**
  - default: Specifies that the default translation list will be used for sessions using this template.
  - name list_name: Specifies an existing translation list. list_name must be an existing translation list.

- **no translation-list name list_name**
  Removes the translation list from this template.

**Usage Guidelines**  
Use this command to specify a translation list for the template.

**Examples**  
The following command specifies a translation list called `trans_list6`:
```
translation-list name trans_list6
```
urn-service-list

Configures an URN service list to be used for sessions using this template.

Product

SCM

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Session Template Configuration

cfg configure context context_name cscf session-template { default | name template_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-session-template)#

Syntax Description

urn-service-list { default | name list_name }

no urn-service-list name list_name

default | name list_name

default: Specifies that the default URN service list will be used for sessions using this template.

name list_name: Specifies an existing URN service list name. list_name must be from 1 to 79 alpha and/or numeric characters and be an existing URN service list.

no urn-service-list name list_name

Removes the service list from this template.

Usage Guidelines

Use this command to specify a URN service list for this template. URN service lists are configured in the URN Service List Configuration Mode.

Examples

The following command specifies that a URN service list named urn_list5 will be used for sessions using this template:

urn-service-list name urn_list5
urn-service-list
CSCF Signalling Compression Configuration Mode Commands

The CSCF Signalling Compression Configuration Mode is used to set memory allocation parameters in support of SIP signalling compression. More information regarding signalling compression refer to the IETF RFC 3320 "Signaling Compression (SigComp)".

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration > Signaling Compression Configuration

`configure > context context_name > cscf service service_name > rfc3261-proxy > sigcomp`

-or-

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > Signaling Compression Configuration

`configure > context context_name > cscf service service_name > proxy-cscf > sigcomp`

Entering the above command sequences results in the following prompt:

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

**Important**

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

- compression-mode, page 1656
- decompression-memory-size, page 1658
- end, page 1659
- exit, page 1660
- state-memory-size, page 1661
**compression-mode**

Configures the dynamic compression mode to be used while sending a SigComp message. Simple dynamic mode is the default.

**Product**  
SCM

**Privilege**  
Administrator

**Command Modes**  
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration > Signaling Compression Configuration

```
configure > context context_name > csf service service_name > rfc3261-proxy > sigcomp
```

- or -

```
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > Signaling Compression Configuration
configure > context context_name > csf service service_name > proxy-cscf > sigcomp
```

Entering the above command sequences results in the following prompt:

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

**Syntax Description**

```
compression-mode { multiple-dynamic | simple-dynamic | static | update-dynamic }
default compression-mode
```

**Compression Mode Options**

**multiple-dynamic**: A maximum of four dynamic states will be created per compartment. The dynamic states are updated for each message by deleting the oldest dynamic state and creating the new one. The dynamic states will be updated in FIFO (First In, First Out) order.

**simple-dynamic**: Only one dynamic state will be created per compartment. The same state will be used for compression.

**static**: No dynamic states will be created. Only static dictionary will be used for compression.

**update-dynamic**: Only one dynamic state will be created per compartment, but the dynamic state will be updated for every new message.

**default compression-mode**

Returns the dynamic compression mode to simple dynamic.
Usage Guidelines

Use this command to configure the dynamic compression mode to be used.

Examples

The following command sets the compression mode to multiple dynamic:

```
compression-mode multiple-dynamic
```

The following command completely disables the creation of dynamic states for compression:

```
compression-mode static
```
decompression-memory-size

Sets the amount of memory available for decompressing one SigComp message. A portion of the allocated memory is used to buffer the message before it is decompressed. The memory is allocated for each SigComp message and is reclaimed once decompression is completed.

**Product**
SCM

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration > Signaling Compression Configuration

`configure > context context_name > csf service service_name > rfc3261-proxy > sigcomp`

~or~

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > Signaling Compression Configuration

`configure > context context_name > csf service service_name > proxy-cscf > sigcomp`

Entering the above command sequences results in the following prompt:

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

**Syntax Description**
`decompression-memory-size {128k | 16k | 32k | 64k | 8k}

default decompression-memory-size`

- `128k | 16k | 32k | 64k | 8k`
  - Default: 8k
  - Specifies the amount of memory (in kilobytes) to allocate for decompressing one SigComp message.

- `default`
  - Returns the command to the default settings.

**Usage Guidelines**
Use this command to set the memory size used to decompress a single SigComp message.

**Examples**
The following command sets the memory size for decompressing SigComp messages to 16k:

`decompression-memory-size 16k`
**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.
**state-memory-size**

Sets the memory allocated to a compartment for the creation of state. Compartments are application-specific groupings of messages that relate to a peer endpoint. The system allocates memory per compartment. The memory is reclaimed when the system determines that the compartment is no longer required.

**Product**

SCM

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration > Signaling Compression Configuration

`configure > context context_name > csf service service_name > rfc3261-proxy > sigcomp`

-or-

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > Signaling Compression Configuration

`configure > context context_name > csf service service_name > proxy-cscf > sigcomp`

Entering the above command sequences results in the following prompt:

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

**Syntax Description**

`state-memory-size { 4k | 8k }`

`default state-memory-size`

- `4k | 8k`
  - Default: `4k`
  - Specifies the amount of memory to allocate to a compartment for the creation of state.

- `default`
  - Returns the command to the default settings.

**Usage Guidelines**

Use this command to specify a memory size allocated to message groupings for the creation of state.

**Examples**

The following command sets the state memory size to `8k`:

`state-memory-size 8k`
CSCF SIP Proxy Configuration Mode Commands

The SIP Proxy Configuration Mode is used to set various commands supporting the role of the CSCF service as a RFC3261-compliant SIP proxy server.

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration

```plaintext
configure > context context_name > csf service service_name > rfc3261-proxy
```

Entering the above command sequences results in the following prompt:

```
{context_name}@host_name(config-csf-service-rfc3261-proxy)#
```

**Important**

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

- as-call, page 1664
- authentication, page 1665
- diversion-info, page 1667
- emergency, page 1668
- end, page 1670
- exit, page 1671
- registration, page 1672
- reliable-prov-resp, page 1674
- sifc, page 1675
- sigcomp, page 1676
- tas, page 1677
- tas-service, page 1678
as-call

Enabling this command causes request-URIs in INVITE messages to be updated with the result of the translation before being passed to an Application Server. This command is disabled by default.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration
`configure > context context_name > cscf service service_name > rfc3261-proxy`

Entering the above command sequences results in the following prompt:
`{context_name}host_name(config-cscf-service-rfc3261-proxy)#`

**Syntax Description**
`| default | no | as-call invite-request-uri update`

- **default | no**
The translation result is ignored.

