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

**GGSN Service Configuration Mode Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting</td>
<td>3</td>
</tr>
<tr>
<td>associate gtpu-service</td>
<td>4</td>
</tr>
<tr>
<td>associate peer-map</td>
<td>5</td>
</tr>
<tr>
<td>associate pgw-service</td>
<td>6</td>
</tr>
<tr>
<td>authorize-with-hss</td>
<td>7</td>
</tr>
<tr>
<td>bind</td>
<td>9</td>
</tr>
<tr>
<td>cc behavior</td>
<td>11</td>
</tr>
<tr>
<td>cc profile</td>
<td>13</td>
</tr>
<tr>
<td>default</td>
<td>16</td>
</tr>
<tr>
<td>dns-client</td>
<td>18</td>
</tr>
<tr>
<td>echo-interval</td>
<td>20</td>
</tr>
<tr>
<td>echo-retransmission-timeout</td>
<td>22</td>
</tr>
<tr>
<td>end</td>
<td>23</td>
</tr>
<tr>
<td>exit</td>
<td>24</td>
</tr>
<tr>
<td>fqdn</td>
<td>25</td>
</tr>
<tr>
<td>gtpc allow-on-congestion</td>
<td>27</td>
</tr>
<tr>
<td>gtpc decode-as-hex</td>
<td>29</td>
</tr>
<tr>
<td>gtpc map-mbr-ambr</td>
<td>30</td>
</tr>
<tr>
<td>gtpc nsapi-in-create-pdp-response</td>
<td>32</td>
</tr>
<tr>
<td>operator-del-cause</td>
<td>33</td>
</tr>
<tr>
<td>gtpc private-extension</td>
<td>35</td>
</tr>
<tr>
<td>gtpc ran-procedure-ready-delay</td>
<td>37</td>
</tr>
<tr>
<td>gtpc support-access-side</td>
<td>39</td>
</tr>
<tr>
<td>gtpc support-earp</td>
<td>41</td>
</tr>
<tr>
<td>gtpc suppress-nrupc</td>
<td>42</td>
</tr>
<tr>
<td>gtpu echo-interval</td>
<td>44</td>
</tr>
<tr>
<td>guard-interval</td>
<td>45</td>
</tr>
</tbody>
</table>
## Global Configuration Mode Commands (A-K)

- `aaa accounting-overload-protection` 85
- `aaa default-domain` 86
- `aaa domain-matching ignore-case` 88
- `aaa domain-matching imsi-prefix` 89
- `aaa large-configuration` 91
- `aaa last-resort` 93
- `aaa tacacs+` 95
- `aaa username-format` 96
- `active-charging service` 98
- `alarm` 100
- `apn-profile` 101
- `apn-remap-table` 102
- `arp` 103
- `autoconfirm` 104
- `autoless` 105
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>banner</td>
<td>106</td>
</tr>
<tr>
<td>bearer-control-profile</td>
<td>108</td>
</tr>
<tr>
<td>boot delay</td>
<td>109</td>
</tr>
<tr>
<td>boot interface</td>
<td>110</td>
</tr>
<tr>
<td>boot nameserver</td>
<td>112</td>
</tr>
<tr>
<td>boot networkconfig</td>
<td>113</td>
</tr>
<tr>
<td>boot system priority</td>
<td>115</td>
</tr>
<tr>
<td>bulkstats</td>
<td>118</td>
</tr>
<tr>
<td>ca-certificate</td>
<td>120</td>
</tr>
<tr>
<td>ca-crl</td>
<td>122</td>
</tr>
<tr>
<td>call-control-profile</td>
<td>124</td>
</tr>
<tr>
<td>card</td>
<td>125</td>
</tr>
<tr>
<td>card-standby-priority</td>
<td>126</td>
</tr>
<tr>
<td>cdr-multi-mode</td>
<td>127</td>
</tr>
<tr>
<td>certificate</td>
<td>128</td>
</tr>
<tr>
<td>cli</td>
<td>130</td>
</tr>
<tr>
<td>cli-encrypt-algorithm</td>
<td>133</td>
</tr>
<tr>
<td>clock</td>
<td>135</td>
</tr>
<tr>
<td>cmp auto-fetch</td>
<td>138</td>
</tr>
<tr>
<td>cmp cert-store location</td>
<td>140</td>
</tr>
<tr>
<td>cmp cert-trap time</td>
<td>142</td>
</tr>
<tr>
<td>commandguard</td>
<td>143</td>
</tr>
<tr>
<td>congestion-control</td>
<td>145</td>
</tr>
<tr>
<td>congestion-control overload-disconnect</td>
<td>147</td>
</tr>
<tr>
<td>congestion-control policy</td>
<td>149</td>
</tr>
<tr>
<td>congestion-control threshold</td>
<td>156</td>
</tr>
<tr>
<td>congestion-control threshold license-utilization</td>
<td>160</td>
</tr>
<tr>
<td>congestion-control threshold max-sessions-per-service-utilization</td>
<td>162</td>
</tr>
<tr>
<td>congestion-control threshold message-queue-utilization</td>
<td>164</td>
</tr>
<tr>
<td>congestion-control threshold message-queue-wait-time</td>
<td>166</td>
</tr>
<tr>
<td>congestion-control threshold mmemgr-average-cpu-utilization</td>
<td>168</td>
</tr>
<tr>
<td>congestion-control threshold port-rx-utilization</td>
<td>170</td>
</tr>
<tr>
<td>congestion-control threshold port-specific</td>
<td>172</td>
</tr>
<tr>
<td>congestion-control threshold port-rx-utilization</td>
<td>174</td>
</tr>
<tr>
<td>congestion-control threshold port-tx-utilization</td>
<td>176</td>
</tr>
</tbody>
</table>
congestion-control threshold service-control-cpu-utilization 178
congestion-control threshold system-cpu-utilization 180
congestion-control threshold system-memory-utilization 182
congestion-control threshold tolerance 184
connectedapps 186
content-filtering category database directory 187
content-filtering category database max-versions 188
content-filtering category database override 189
context 190
crash enable 192
crypto blacklist file 195
crypto peer-list 197
crypto remote-secret-list 199
crypto whitelist file 201
cs-network 203
css acsmgr-selection-attempts 205
css delivery-sequence 206
css service 207
diameter dynamic-dictionary 208
diameter-host-template 210
diameter-proxy ram-disk 212
ecmp-lag hash 213
end 214
enforce imsi-min equivalence 215
exit 217
fa-spi-list 218
fabric egress drop-threshold 219
fabric fsc-auto-recovery 221
failure-handling-template 222
global-title-translation address-map 224
global-title-translation association 225
gtpc-load-control-profile 226
gtpc-overload-control-profile 227
gtpp compression-process 228
gtpp push-to-active 229
CHAPTER 3