**Usage Guidelines**
Use this command to update the request-URI in INVITE messages with the result of the translation before passing it to an AS.
**authentication**

Configures the authentication method used by the CSCF service.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration

`configure > context context_name > csfc service service_name > rfc3261-proxy`

Entering the above command sequences results in the following prompt:

`[context_name] host_name(config-cscf-service-rfc3261-proxy)#`

**Syntax Description**

`authentication { aka-v1 value | allow-noauth | invite | re-register | register | | allow-noipauth | invite | re-register | register | | allow-unsecure | aor-auth | md5 value }`

no authentication { aka-v1 | allow-noauth | invite | re-register | register | | allow-noipauth | invite | re-register | register | | allow-unsecure | aor-auth | md5 }

no

Disables the specified authentication method for the CSCF service.

**aka-v1 value**

Specifies that AKA-v1 algorithm is used as the authentication type when accessing the CSCF service.

`value` specifies a preference - the lower the value, the higher the preference. `value` must be an integer from 1 to 1000.

**Important**

In order to change a priority level, you must remove the original value and configure a new one.

`allow-noauth | invite | re-register | register`

Specifies that access to the CSCF service is allowed if authentication fails.

`invite`: Specifies that access to the CSCF service is allowed if authentication fails on INVITE requests only.

`re-register`: Specifies that access to the CSCF service is allowed if authentication fails on RE-REGISTER requests when the request is integrity-protected only.
**registration**: Specifies that access to the CSCF service is allowed if authentication fails on REGISTER requests only.

**allow-noipauth [ invite | re-register | register ]**

Specifies that access to the CSCF service is allowed if early IMS-based IP authentication fails.

**invite**: Specifies that access to the CSCF service is allowed if early IMS-based IP authentication fails on INVITE requests only.

**re-register**: Specifies that access to the CSCF service is allowed if authentication fails on RE-REGISTER requests when the request is integrity-protected only.

**registration**: Specifies that access to the CSCF service is allowed if early IMS-based IP authentication fails on REGISTER requests only.

**allow-unsecure**

Specifies that un-secure access is allowed to the CSCF service.

**aor-auth**

Specifies that authentication is based on the AoR when accessing the CSCF service.

**md5 value**

Specifies that the MD5 algorithm is used as the authentication type for accessing the CSCF service. *value* specifies a preference - the lower the value, the higher the preference. *value* must be an integer from 1 to 1000.

---

**Important**

In order to change a priority level, you must remove the original value and configure a new one.

---

**Usage Guidelines**

Use this command to configure the authentication method used by the CSCF service.

---

**Important**

The S-CSCF supports multiple authorization schemes, but this requires disabling all authorization configured in the S-CSCF service so that it will send "Unknown" in the Sip-Authorization-Scheme AVP. This allows the HSS to dictate authorization. The following commands disable all authorization configured in the S-CSCF service to allow HSS to control authorization:

```
authentication allow-noipauth
allow rfc3261-ua-interworking
no authentication aka-v1
no authentication md5
```

---

**Examples**

The following command configures the authentication method used by the CSCF service to MD5 with a preference of 3:

```
authentication md5 3
```
**diversion-info**

Enabling this command prompts the service to add a diversion header (draft-levy-sip-diversion-08) when the call is diverted to a different endpoint due to a call feature. By default diversion-info is disabled.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration

configure > context context_name > csf service service_name > rfc3261-proxy

Entering the above command sequences results in the following prompt:

{context_name}host_name(config-cscf-service-rfc3261-proxy)#

**Syntax Description**

| default | no | diversion-info |

  default | no

The service will not add a diversion header.

**Usage Guidelines**
Use this command to enable the service to add a diversion header to call setup packets when calls are diverted due to the application of call features.
emergency

Configures the function to allow or disallow the emergency-session or emergency-registration of a particular type.

Product

SCM (P-CSCF, A-BG, SIP Proxy)

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration
configure > context context_name > cscf service service_name > rfc3261-proxy

Entering the above command sequences results in the following prompt:

{context_name}@host_name(config-cscf-service-rfc3261-proxy) #

Syntax Description

| default | no | emergency { registration | visited-ue } | session | 3gpp-ims-xml-body | anonymous | non-emergency-registered | sdp-cs-media | visited-ue |


default

Specifies that the emergency-session or emergency-registration of a particular type can be allowed.

no

Disallows the emergency-session or emergency-registration of a particular type.

registration | visited-ue

Allow emergency-registration. By default, it's allowed.

visited-ue: Allow emergency-registration from a visited UE. By default, it's allowed.

session | 3gpp-ims-xml-body | anonymous | non-emergency-registered | sdp-cs-media | visited-ue

Specifies the type of emergency-session to be allowed or disallowed. By default, all are allowed.

3gpp-ims-xml-body: Allow 3GPP IM CN XML body to be added in 380 response messages.

anonymous: Allow anonymous subscribers (unregistered UEs) to initiate emergency sessions.

non-emergency-registered: Allow non-emergency registered subscribers to initiate emergency sessions.

sdp-cs-media: Allow emergency calls with SDP CS Media.

visited-ue: Allow emergency calls from visited UE.
Usage Guidelines

Use this command to configure the function to allow or disallow the emergency-session or emergency-registration of a particular type.

Examples

The following command configures the function to allow non-emergency registered subscribers to initiate emergency sessions:

emergency session non-emergency-registered
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.
registration

Configures a registration lifetime for all subscribers to the service.

**Product**

SCM (S-CSCF, SIP Proxy)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration

```bash
configure > context context_name > cscf service service_name > rfc3261-proxy
```

Entering the above command sequences results in the following prompt:

```bash
(context_name)host_name(config-cscf-service-rfc3261-proxy)#
```

**Syntax Description**

```
registration lifetime | default sec | max sec | min sec |
default registration lifetime
```

**default**

Returns the command to the default settings.

```
default sec | max sec | min sec
```

**default sec**

 Specifies the default amount of time that a registration can exist on the system. `sec` must be an integer from 60 to `max sec` -1. Default is 3600. `default sec` must be `< or = to max sec` and `> or = to min sec`.

**max sec**

Specifies the maximum amount of time that a registration can exist on the system. `sec` must be an integer from 60 to 1209600. Default is 86400. `max sec` must be `> or = to min sec`.

**min sec**

Specifies the minimum amount of time that a registration can exist on the system. `sec` must be an integer from 60 to `max sec` -1. Default is 60. `min sec` must be `< or = to max sec`.

**Usage Guidelines**

Use this command to control the amount of time registrations are allowed to exist on this service.

The system responds to registrations in the following manner:

Using default values:

- If a registration with an expiration value lower than the service's minimum (60) is received, the service will respond with a 423 Interval Too Small message.
- If a registration with an expiration value higher than the service's maximum (2147483646) is received, the service will automatically reduce the expiration value to the default value.
• If a registration is received missing the "Expires" value, or the value is malformed, the service will automatically respond with 3761 in the 200OK message.

**Examples**

The following command configures the maximum registration lifetime to 43200 (12 hours):

```
registration lifetime max 43200
```
reliable-prov-resp

Enables/disables the reliability of provisional responses feature.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration

cfg>context context_name>csf service service_name>rfc3261-proxy

Entering the above command sequences results in the following prompt:

{context_name}host_name(config-cscf-service-rfc3261-proxy)#

Syntax Description
reliable-prov-resp { mandatory | optional }
no reliable-prov-resp

no
Disables the reliability of provisional responses feature.

mandatory | optional

mandatory: Both inbound and outbound will request reliability.

optional (default): Reliability is imposed by inbound side. Only if inbound call requests reliability will outbound also request reliability.

Usage Guidelines
Use this command to enable/disable the reliability of provisional responses feature.

Examples
The following command sets the reliability of provisional responses feature to mandatory:

reliable-prov-resp mandatory

The following command disables the reliability of provisional responses feature:

no reliable-prov-resp
**sifc**

Enables Shared Initial Filter Criteria (SiFC) functionality. This command is disabled by default.

**Product**

SCM (S-CSCF, SIP Proxy)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration

`configure > context context_name > csf service service_name > rfc3261-proxy`

Entering the above command sequences results in the following prompt:

```
[context_name] host_name (config-csfc-service-rfc3261-proxy) #
```

**Syntax Description**

```
[ default | no ] sifc
```

- **default**
  - Disables shared iFC functionality for this SIP Proxy.
- **no**

**Usage Guidelines**

Use this command to configure the SIP Proxy to share iFC functionality.

If both the HSS and the SIP Proxy support this feature, subsets of iFC may be shared by several service profiles. The HSS downloads the unique identifiers of the shared iFC sets to the SIP Proxy. The SIP Proxy uses a locally administered database to map the downloaded identifiers onto the shared iFC sets.

If the SIP Proxy does not support this feature, the HSS will not download identifiers of shared iFC sets.

**Important**

When using this feature option, the network operator is responsible for keeping the local databases in the S-CSCFs and HSSs consistent.
sigcomp

Enables signaling compression for the SIP Proxy service and enters the Signaling Compression Configuration Mode.

**Product**

SCM (S-CSCF, SIP Proxy)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration

configure > context *context_name* > cscf service *service_name* > rfc3261-proxy

Entering the above command sequences results in the following prompt:

{context_name}host_name(config-cscf-service-rfc3261-proxy)#

**Syntax Description**

| no | sigcomp |

no

Disables signaling compression for the CSCF service.

**Usage Guidelines**

Use this command to enable signaling compression for the SIP Proxy service and enter the CSCF Signaling Compression Configuration Mode.

Entering this command results in the following prompt:

{context_name}hostname(config-sigcomp)#

Signaling Compression Configuration Mode commands are defined in the *CSCF Signaling Compression Configuration Mode Commands* chapter in this guide.
**tas**

Configures the SIP Proxy to perform Telephony Application Server (TAS) functions.

**Product**

SCM (S-CSCF, SIP Proxy)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration

configure > context context_name > cs cf service service_name > rfc3261-proxy

Entering the above command sequences results in the following prompt:

<context_name>host_name(config-cscf-service-rfc3261-proxy)#

**Syntax Description**

[ default | no ] tas

default | no

Disables the TAS feature for this SIP Proxy.

**Usage Guidelines**

Use this command to configure the SIP Proxy to perform TAS functions.
tas-service

Identifies the name of the service configured on the system performing Telephony Application Server (TAS) functions.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration

`configure > context context_name > cscf service service_name > rfc3261-proxy`

Entering the above command sequences results in the following prompt:

```
[context_name]host_name(config-cscf-service-rfc3261-proxy)#
```

**Syntax Description**

```
tas-service name
| default | no | tas-service
```

default | no

Removes the TAS name from the SIP Proxy configuration.

```
name
```

Specifies the name of the service configured on the system performing TAS functions. *name* must be from 1 to 63 alpha and/or numeric characters and be an existing service.

**Usage Guidelines**
Use this command to identify the name of the service configured on the system performing TAS functions. The `ims-sh-service` commands are defined in the Context Configuration Mode Commands chapter in this guide.

**Examples**
The following command identifies the TAS service name as `scscf3`:

```
tas-service scscf3
```
CSCF Subdomain-route List Configuration Mode
Commands

The CSCF Subdomain-route List Configuration Mode is used to configure the subdomain-routes for the I-CSCF. These subdomain-routes are used to send messages over the Ma-interface (I-CSCF interface toward AS).

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Subdomain-routes List Configuration

configure > context context_name > cscf subdomain-routes

Entering the above command sequence results in the following prompt:

(context_name)host_name(config-cscf-subdomain-route)#

---

**Important**

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

- after, page 1680
- before, page 1681
- end, page 1682
- exit, page 1683
- route, page 1684
**after**

Places the subdomain-route at the bottom or end of the subdomain-routes list. Use this command in conjunction with the `route` command.

**Product**

SCM (I-CSCF)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Subdomain-routes List Configuration

`configure > context context_name > cscf subdomain-routes`

Entering the above command sequence results in the following prompt:

`{context_name}@host_name(config-cscf-subdomain-route)#`

**Syntax Description**

`after`

**Usage Guidelines**

Add this command before the `route` command to place the route at the end of the subdomain-routes list.
before

Places the subdomain-route at the beginning or top of the subdomain-routes list. Use this command in conjunction with the `route` command.

**Product**

SCM (I-CSCF)

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Subdomain-routes List Configuration

```
configure > context context_name > cscf subdomain-routes
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-cscf-subdomain-route)#
```

**Syntax Description**

`before`

**Usage Guidelines**

Add this command before the `route` command to place the route at the beginning of the subdomain-routes list.
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

default

Usage Guidelines

Use this command to return to the Exec mode.
exit

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

Product
All

Privilege
Security Administrator, Administrator

Syntax Description
exit

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

Creates a route entry to be used in the subdomain-routes list for the I-CSCF.