Global Configuration Mode Commands (L-S) 245

license 249
line 251
link-aggregation 252
local-policy-service 254
local-user allow-aaa-authentication 256
local-user lockout-time 257
local-user max-failed-logins 258
local-user password 260
local-user username 263
logging console 267
logging disable 268
logging display 269
logging filter 271
logging include-ueid 281
logging monitor 284
logging runtime 286
lte-policy 287
mediation-device 288
network-overload-protection mme-new-connections-per-second 289
network-overload-protection mme-tx-msg-rate-control 293
network-overload-protection sgsn-new-connections-per-second 295
network-service-entity 297
ntp 298
ntspool-id 299
operator-policy 300
CHAPTER 4  
Global Configuration Mode Commands (T-threshold phspc)  405

    tacacs mode  409
    task facility acsmgr  410
    task facility imsimgr  411
    task facility ipsecmgr  414
    task facility linkmgr  416
    task facility mmedemux  418
CHAPTER 5  
Global Configuration Mode Commands (threshold poll commands A - N)  613

threshold poll 10sec-cpu-utilization interval  617  
threshold poll a11-ppp-send-discard interval  619  
threshold poll a11-rac-msg-discard interval  621  
threshold poll aa11-rrp-failure interval  623  
threshold poll a11-rrq-msg-discard interval  625
threshold poll aaa-acct-archive-queue-size interval 627
threshold poll aaa-acct-archive-size interval 629
threshold poll aaa-acct-failure interval 630
threshold poll aaa-acct-failure-rate interval 632
threshold poll aaa-auth-failure interval 634
threshold poll aaa-auth-failure-rate interval 636
threshold poll aaa-retry-rate interval 638
threshold poll aamgr-request-queue interval 640
threshold poll active-subscriber interval 642
threshold poll asngw-auth-failure interval 644
threshold poll asngw-handoff-denial interval 646
threshold poll asngw-max-eap-retry interval 648
threshold poll asngw-network-entry-denial interval 650
threshold poll asngw-r6-invalid-nai interval 652
threshold poll asngw-session-setup-timeout interval 654
threshold poll asngw-session-timeout interval 656
threshold poll asnpc-idle-mode-timeout interval 658
threshold poll asnpc-im-entry-denial interval 660
threshold poll asnpc-lu-denial interval 662
threshold poll asnpc-session-setup-timeout interval 664
threshold poll available-ip-pool-group interval 666
threshold poll call-reject-no-resource interval 668
threshold poll call-setup interval 670
threshold poll call-setup-failure interval 672
threshold poll call-setup-failures interval 674
threshold poll call-total-active interval 676
threshold poll card-temperature-near-power-off-limit interval 678
threshold poll cdr-file-space interval 680
threshold poll contfilt-block interval 682
threshold poll contfilt-rating interval 684
threshold poll cpu-available-memory interval 686
threshold poll cpu-load interval 688
threshold poll cpu-memory-usage interval 690
threshold poll cpu-orbs-crit interval 692
threshold poll cpu-orbs-warn interval 694
CHAPTER 6