Product

SCM (I-CSCF)

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Subdomain-routes List Configuration
configure > context context_name > cscf subdomain-routes

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-cscf-subdomain-route)#

Syntax Description

| no | route peer-servers name | log | base-criteria destination aor aor |

no

Removes specified route entry.

peer-servers name

Specifies the name of a peer server group. 

name must be an existing peer server group from 1 to 79 alpha and/or numeric characters in length.

log

Enables logging for CSCF sessions meeting the criteria specified. The logs can be viewed by executing the 
logging filter active facility cscf command in the Exec mode.

base-criteria destination aor aor

Filters routes based on the destination AoR.

aor must be an existing AoR from 1 to 79 alpha and/or numeric characters in length.

Important

AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.
Usage Guidelines

Use this command to create and order routes in the subdomain-routes list for the I-CSCF. I-CSCF, upon receiving the terminating request, checks the subdomain-route list for matches. If a match is found, the routing will happen based on it. Otherwise, I-CSCF performs a User Location Query (Location-Information-Request) before proceeding.

Examples

The following command creates a route for the subdomain-routes list to peer server group ps5 with a destination AoR of $.@abc123.com:

```
route peer-servers ps5 base-criteria destination aor $.@abc123.com
```
CSCF Translation Configuration Mode Commands

The CSCF Translation Configuration Mode is used to configure session re-addressing within the system.

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Translation Configuration

```
configure > context context_name > csf translation name list_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-cscf-translation)#
```

**Important**

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

- after, page 1688
- before, page 1689
- end, page 1690
- exit, page 1691
- uri-readdress, page 1692
after

Places the CSCF translation entry at the bottom or end of the translation list. Use this command in conjunction with the `uri-readdress` command.

**Product**  
SCM

**Privilege**  
Administrator

**Command Modes**  
Exec > Global Configuration > Context Configuration > CSCF Translation Configuration

```
configure > context context_name > cscf translation name list_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-cscf-translation)#
```

**Syntax Description**  
`after`

**Usage Guidelines**  
Add this command before the `uri-readdress` command to place the entry at the end of the translation list.
**before**

Places the CSCF translation entry at the top or beginning of the translation list. Use this command in conjunction with the `uri-readdress` command.

**Product**

SCM

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > CSCF Translation Configuration

configure > context context_name > cscf translation name list_name

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-cscf-translation)#
```

**Syntax Description**

`before`

**Usage Guidelines**

Add this command before the `uri-readdress` command to place the entry at the beginning of the translation list.
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.
**uri-readdress**

Configures readdress criteria for URI translations.

**Product**
SCM

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > CSCF Translation Configuration

configure > context context_name > cscf translation name list_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-translation)#
```

**Syntax Description**

```
uri-readdress type trans_type [ log ] [ base-criteria criteria ] [ filter-criteria1 criteria ] [ filter-criteria2 criteria ]
```

```
no uri-readdress type trans_type [ base-criteria criteria ] [ filter-criteria1 criteria ] [ filter-criteria2 criteria ]
```

```
no
```

Remove the readdress configuration.

**type trans_type**

Specifies that the translation list (trans_type) entry is to be identified as one of the following:

- **blocking-cid**: Identifies the translation list entry type as "call ID blocking".
- **cancel-blocking-cid**: Identifies the translation list entry type as "cancel call ID blocking".
- **cancel-cid**: Identifies the translation list entry type as "cancel call ID display".
- **cancel-cw**: Identifies the translation list entry type as "cancel call-waiting".
- **cfbl-off**: Identifies the translation list entry type as "call forward busy line off".
- **cfbl-on**: Identifies the translation list entry type as "call forward busy line on".
- **cfna-off**: Identifies the translation list entry type as "call forward no answer off".
- **cfna-on**: Identifies the translation list entry type as "call forward no answer on".
- **cfu-off**: Identifies the translation list entry type as "call forward unconditional off".
- **cfu-on**: Identifies the translation list entry type as "call forward unconditional on".
• **cid**: Identifies the translation list entry type as "call ID display".
• **cw-off**: Identifies the translation list entry type as "call-waiting off".
• **cw-on**: Identifies the translation list entry type as "call-waiting on".
• **directory-assistance**: Identifies the translation list entry type as "directory assistance".
• **emergency**: Identifies the translation list entry type as "emergency".
• **international**: Identifies the translation list entry type as "international".
• **local**: Identifies the translation list entry type as "local".
• **long-distance**: Identifies the translation list entry type as "long-distance".
• **none**: Identifies the translation list entry type as "any".
• **operator-assistance**: Identifies the translation list entry type as "operator assistance".
• **premium-service**: Identifies the translation list entry type as "premium service".
• **service**: Identifies the translation list entry type as "special service".
• **tollfree**: Identifies the translation list entry type as "toll free".

**log**

Enables logging for CSCF sessions meeting the readdress criteria for URI translations.

**base-criteria criteria**

Specifies the base criteria that packets will be compared against. The following criteria is supported:

• **any**: Filters all CSCF sessions.
• **destination aor** aor: Filters sessions based on the destination AoR.
  
  **Important**
  AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

  
  aor must be an existing AoR from 1 to 79 characters in length.

• **plmn-id mcc mcc_code mnc mnc_code**: Filters sessions based on the mobile country and network codes.
  
  **Important**
  mcc_code must be a three-digit integer from 200 to 999.
  
  mnc_code must be either a two or three-digit integer from 00 to 999 or any (any MNC code).

• **source address** ip_address: Filters sessions based on source IP address.
  
  **Important**
  ip_address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

• **source aor** aor: Filters sessions based on the source AoR.
  
  **Important**
  aor must be an existing AoR from 1 to 79 characters in length.
filter-criteria1 criteria

Specifies the filter criteria that packets that have passed the base criteria will be compared against. The following criteria is supported:

- **any**: Filters all CSCF sessions.
- **destination aor aor**: Filters sessions based on the destination AoR.
  
  `aor` must be an existing AoR from 1 to 79 characters in length.

---

**Important**

AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

- **plmn-id mcc mcc_code mnc mnc_code**: Filters sessions based on the mobile country and network codes.
  
  `mcc_code` must be a three-digit integer from 200 to 999.
  
  `mnc_code` must be either a two or three-digit integer from 00 to 999 or **any** (any MNC code).

- **source address ip_address**: Filters sessions based on source IP address.
  
  `ip_address` must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

- **source aor aor**: Filters sessions based on the source AoR.
  
  `aor` must be an existing AoR from 1 to 79 characters in length.

filter-criteria2 criteria

Specifies the filter criteria that packets that have passed the base criteria and filter criteria1 will be compared against. The following criteria is supported:

- **any**: Filters all CSCF sessions.
- **destination aor aor**: Filters sessions based on the destination AoR.
  
  `aor` must be an existing AoR from 1 to 79 characters in length.

---

**Important**

AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

- **plmn-id mcc mcc_code mnc mnc_code**: Filters sessions based on the mobile country and network codes.
  
  `mcc_code` must be a three-digit integer from 200 to 999.
  
  `mnc_code` must be either a two or three-digit integer from 00 to 999 or **any** (any MNC code).

- **source address ip_address**: Filters sessions based on source IP address.
  
  `ip_address` must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

- **source aor aor**: Filters sessions based on the source AoR.
  
  `aor` must be an existing AoR from 1 to 79 characters in length.
**Usage Guidelines**

Use this command to readdress URIs based on specified criteria and enters the URI Readdress Configuration Mode. Readdressing can be used for:

- **Mobility**: When roaming in a visited domain.
- **Service Aliases**: Resolving well-known addresses via SIP-AS.
- **Number Translation**: Adding or deleting prefixes such as +1 to/from PSTN numbers.
- **Voice VPNs**: Using inter-office extensions to dial remote offices.

Entering this command results in the following prompt:

```
[context_name] hostname(config-uri-readdress)#
```

URI readdress commands are defined in the *CSCF URI Readdress Configuration Mode Commands* chapter of this reference.

**Examples**

The following command readdresses sessions to a domain named *service.com*, filters sessions with a base criteria of the source address *(1.2.3.4)* and a filter criteria of the destination AoR *($.@test.com)*:

```
uri-readdress type service base-criteria source address 1.2.3.4 filter-criteria destination aor $.@test.com
```
uri-readdress
CSCF URI Readdress Configuration Mode Commands

The URI Readdress Configuration Mode is used to set URI translations.

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Translation Configuration > URI Readdress Configuration

configure > context context_name > cscf translation name list_name > uri-readdress type readdress_type base-criteria base_criteria

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-uri-readdress)#

Important

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

- action, page 1698
- end, page 1700
- exit, page 1701
action

Adjusts a target address to route sessions to appropriate locations.

Product

SCM

Privilege

Administrator, Config-administrator

Command Modes

Exec > Global Configuration > Context Configuration > CSCF Translation Configuration > URI Readdress Configuration

configure > context context_name > cscf translation name list_name > uri-readdress type readdress_type base-criteria base_criteria

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-uri-readdress)#

Syntax Description

action { add string | delete num_chars | modify string } position num length length target { destination | source } { aor | domain | user }

no action

add string | delete num_chars | modify string

add string: Adds a specified string to a location indicated by the position keyword for the targeted source or destination address component (aor, domain, or user). string must be from 1 to 79 alpha and/or numeric characters.

delete num_chars: Deletes a number of characters starting from a location specified by the position keyword for the targeted source or destination address component (aor, domain, or user). num_chars must be an integer from 1 to 79.

modify string: Modifies a specified string in a location starting with the position keyword for the targeted source or destination address component (aor, domain, or user). The number of characters in the string variable will replace the same number in the address. string must be from 1 to 79 alpha and/or numeric characters.

position num

Specifies the position in the target string where the action is to occur. num must be an integer from 1 to 79.

length length

Specifies the length of the target string where the action is to occur. length must be an integer from 1 to 79.
The length keyword is only supported in modify actions.

**target {destination | source}**

Species that the action is to occur within the source or destination address.

**aor | domain | user**

**aor:** Specifies that the action is applied to AoRs in the targeted source or destination address.

**domain:** Specifies that the action is applied to domains in the targeted source or destination address.

**user:** Specifies that the action is applied to users in the targeted source or destination address.

**no**

Disables target address to route sessions.

**Usage Guidelines**

Use this command to manipulate SIP packets matching the criteria in the uri-readdress command.

**Examples**

The following command prepends a "+1" to a destination AoR:

```
action add +1 position 1 target destination aor
```

The following command removes the first two characters from the destination AoR:

```
action delete 2 position 1 target destination aor
```

The following command replaces characters 2 through 4 with the characters "abc" in the destination AoR:

```
action modify abc position 2 target destination aor
```
**end**

Exits the current 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.
CSCF URN List Configuration Mode Commands

The CSCF URN List Configuration Mode is used to map URNs to URIs for emergency and local call services.

Command Modes

Exec > Global Configuration > Context Configuration > CSCF URN List Configuration

\texttt{configure} > context context\_name > cscf\_urn\_service\_list name list\_name

Entering the above command sequence results in the following prompt:

\texttt{[context\_name] host\_name}(config-cscf-service-urn)\$

\begin{itemize}
  \item \texttt{cscf-urn-service-mapping}, page 1704
  \item \texttt{end}, page 1706
  \item \texttt{exit}, page 1707
\end{itemize}

Important

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

Adds an entry to the service URN mapping table that maps uniform resource names (URNs) to URIs in order to direct specific service-oriented identifiers to the proper location in a network. The table is used after CSCF translation if the result is a local service.

**Product**  
SCM

**Privilege**  
Administrator

**Command Modes**  
Exec > Global Configuration > Context Configuration > CSCF URN List Configuration

```
configure > context context_name > cscf urn-service-list name list_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-cscf-service-urn)#
```

**Syntax Description**

```
[ no ] cscf-urn-service-mapping urn uri uri
```

- **no**  
  Removes an entry from the service URN mapping table.

- **urn urn**  
  Specifies the URN to be routed via a URL to the appropriate destination. *urn* must be from 1 to 79 alpha and/or numeric characters.

- **uri uri**  
  Specifies the URI used to route the URN to the appropriate location. *uri* must be from 1 to 79 alpha and/or numeric characters.

**Usage Guidelines**  
Use this command to add an entry to the service URN mapping table that routes a translated URN to a URI for local services.

**Important**  
Service URN mapping tables are limited to 30 URN to URI mapping entries.
Examples

The following command maps URN `business` to URI `corp@123.45.678.9:5020` and adds it to the service URN mapping table:

cscf-urn-service-mapping urn business uri corp@123.45.678.9:5020
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.
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, page 1710
- exit, page 1711
- recovery, page 1712
- server-interface, page 1713
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.
DDN APN Profile Configuration Mode Commands

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.

**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)#
```

**Important**

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

- end, page 1716
- exit, page 1717
- isr-sequential-paging, page 1718
- qci, page 1719
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

**Examples**
Use the following example to enable ISR sequential paging on the S-GW or SAEGW:

```
isr-sequential-paging
```
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.

**Examples**

The following example configures the minimum buffer size as 3 KB for QCI 3.