Global Configuration Mode Commands (threshold poll commands O - Z) 775

threshold poll ipsec-tunnels-established interval 758
threshold poll ipsec-tunnels-setup interval 760
threshold poll license-remaining-session interval 762
threshold poll mgmt-cpu-memory-usage interval 763
threshold poll mgmt-cpu-utilization interval 764
threshold poll mme-attach-failure interval 765
threshold poll mme-auth-failure interval 767
threshold poll nat-pkt-drop 769
threshold poll nat-portChunks-usage interval 771
threshold poll npu-utilization interval 773

threshold poll packets-filtered-dropped interval 778
threshold poll packets-forwarded-to-cpu interval 779
threshold poll pdg-current-active-sessions interval 781
threshold poll pdg-current-sessions interval 783
threshold poll pdif-current-active-sessions interval 785
threshold poll pdif-current-sessions interval 787
threshold poll pdsn-init-rrq-rcvd-rate interval 789
threshold poll pdsn-svc-init-rrq-rcvd-rate interval 791
threshold poll per-service-asngw-sessions interval 793
threshold poll per-service-ggsn-sessions interval 795
threshold poll per-service-gprs-pdp-sessions interval 797
threshold poll per-service-gprs-sessions interval 799
threshold poll per-service-ha-sessions interval 801
threshold poll per-service-lns-sessions interval 803
threshold poll per-service-pdg-sessions interval 805
threshold poll per-service-pdsn-sessions interval 807
threshold poll per-service-samog-sessions interval 809
threshold poll per-service-sgsn-pdp-sessions interval 811
threshold poll per-service-sgsn-sessions interval 813
threshold poll phsgw-auth-failure interval 815
threshold poll phsgw-eapol-auth-failure interval 817
threshold poll phsgw-handoff-denial interval 819
threshold poll phsgw-max-eap-retry interval 820
threshold poll phsgw-max-eapol-retry interval 822
threshold poll phsgw-network-entry-denial interval 824
threshold poll phsgw-session-setup-timeout interval 825
threshold poll phsgw-session-timeout interval 827
threshold poll phspc-session-setup-timeout interval 829
threshold poll phspc-sleep-mode-timeout interval 831
threshold poll phspc-sm-entry-denial interval 833
threshold poll port-high-activity interval 835
threshold poll port-rx-utilization-denial interval 837
threshold poll port-tx-utilization 839
threshold poll ppp-setup-fail-rate interval 841
threshold poll reg-reply-error interval 843
threshold poll rereg-reply-error interval 845
threshold poll route-service interval 846
threshold poll rp-setup-fail-rate interval 848
threshold poll sess-flow-count interval 850
threshold poll storage-utilization interval 851
threshold poll system-capacity interval 853
threshold poll total-asngw-sessions interval 855
threshold poll total-ggsn-sessions interval 857
threshold poll total-gprs-pdp-sessions interval 859
threshold poll total-gprs-sessions interval 861
threshold poll total-ha-sessions interval 863
threshold poll total-henbgw-henb-sessions 865
threshold poll total-henbgw-ue-sessions 867
threshold poll total-hnbgw-hnb-sessions 869
threshold poll total-hnbgw-iu-sessions 871
threshold poll total-hnbgw-ue-sessions 873
threshold poll total-hsgw-sessions interval 875
threshold poll total-lma-sessions interval 877
threshold poll total-lns-sessions interval 879
threshold poll total-mme-sessions 881
threshold poll total-pdsn-sessions interval 883
threshold poll total-pgw-sessions interval 885
threshold poll total-saegw-sessions interval 887
threshold poll total-sgsn-pdp-sessions interval 889
threshold poll total-sgsn-sessions interval 891
threshold poll total-sgw-sessions interval 893
threshold poll total-subscriber interval 895

CHAPTER 7

Global Configuration Mode Commands (threshold ppp-url-blacklisting) 897
threshold ppp-setup-fail-rate 899
threshold route-service bgp-routes 901
threshold route-service vrf-framed-routes 903
threshold route-service vrf-total-routes 905
threshold rp-setup-fail-rate 907
threshold sess-flow-count 909
threshold storage-utilization 910
threshold subscriber active 912
threshold subscriber total 914
threshold system-capacity 916
threshold total-asngw-sessions 918
threshold total-ggsn-sessions 920
threshold total-gprs-pdp-sessions 922
threshold total-gprs-sessions 924
threshold total-ha-sessions 926
threshold total-hnbgw-hnb-sessions 928
threshold total-hnbgw-ue-sessions 932
threshold total-hsgw-sessions 934
threshold total-lns-sessions 936
threshold total-mme-sessions 940
threshold total-pdsn-sessions 942
threshold total-pgw-sessions 944
threshold total-saegw-sessions 946
threshold total-sgsn-pdp-sessions 948
threshold total-sgsn-sessions 950
threshold total-sgw-sessions 952
throttling-override-policy 954
timestamps 955
traffic shape 956
unexpected-scenario session drop-call 958
upgrade limit 960
url-blacklisting database 962
wsg-lookup 964

CHAPTER 8

Global Title Translation Address-Map Configuration Mode Commands 965
associate 966
description 968
do 969
der 970
exit 971
gt-address 972
mode 973
out-address 974

CHAPTER 9

Global Title Translation Association Configuration Mode Commands 975
action 976
description 978
do 979
der 980
exit 981
gt-format 982
variant 983

CHAPTER 10

GPRS Service Configuration Mode Commands 985
accounting 987
admin-disconnect-behavior 989
associate 991
associate-dscp-template 995
associate-service 997
cc profile 999
check-imei 1001
check-imei-timeout-action 1003
ciphering-algorithm 1004
dns mcc-mnc-encoding 1007
dns israu-mcc-mnc-encoding 1009
end 1011
exit 1012
gmm 1013
llc 1019
network-sharing 1023
nri 1026
paging-policy 1029
peer-nsei 1031
plmn 1033
rai-skip-validation 1035
reporting-action event-record 1036
s4-overcharge-protection 1038
setup-timeout 1040
sgsn-context-request 1041
sgsn-number 1042
sm 1043
sndcp 1046

CHAPTER 11
GRE Tunnel Interface Configuration Mode Commands 1047
destination 1048
end 1049
exit 1050
keepalive 1051
source 1053
tos 1055
ttl 1057

CHAPTER 12
Gs Service Configuration Mode Commands 1059
associate-sccp-network 1060
bssap+ 1062
end 1064
exit 1065
max-retransmission 1066
non-pool-area 1068
pool-area 1070
gsxn-number 1072
timeout 1073
vlr 1075

CHAPTER 13
GT-Format1 Configuration Mode Commands 1077
end 1078
exit 1079
nature-of-address 1080
odd-even-indicator 1081

CHAPTER 14
GT-Format2 Configuration Mode Commands 1083
end 1084
exit 1085
translation-type 1086

CHAPTER 15
GT-Format3 Configuration Mode Commands 1087
encoding-scheme 1088
end 1089
exit 1090
numbering-plan 1091
translation-type 1092

CHAPTER 16
GT-Format4 Configuration Mode Commands 1093
encoding-scheme 1094
end 1095
exit 1096
nature-of-address 1097
numbering-plan 1098
translation-type 1099

CHAPTER 17
GTPC Load Control Profile Configuration Mode Commands 1101
end 1102
CHAPTER 18

GTPC Overload Control Profile Configuration Mode Commands 1115

exit 1103
inclusion-frequency 1104
load-control-handling 1106
load-control-publishing 1108
threshold 1110
weightage 1112

CHAPTER 19

GTPP Server Group Configuration Mode Commands 1137

end 1117
exit 1118
inclusion-frequency 1119
message-prioritization 1121
overload-control-handling 1123
overload-control-publishing 1125
self-protection-behavior 1127
tolerance 1129
throttling-behavior 1131
validity-period 1133
weightage 1135
CHAPTER 20
GTP-U Service Configuration Mode Commands 1217

bind 1219
echo-interval 1221
echo-retransmission-timeout 1223
end 1225
exit 1226
extension-header 1227
ip qos-dscp 1228
ipsec-allow-error-ind-in-clear 1231
ipsec-tunnel-idle-timeout 1232
max-retransmissions 1233
path-failure clear-trap 1234
path-failure detection-policy 1236
retransmission-timeout 1238
sequence-number 1240
source-port 1241
udp-checksum 1243

CHAPTER 21
HA Proxy DNS Configuration Mode Commands 1245
description 1246
end 1247
exit 1248
pass-thru 1249
redirect 1251

CHAPTER 22
HA Service Configuration Mode Commands 1253
a11-signalling-packets 1256
aaa 1257
access-network 1259
associate 1260
authentication 1261
bind 1264
binding-update 1266
default 1267
default subscriber 1270
description 1271
encapsulation 1272
end 1274
exit 1275
fa-ha-spi 1276
gre 1279
idle-timeout-mode 1281
ikev1 1283
ip context-name 1285
ip local-port 1286
ip pool 1287
isakmp 1288
min-reg-lifetime 1290
CHAPTER 23
HD Storage Policy Configuration Mode Commands 1333

- directory 1334
- end 1335
- exit 1336
- file 1337

CHAPTER 24
HeNB-GW Access Service Configuration Mode Commands 1339

- associate henbgw-network-service 1341
- associate sctp-param-template 1343
CHAPTER 25
HeNBGW QCI Dscp Mapping Table Configuration Mode Commands  

dscp-marking-default  1362
end  1364
exit  1365
qci  1366

CHAPTER 26
HeNB-GW Network Service Configuration Mode Commands  1369

anr-info-retrieval  1370
associate sctp-param-template  1371
default-paging-drx  1372
end  1373
exit  1374
logical-enb  1375
paging-rate-control  1377
public-warning-system  1379
pws  1380
s1ap-max-retransmissions  1382
s1ap-retransmission-timeout  1383