```bash
qci 3 ddn min-buf-size 3
```
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, page 1722
- dhcpv6-client-unicast, page 1724
- disable, page 1725
- enable, page 1726
- end, page 1728
- exit, page 1729
- request, page 1730
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.
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`

- 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.

**Examples**
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.

**Examples**

The following command disables support of the rapid commit feature for DHCPv6 client functionality:

```bash
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).
**Usage Guidelines**

Use this command to enable options on the DHCP client.

**Examples**

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.
Examples  The following command enables the DHCP client to request DNS address:
request dhcp-option dns-address
request
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, page 1734
- disable, page 1735
- enable, page 1736
- end, page 1738
- exit, page 1739
- process, page 1740
**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.

**Examples**

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.

**Examples**

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.

**Examples**  
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.

**Examples**

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
```
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, page 1745
- bind, page 1747
- default, page 1750
- dhcp chaddr-validate, page 1752
- dhcp client-identifier, page 1754
- dhcp deadtime, page 1756
- dhcp detect-dead-server, page 1758
- dhcp ip vrf, page 1760
- dhcp server, page 1762
- dhcp server selection-algorithm, page 1764
- end, page 1766
- exit, page 1767
- lease-duration, page 1768
• lease-time, page 1770
• max-retransmissions, page 1771
• retransmission-timeout, page 1772
• T1-threshold, page 1773
• T2-threshold, page 1774
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.

**Examples**
The following command enables support of the rapid commit feature for DHCP server functionality:

```
allow dhcp-server rapid-commit
```
bind

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 [ nexpath-forwarding-address nexthop_ip_address [ mpls-label input in_mpls_label_value output output_mpls_label_value1 [ output_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.
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.
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.

Examples

The following command binds the DHCP service to the interface with an IP address of 192.168.1.210:

`bind address 192.168.1.210`
default

Restores DHCP service parameters to their factory default settings.

**Product**

- GGSN
- ASN-GW
- HA
- P-GW
- SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

```
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.

Examples
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.
Examples

The following command specifies that the chaddr will not be validated in the DHCP messages:

```bash
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:

```console
(context_name)host_name(config-dhcp-service)#
```

**Syntax Description**

```console
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**
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.

Examples
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

```bash
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.
Examples

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.
**Examples**

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 dhcp ip vrf`

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

  - `vrf_name`
  
  Specifies the name of a pre-configured VRF context instance to be associated with a DHCP service. `vrf_name` is 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.
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.

**Examples**

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

```text
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.
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

While configuring HNB-GW for DHCP proxy support, the operator must define 61610 as UDP port for DHCP server. The source port used by HNB-GW 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.

**Examples**

The following command configures a DHCP server with an IP address of 192.168.1.200 and a priority of 1:

```
dhcp server 192.168.1.200 priority 1
```
**dhcp server selection-algorithm**

Specifies the algorithm used to select DHCP servers with which to communicate when multiple servers are configured.

**Product**

- GGSN
- ASN-GW
- 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.

Examples
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 through 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.

**Examples**

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.

Examples
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.

**Examples**

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.

**Examples**

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 RENEWINING state after 4800 seconds.

**Examples**

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.

**Examples**

The following command configures the T2 threshold to 70%:

```
T2-threshold 70 70
```
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, page 1776
- exit, page 1777
- max-retransmissions, page 1778
- server-dead-time, page 1780
- server-ipv6-address, page 1782
- server-resurrect-time, page 1784
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

```plaintext
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.
Examples

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.
Examples

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**

```
syntax server-ipv6-address ipv6_address [port port_number] [priority priority] [-noconfirm]
noserver-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.

Examples

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.

**Examples**
The following command configures the client to wait 25 seconds before considering a dead DHCPv6 server alive again:

```
server-resurrect-time 25
```
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, page 1786
- exit, page 1787
- ipv6, page 1788
- preferred-lifetime, page 1789
- prefix-delegation, page 1790
- rebind-time, page 1791
- renew-time, page 1792
- valid-lifetime, page 1793
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

**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.

**Examples**

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
```

- **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.

**Examples**
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.

**Examples**

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.

**Examples**

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.

**Examples**
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.

**Examples**
The following command configures the valid lifetime for 1001 seconds:

`valid-lifetime 1001`
valid-lifetime
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, page 1796
- deadtime, page 1798
- detect-dead-server, page 1800
- dhcpv6-client, page 1802
- dhcpv6-server, page 1803
- end, page 1804
- exit, page 1805
- server, page 1806
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.

**Examples**

The following command binds the DHCPv6 service to the interface with an IP address of 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.

Examples

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.

**Examples**

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>hostname(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.

---

**Important**

If a server is removed, all calls having an IP address allocated from the server will be released.

---

**Examples**

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
```
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, page 1811
- associate, page 1813
- cea-timeout, page 1815
- connection retry-timeout, page 1816
- connection timeout, page 1817
- description, page 1818
- destination-host-avp, page 1819
- device-watchdog-request, page 1821
- dpa-timeout, page 1822
- dscp, page 1823
- dynamic-peer-discovery, page 1825
- dynamic-peer-failure-retry-count, page 1827
• dynamic-peer-realm, page 1828
• dynamic-route, page 1829
• end, page 1830
• exit, page 1831
• load-balancing-algorithm, page 1832
• max-outstanding, page 1833
• origin address, page 1835
• origin host, page 1836
• origin realm, page 1839
• peer, page 1840
• peer-backoff-timer, page 1843
• reconnect-timeout, page 1845
• response-timeout, page 1847
• rlf-template, page 1848
• route-entry, page 1850
• route-failure, page 1852
• server-mode, page 1854
• tls, page 1855
• use-proxy, page 1857
• vsa-support, page 1859
• watchdog-timeout, page 1860
**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

```plaintext
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**

```plaintext
| 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.

**Examples**

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.
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)

**Examples**

The following command associates a pre-configured SCTP parameter template called *sctp1* to the Diameter endpoint:

```sh
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.

**Examples**

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.

**Examples**
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.

**Examples**
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

description text

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 | retried-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-requests` 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) retried-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.

**Examples**

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.

**Examples**

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.

**Examples**

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.

- **afxx**
  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.

- **csx**
  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.
Diameter Endpoint Configuration Mode Commands

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.

**Examples**

The following command configures the system to dynamically locate peer Diameter servers using SCTP:

```
dynamic-peer-discovery protocol scpt
```


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.

**Examples**

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.

**Examples**
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.

**Examples**

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 Diameter 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

```plaintext
configure > context context_name > diameter endpoint endpoint_name
```

Entering the above command sequence results in the following prompt:

```plaintext
{context_name}host_name(config-ctx-diameter)#
```

**Syntax Description**

```plaintext
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. If multiple servers have the same high weight, load balancing is performed among those servers.