CHAPTER 27
HLR Configuration Mode Commands  1385

acn-version-retention  1386
ip iu-qos-dscp 1436
ip iuh-qos-dscp 1439
ipsec connection-timeout 1443
iurh-handoff 1444
iurh-handoff-guard-timer 1445
mocn-max-reroute-attempts 1446
mocn-reroute-timeout 1447
paging cs-domain 1448
paging imsi-purge-timer 1450
paging ps-domain 1451
paging open-hnb 1453
radio-network-plmn 1455
ranap reset 1457
rtcp report 1459
rtp address 1461
rtp port 1463
rtp mux 1465
sctp bind 1466
sctp checksum-type 1468
sctp connection-timeout 1469
sctp cookie-life 1471
sctp heart-beat-timeout 1472
sctp mtu-size 1474
sctp rto 1475
sctp sack-frequency 1476
sctp sack-period 1477
security-gateway bind 1478
sessmgr-to-cbsmgr-pacing-timer 1480
tnsf-timer 1481
ue registration-timeout 1482

CHAPTER 30  HNB-CS Network Configuration Mode Commands 1483
associate alcap-service 1485
associate rtp pool 1487
associate sccp-network 1489
CHAPTER 31  
HNB-PS Network Configuration Mode Commands  
associate gtpu-service 1519  
associate-sccp-network 1521  
end 1522  
exit 1523  
global-rnc-id 1524  
map core-network-id 1526  
map idns range 1528  
map nri range 1530  
nri length 1532  
null-nri 1534  
offload-sgsn 1536  
ranap reset 1538  
sgsn deadtime 1540  
sgsn point-code 1542  
sccp 1544

CHAPTER 32  
HNB-RN PLMN Configuration Mode Commands 1545  
associate cs-network 1546
CHAPTER 33

HSGW Service Configuration Mode Commands 1553

associate ps-network 1547
authorised-macro-lai 1548
end 1550
exit 1551
mc-id 1552

a11-signalling-packets 1555
associate 1556
bind address 1557
context-retention-timer 1559
data-available-indicator 1560
data-over-signaling 1561
dns-pgw 1562
end 1564
exit 1565
fqdn 1566
fragment 1568
gre 1569
ip 1572
lifetime 1575
max-retransmissions 1576
mobile-access-gateway 1577
network-initiated-qos 1578
plmn-id 1579
policy-overload 1580
profile-id-qci-mapping 1582
registration-deny 1583
retransmission-timeout 1585
rsip 1586
setup-timeout 1588
spi remote-address 1589
ue-initiated-qos 1592
unauthorized-flows 1593
### CHAPTER 34

**HSGW Service RoHC Configuration Mode Commands**

- cid-mode 1596
- end 1598
- exit 1599
- mrru 1600
- profile 1601

### CHAPTER 35

**HSS Peer Service Configuration Mode Commands**

- auth-request 1604
- diameter hss-dictionary 1606
- diameter hss-endpoint 1608
- diameter suppress 1610
- diameter update-dictionary-avps 1611
- dynamic-destination-realm 1613
- end 1614
- exit 1615
- failure-handling 1616
- request timeout 1619
- zone-code-format 1620
GGSN Service Configuration Mode Commands

The Gateway GPRS Support Node (GGSN) Configuration Mode is used to create and manage GGSN services within the current context.

**Command Modes**

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

`configure > context context_name > ggsn-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-ggsn-service)#
```

**Important**

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

- accounting, page 3
- associate gtpu-service, page 4
- associate peer-map, page 5
- associate pgw-service, page 6
- authorize-with-hss, page 7
- bind, page 9
- cc behavior, page 11
- cc profile, page 13
- default, page 16
- dns-client, page 18
- echo-interval, page 20
- echo-retransmission-timeout, page 22
- end, page 23
• exit, page 24
• fqdn, page 25
• gtpc allow-on-congestion, page 27
• gtpc decode-as-hex, page 29
• gtpc map-mbr-ambr, page 30
• gtpc nsapi-in-create-pdp-response, page 32
• operator-del-cause, page 33
• gtpc private-extension, page 35
• gtpc ran-procedure-ready-delay, page 37
• gtpc support-access-side, page 39
• gtpc support-earp, page 41
• gtpc suppress-nrupc, page 42
• gtpu echo-interval, page 44
• guard-interval, page 45
• ip local-port, page 47
• ip qos-dscp, page 49
• max-contexts, page 53
• max-retransmissions, page 55
• mbms policy, page 56
• newcall, page 57
• path-failure, page 59
• plmn id, page 61
• plmn unlisted-sgsn, page 63
• policy, page 65
• retransmission-timeout, page 67
• retransmission-timeout-ms, page 69
• setup-timeout, page 71
• sgsn address, page 72
• sgsn define-multiple-address-group, page 74
• sgsn multiple-address-group, page 76
• sgsn mcc-mnc, page 78
• trace-collection-entity, page 79
accounting

Configures the name of the context configured on the system that processes accounting for PDP contexts handled by this GGSN service.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax Description**