**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.

**Examples**

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:

```plaintext
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.
Examples

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 1836 and origin realm, on page 1839 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
c On figur > 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. In releases prior to 16.0, the host name must be an alphanumeric string of 1 through 64 characters. In 16.0 and later releases, 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
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.

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.

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.

Examples

The following command sets the origin host name to test and the IP address to 10.1.1.1:

```
origin host test address 10.1.1.1
```
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.

**Examples**

The following command sets the origin realm to `companyx`:

```
origin realm companyx
```
peer

This command specifies a peer address for the Diameter endpoint.

Product

All

Privilege

Security Administrator, Administrator

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 ] [ 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 ]

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.

**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.

---

**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.

---

**Examples**

The following command adds the peer named *test* with IP address *10.1.1.1* using port *126*:

```
peer test address 10.1.1.1 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.
Examples

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.
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.

**Examples**

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
```

**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.

**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.
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 a "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.

Examples
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.

**Examples**

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**

```plaintext
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
```

**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.

**Examples**

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:

```bash
<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.

**Examples**
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:

```bash
server-mode demux-mode
```
**tls**

This command enables/disables the Transport Layer Security (TLS) support between a Diameter client and Diameter server node.

**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**

```
tls { certificate certificate | password password | privatekey private_key }
default tls
```

**default**
Disables the TLS support at Diameter endpoint.

**certificate certificate**
Specifies the certificate for TLS support. The certificate must appear encrypted, and must be an alphanumeric string of 700 through 900 characters.

**password password**
Specifies the password for TLS support. The password must be encrypted, and must be an alphanumeric string of 6 through 50 characters.

**privatekey private_key**
Specifies the private key for TLS support. The private key must be encrypted, and must be an alphanumeric string of 900 through 1500 characters.

**Usage Guidelines**
Use this command to configure TLS support between a Diameter client and Diameter server node. By default, TLS is disabled.
Both the Diameter client and server must be configured with TLS enabled or TLS disabled; otherwise, the Diameter connection will be rejected.

**Examples**

The following commands enable the TLS between a Diameter client and Diameter server node:

```bash
tls certificate "-----BEGIN CERTIFICATE-----

MIICGDCCAYECAgEBMA0GCSqGSIb3DQEBAUAMFexCzAJBgNVBAYTAlVTMRMwEQYD
nVQQEwpSVEZNLCBjhmMuMRkwFwYDVQQLEBtBXaWRnZXRzIERpdmZaW9uMRgwFgYD
nVQDew9UZXN0IENBMjAwMTA1MTEwHhcNMDEwNTE3MTYxMDU5WhcNMQwMzA2MTYx
nMDU5WjBRMQswCQYDVQQGEwJUVEtEMBEGAIUEChMKU1RTGSwWj5JlEZMBECG1U
nCXMQV2lkZ2V0cyBEaXZpc2lvbجESMBAGAIUEAkJB9jYWxob3N0MIGfMA0GCSqG
nSIb3DQEBAQUAA4GNADCBiQKBgMQOIPIPLN4DJFBlL2FEIkJHvovR0pKw25
nJ0ZYHW93IHQ4yx6af0Rj99ayRjMY0D26pH4J0qDg040XskSnaYOFzapSZiQMBt

1+oOLommgRJomFlFgW1ryUtKQ1n0hemtUdPOLOI0Q1nCPqZLQIDAIQABMA0GCCG
SqGSIb3DQEBAUAA4GBAIUwmUuwly0WoWuyN2xfoBHya+iRLY

nKmFLoi5+iMcWIsksmA+i+oFLRAN4wmpnSnn8eXycgYdCRklv2xWcvKDm3mp5m7nAMlvvWt/EFpYz6J8

Mo1sf4Vys08A/unXKt23jyKoe2hMwu8mywkgXCYXFY2e7pEeBr/ndsbmkWK

5NgoM8eMun-END CERTIFICATE-----

tls privatekey BEGIN RSA PRIVATE KEY-----

DES-EDE3-CBC,5772A2A7BE34B611\n\n\n1yJ+xAn4MudcIfXXy7EIYng9EohlH8yvce

VLmE4kV0deL/Bhvk25BjYCK5d9\n
BoJDcFzMKkmJXxDbSToArN1sVwiAR\n\nSnb4lllHggYu0V5zdRJn53ft71mjB6Rw

GH+1d2x6t95Qo\n
BoJcKkSeN5zBrZCUXo0NBNEZkFuEvjR+KsA\n
8RtG1QZKbbXzfybwag6+LqkhWYKQHE11546ywWK\n
nus1HJ734ukZooyyazG

6pYGCCYV2u/aYo3qmdcyDq1vmVlve7E4glBrDT597D40\nnvPshivOat0PzIK

4Y0QSvr13G1vTsIZT3IOZto4Au0kLNfYS2ce7prOreF0KjvhV0/n3ttggw9pHd

DmTjHy61KqheZxZVTv+ppdZW+CuB6i8ICBPWP7os1f21e3eoD/oYvnYPCi44a

JvgP+uzORuZBWqAJ0AA1uVW9S8313yzt/tlSFVIoebyd8Cug4TlxKlVnq6bhSafl

4C8ma7YlZvqMzqFfCiolcbx+1A606uiay.JTura4d64cRbe9RflG01nJDCWC6aii9YkAg

R9Wqsd3lyASge/HdqVxVbh48qdfQ57rcHvixyrwRDFnW/IxunM6FLPpDKEco

4MKge7SR2kK2c2AgxUzgZeAY6ePyxhdbdAh0eY21nDeFd/Rbws5seneTiCCMr41OB

4hBFXDKDQsM3K7khozd5DSWsgE6u3IDoTdz76xOSTg==

END RSA PRIVATE KEY-----

tls password TLSpassword_3B167E
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. In 18.0 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.

**Examples**

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.

**Examples**
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.

**Examples**
The following command sets the watchdog timeout setting to 15 seconds:

watchdog-timeout 15
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, page 1862
- end, page 1867
- exit, page 1868
- file, page 1869
**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:

```plaintext
[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.

**Examples**

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.
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
```

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 \textit{string}

Specifies a string to add to the beginning of the Diameter file that is currently being used to store Diameter records.

\textit{string} must be an alphanumeric string of 1 through 31 characters.

Default: \textit{curr}

delete-timeout \textit{seconds}

Specifies a timeout period (in seconds) when completed Diameter files are deleted. By default, files are never deleted.

\textit{seconds} must be an integer from 3600 through 31536000.

Default: Disabled

directory \textit{directory\_name}

Specifies a subdirectory in the default directory in which to store Diameter files.

\textit{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:

- \textit{hyphen}: Specifies to use "-" (hyphen) as the field separator.
- \textit{omit}: Excludes the field separator.
- \textit{underscore}: Specifies to use "_" (underscore) as the field separator. This is the default field separator.

name \textit{file\_name}

Specifies a string to be used as the base file name for Diameter files.

Default: \textit{diameter}

\textit{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.

- \textbf{expanded-format}: Specifies the UTC MMDDYYYYHHMMSS format. This is the default setting.
- \textbf{rotated-format}: Specifies the time stamp format to YYYYMMDHHMMSS format.
- \textbf{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.

\textit{string} must be an alphanumeric string of 1 through 30 characters.

Default: 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


Usage Guidelines
Use this command to configure file characteristics for Diameter records.

Examples
The following command sets the prefix of the current active Diameter file to \textit{Current}:

\texttt{file current-prefix Current}
Diameter Failure Handling Template Configuration Mode Commands

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.

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) #

Important

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

- end, page 1874
- exit, page 1875
- msg-type, page 1876
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 | 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 | 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.
  - 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.

Examples

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
```
msg-type
Diameter Host Select Configuration Mode

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`, page 1882
- `exit`, page 1883
- `host-select row-precedence`, page 1884
- `host-select table`, page 1887
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 } [ range-table { 1 | 2 } ] } [ prefix | suffix ] [ to | to ] [ msisdn-based { prefix | suffix } ] [ active-standby | round-robin ] [ algorithm ]
```

```
o 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.

**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.

### Examples

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.

<table>
<thead>
<tr>
<th>Product</th>
<th>GGSN</th>
<th>HA</th>
<th>HSGW</th>
<th>IPSG</th>
<th>PDSN</th>
<th>P-GW</th>
<th>SCM</th>
<th>SAEGW</th>
<th>S-GW</th>
</tr>
</thead>
</table>

**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.
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 | prefix-table { 1 | 2 } }

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.

table { 1 | 2 | range-table { 1 | 2 } }

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.

algorithm { ip-address-modulus | prefer-ipv4 | prefer-ipv6 | msisdn-modulus | round-robin }

The Round Robin algorithm is effective only over a large number of selections, and not at a granular level.

Important

Usage Guidelines

Use this command to add or modify a Diameter host server table associated with a Diameter host template.

Examples

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
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, page 1890
- cache algorithm, page 1892
- cache size, page 1893
- cache ttl, page 1894
- case-sensitive, page 1896
- description, page 1897
- end, page 1898
- exit, page 1899
- resolver, page 1900
- round-robin answers, page 1901
**bind**

Binds the DNS client to a pre-configured logical IP interface.

**Product**

- MME
- SCM
- SGSN

**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.
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**
- MME
- SCM
- SGSN

**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.

**Usage Guidelines**
Use this command to configure the method by which entries are added and removed from the DNS cache.

**Examples**
The following command configures the cache algorithm for the central proclet to least frequently used (LFU):

```text
cache algorithm central lfu
```
cache size

Configures the maximum number of entries allowed in the DNS cache.

Product
MME
SCM
SGSN

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.

Examples
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**
- MME
- SCM
- SGSN

**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.
  - `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.
Examples

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**

- MME
- SCM
- SGSN

**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

Ends 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.
resolver

Configures the number of DNS query retries and the retransmission interval once the response timer expires.

Product

MME
SGSN

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
Reset 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.

Examples

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**

MME  
SGSN

**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.

**Examples**

The following command configures the DNS client to use round robin method for DNS query answers:  
default | round-robin-answers
round-robin answers
DSCP Template Configuration Mode Commands

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.

**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)#
```

**Important**

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

- control-packet, page 1904
- end, page 1907
- exit, page 1908
- data-packet, page 1909
**control-packet**

Configures the diffserv code point marking (DSCP) value for 3GPP quality of service (QoS) class downlink control packets.

**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
```

- **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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>af11</strong></td>
<td>Assured Forwarding 11 per-hop-behavior (PHB)</td>
</tr>
<tr>
<td><strong>af12</strong></td>
<td>Assured Forwarding 12 PHB</td>
</tr>
<tr>
<td><strong>af13</strong></td>
<td>Assured Forwarding 13 PHB</td>
</tr>
<tr>
<td><strong>af21</strong></td>
<td>Assured Forwarding 21 PHB</td>
</tr>
<tr>
<td><strong>be</strong></td>
<td>Best Effort for Forwarding</td>
</tr>
<tr>
<td><strong>cs1</strong></td>
<td>Class Selector 1 PHB</td>
</tr>
<tr>
<td><strong>cs2</strong></td>
<td>Class Selector 2 PHB</td>
</tr>
<tr>
<td><strong>cs3</strong></td>
<td>Class Selector 3 PHB</td>
</tr>
</tbody>
</table>
### 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 specific 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 associate a specific 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.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>af22:</strong> Assured Forwarding 22 PHB</td>
<td><strong>cs4:</strong> Class Selector 4 PHB</td>
</tr>
<tr>
<td><strong>af23:</strong> Assured Forwarding 23 PHB</td>
<td><strong>cs5:</strong> Class Selector 5 PHB</td>
</tr>
<tr>
<td><strong>af31:</strong> Assured Forwarding 31 PHB</td>
<td><strong>cs6:</strong> Class Selector 6 PHB</td>
</tr>
<tr>
<td><strong>af32:</strong> Assured Forwarding 32 PHB</td>
<td><strong>cs7:</strong> Class Selector 7 PHB</td>
</tr>
<tr>
<td><strong>af33:</strong> Assured Forwarding 33 PHB</td>
<td><strong>ef:</strong> Expedited forwarding PHB</td>
</tr>
<tr>
<td><strong>af41:</strong> Assured Forwarding 41 PHB</td>
<td></td>
</tr>
<tr>
<td><strong>af42:</strong> Assured Forwarding 42 PHB</td>
<td></td>
</tr>
<tr>
<td><strong>af43:</strong> Assured Forwarding 43 PHB</td>
<td></td>
</tr>
</tbody>
</table>
Examples

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 different service 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.

**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
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 specific 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.
Examples

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
```