```
accounting context context_name
no accounting context
```

- **no**
  - Removes a previously configured accounting context.

  **context_name**
  - Specifies the name of the context to be used for accounting. `context_name` must be an alphanumeric string of 1 through 79 characters that is case sensitive.

**Usage Guidelines**

By default, the system attempts to use the same context as the one in which the GGSN service is configured for accounting purposes. This command can be used to either change the system's default behavior, or allow GPRS Tunneling Protocol Prime (GTPP) accounting to a charging gateway (CG).

By default when GTPP accounting is used, accounting records will be sent to the accounting servers configured in whichever context the GGSN service is configured. This command may be used to override that default.

**Examples**

The following command configurations the GGSN service's accounting context to be plmn1:

```
accounting context plmn1
```
associate gtpu-service

This command associates a previously configured GTP-U service to bind the GGSN service with a peer. A GTP-U service must be configured in Context Configuration mode before using this configuration.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration
configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-ggsn-service)#
```

**Syntax Description**

- **associate gtpu-service svc_name**
- **no associate gtpu-service**

**no**
Removes the associated GTP-U service from this GGSN service configuration.

**svc_name**
Identifies the name of the GTP-U service preconfigured in Context Configuration mode to associate with a GGSN service. *svc_name* is an alphanumeric string from 1 through 63 characters.

**Usage Guidelines**
Use this command to configure GTP-U data plan between GGSN service and peer node. The service defined for GTP-U can be configured in Context configuration mode.

**Examples**
Following command associates GTP-U service named *gtpu-hnb1* with specific GGSN service.

```
associate gtpu-service gtpu-hnb1
```
associate peer-map

This command associates a previously configured GGSN peer-map in LTE Policy Configuration mode with GGSN service. A peer-map must be configured before using this configuration.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

`configure > context context_name > ggsn-service service_name`

Entering the above command sequence results in the following prompt:

`
{context_name}@host_name(config-ggsn-service)#
`

**Syntax Description**

- **associate peer-map** *peer_map_name*
  
- **no associate peer-map**

  _**no**_

  Removes the associated Peer-Map from this GGSN service configuration.

  _**peer_map_name**_

  Identifies the name of the Peer Map preconfigured in LTE-Policy Configuration mode to associate with a GGSN service. *peer_map_name* is an alphanumeric string from 1 through 63 characters.

**Usage Guidelines**

Use this command to associate Peer Map with GGSN service. The peer-profile associated with peer map can be configured in GGSN Peer-Profile configuration mode.

---

**Important**
When there is no association of peer-map in any of the service, then "default" peer profile of the corresponding service-interface type shall be applied except for GTP-C parameters. Also GTP-C parameters configuration shall be applied from GG service level configuration for GGSN.

A maximum of 1024 peer map rules can be configured on one system.

**Examples**

Following command associates Peer Map named `ggsn_peer_map1` with specific GGSN service.

`associate peer-map ggsn_peer_map1`
**associate pgw-service**

This command enables a previously configured P-GW service to which handover will be done by the GGSN service. The P-GW service must be configured in Context Configuration mode before using this configuration.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
/context_name/host_name(config-ggsn-service)#
```

**Syntax Description**

- `associate pgw-service svc_name`
- `no associate pgw-service`

- `no`
  
  Removes the associated P-GW service from this GGSN service configuration.

- `svc_name`
  
  Identifies the name of the P-GW service preconfigured in Context Configuration mode to which handover will be done.

  The `svc_name` must be an alphanumeric string from 1 through 63 characters.

**Usage Guidelines**

Use this command to allow enabling/disabling bearer handover from GGSN to a P-GW service. The service defined for P-GW can be configured in Context configuration mode.

The P-GW’s eGTP service should have the same bind address as GGSN service and P-GW and GGSN should share same GTP-U, otherwise handover will fail.

**Examples**

Following command enables P-GW service named `pgw-test` handover with specific GGSN service.

```
associate pgw-service pgw-test
```
authorize-with-hss

This command enables or disables subscriber session authorization via a Home Subscriber Server (HSS) over an S6b Diameter interface. This feature is required to support the interworking of GGSN with P-GW and HA.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax Description**
```
authorize-with-hss [ report-ipv6-addr ]
{ default | no } authorize-with-hss
```

- **default**
  Disables the default authorization of subscriber over S6b interface. Resets the command to the default setting of "authorize locally" from an internal APN authorization configuration.

- **no**
  Disables the default authorization of subscriber over S6b interface. Resets the command to the default setting of "authorize locally" from an internal APN authorization configuration.

- **report-ipv6-addr**
  Enables IPv6 address reporting through Authorization-Authentication-Request (AAR) towards the S6b interface.

**Usage Guidelines**
Use this command to enable/disable the authorization support for subscriber over S6b interface, which is used between GGSN and the 3GPP AAA to exchange the information related to charging, P-CSCF discovery, etc. Use of this feature allows the GGSN service to interact with HSS over S6b interface through Diameter configuration which is already configured on the system.
**Important**

Diameter configuration must be available before enabling this command. For more information regarding Diameter interface configuration, refer Diameter Endpoint Configuration Mode Commands chapter.

**Important**

This command is a license-enabled feature.

**Examples**

The following command enables subscriber authorization via an HSS over an S6b Diameter interface to provide session interoperability between GGSN and P-GW and HA in this GGSN service:

```
authorize-with-hss
```
**bind**

Binds the GGSN service to a logical IP interface serving as the Gn interface. Specifies the maximum number of subscribers that can access this service over the interface.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```bash
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax Description**

```
[ no ] bind { address ipv4_address | ipv6-address ipv6_address } | ipv4-address ipv4_address | ipv6-address ipv6_address | ipv4-address ipv4_address }
```

- **no**
  
  Removes a previously configured binding for the GGSN service.

- **address ipv4_address**
  
  Specifies the IP address (address) of the interface configured as the Gn interface. `ipv4_address` is specified in IPv4 dotted-decimal notation.

- **ipv4-address ipv4_address**
  
  Specifies the IP address (address) of the interface configured as the Gn interface. `ipv4_address` is specified in IPv4 dotted-decimal notation.

- **ipv6-address ipv6_address**
  
  Specifies the IP address (address) of the interface configured as the Gn interface. `ipv6_address` is specified in IPv6 colon-separated hexadecimal notation.

**Usage Guidelines**

Used to associate or tie the GGSN service to a specific logical IP address. The logical IP address or interface takes on the characteristics of a Gn interface. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.
**Examples**

The following command would bind the logical IP interface with the IPv4 address of 192.168.3.1 to the GGSN service:

`bind ipv4-address 192.168.3.1`

The following command disables a binding that was previously configured:

`no bind ipv4-address 192.168.3.1`
cc behavior

Configures the 3GPP behavior bits associated with the GGSN's charging characteristics (CC).

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

`configure > context context_name > ggsn-service service_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ggsn-service)#`

**Syntax Description**

- `cc behavior no-records nr_value`
- `default cc behavior`
- `no cc behavior no-records`

**default**
Restores behavior parameters to default value of 0 (disabled).

**no**
Removes the previously configured behavior bit.

**no-records nr_value**
Default: 0 (disabled)

Specifies the behavior bit upon which the GGSN ceases sending accounting records to a server.

`nr_value` can be configured to an integer from 1 through 12 corresponding to the 12 behavior bits – B1 through B12.

**Usage Guidelines**

3GPP standards after 3GPP R98 included 12 behavior bits as part of GGSN charging characteristics. Like the charging characteristics profile index, the behavior bits are sent by the SGSN to the GGSN in the Create PDP Context request message.

This command configures the behavior bits for each of the conditions described.
Examples

The following command configures a behavior bit of 10 for no-records:

```
cc behavior no-records 10
```
**cc profile**

Configures the charging characteristic (CC) profile index properties.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

\[(context_name) host_name(config-ggsn-service)#\]

**Syntax Description**

```
cc profile index | buckets number | interval time | downlink down_octets uplink up_octets | total total_octets | prepaid { prohibited | use-rulebase-configuration } | sgsns num_changes | tariff time1 mins hours | time2 mins hours | time3 mins hours | time4 mins hours | time5 mins hours | time6 mins hours | volume { downlink vol_down_octets uplink vol_up_octets | total total_octets } |
```

default cc profile index

default

Returns the specified cc profile to the original default system settings. The following defaults are applied:

- buckets: 4
- interval: Disabled
- volume: Disabled
- sgsns: 4
- tariff-time: Disabled

**no**

Removes a previously configured profile index.

**index**

Configures a profile index for the parameter to be specified. index can be configured to an integer from 0 through 15.
3GPP standards suggest that profile index values of 1, 2, 4, and 8 be used for hot billing, flat rate billing, prepaid billing and normal billing, respectively. A single charging characteristics profile can contain multiple behavior settings.

**buckets number**

Default: 4

Specifies the number of statistics container changes due to QoS changes or tariff time that can occur before an accounting record should be closed.

*number* can be configured to an integer from 1 through 4.

**interval time [downlink down_octets uplink up_octets | total total_octets ]**

Specifies the normal time duration that must elapse before closing an accounting record provided that any or all of the following conditions occur:

- Downlink traffic volume is reached within the time interval
- Uplink traffic volume is reached within the time interval
- Total traffic volume (up and downlink) is reached within the time interval

*time* is measured in seconds and can be configured to an integer from 60 through 4000000.

*down_octets* is the downlink traffic volume measured in octets and can be configured to an integer from 0 through 1000000.

*up_octets* is the uplink traffic volume measured in octets and can be configured to an integer from 0 through 1000000.

*total_octets* is the total traffic volume measured in octets and can be configured to an integer from 0 through 1000000.

**prepaid { prohibited | use-rulebase-configuration }**

This command enables or disables prepaid for the specified profile index.

Default: N/A

**prohibited**: Disable prepaid for the specified profile index.

**use-rulebase-configuration**: Use the prepaid configuration in the rulebase.

**sgsns num_changes**

Default: 4

Specifies the number of SGSN changes (such as, inter-SGSN switchovers) resulting in a new RAI (Routing Area Identity) that can occur before closing an accounting record.

*num_changes* can be configured to an integer from 1 through 15.
tariff time1 mins hours time2 mins hours time3 mins hours time4 mins hours time5 mins hours time6 mins hours

Specifies time-of-day time values to close the current statistics container (but not necessarily the accounting record). Six different tariff times may be specified. If less than six times are required, the same time can be specified multiple times.

---

Important

The system assumes that the billing system uses the day/date to determine if the statistics container represents an actual tariff period.

---

For each of the different tariff times, the following parameters must be configured:

- **mins**: The minutes of the hour, an integer value from 0 to 59.
- **hours**: The hour of the day, an integer value from 0 to 23.

volume {downlink vol_down_octets uplink vol_up_octets | total total_octets }

Specifies the downlink, uplink, and total volumes that must be met before closing an accounting record.

- **vol_down_octets** is measured in octets and can be configured to an integer from 100000 to 4000000000.
- **vol_up_octets** is measured in octets and can be configured to an integer from 100000 to 4000000000.
- **total_octets** is the total traffic volume (up and downlink) measured in octets and can be configured to an integer from 100000 to 4000000000.

---

Usage Guidelines

Charging characteristics consist of a profile index and behavior settings. This command configures profile indexes for the GGSN's charging characteristics. The GGSN supports up to 16 profile indexes.

This command works in conjunction with the `cc-sgsn` command located in the APN Configuration Mode that dictates which CCs should be used for subscriber PDP contexts.

---

Examples

The following command configures a profile index of 10 for tariff times of 7:00 AM and 7:30 PM:

```
cc profile 10 tariff time1 0 7 time2 30 19 time3 0 7 time4 30 19
```
**default**

Sets/restores the default value assigned for the specified parameter.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```bash
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-ggsn-service)#
```

**Syntax Description**

```bash
| default | { cc { behavior | profile index } | echo-interval | gtpu echo-interval | gtpu reorder { context | sequence-numbers | timeout } | guard-interval | ip { local-port gtpc-v1 | qos-dscp } | max-retransmissions | plmn { unlisted-sgsn } | setup-timeout | timeout }
```

cc { behavior | profile index }

Restores the GGSN's charging characteristics parameters to the following default settings:

- **behavior**: Restores all behavior parameters to their default values of 0 (disabled).
- **profile**: For the specified index, the following defaults are applied:
  - buckets: 4
  - interval: Disabled
  - volume: Disabled
  - sgsns: 4
  - tariff-time: Disabled

**echo-interval**

Restores the GTP echo-interval parameter to its default setting of 60.

**gtpu echo-interval**

Restores the GTPU echo-interval parameter to its default setting of 60.
gtpu reorder \{ context | sequence-numbers | timeout \}
Restores the gtpu reordering parameters to the following default settings:

- gtpu reorder context: Disabled
- gtpu reorder sequence-numbers: Disabled
- gtpu reorder timeout: 100 milliseconds

gtpu udp-checksum insert
Restores the GGSN gtpu udp-checksum parameter to its default setting of enabled.

guard-interval
Restores the GGSN guard-interval parameter to its default setting of 100.

ip \{local-port gtpc-v1 | qos-dscp \}
Restores the GGSN ip parameters to the following default setting:

- local-port gtpc-v1: 2123
- qos-dscp: conversational ef streaming af11 interactive af21 background be

max-retransmissions
Restores the GGSN max-retransmissions parameter to its default setting of 4.

plmn \{ unlisted-sgsn \}
Restores the GGSN plmn unlisted-ggsn parameter to its default setting of reject.

setup-timeout
Restores the GGSN setup-timeout parameter to its default setting of 60.

timeout
Restores the GGSN timeout parameter to its default setting of 5.

Usage Guidelines
After the system has been modified from its default values, this command is used to set/restore specific parameters to their default values.

Examples
The following command restores the GGSN service's guard interval parameter to its default setting:

default guard-interval
**dns-client**

This command defines the context name where a DNS client is configured. It associates an existing DNS client configuration with the GGSN to perform a DNS query for P-CSCF, if a P-CSCF query request in an AAA message is received from the Diameter node.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-ggsn-service)##
```

**Syntax Description**

```
dns-client context dns_ctxt_name
{ no | default } dns-client context
```

- **no**
  
  Removes the association of DNS context which was configured to perform DSN query in this GGSN service.

- **default**
  
  Sets the default context for the DNS client.

**dns_ctxt_name**

Specifies the name of the context in which a DNS client configuration is present. Typically this should be the same context in which this GGSN service is configured.

**Usage Guidelines**

Use this command to associate a DNS client configuration to perform DNS query used for the resolution of P-CSCF query received in AAA message from Diameter peer, on the basis of DNS client parameters configured in a context.

A DNS client configuration must be present in the same context as GGSN service before enabling this command to perform DNS query for P-CSCF.
**Important**  This command is a license-enabled feature.

**Examples**  
The following command associates a DNS client configuration to perform DNS query for P-CSCF with this GGSN service which is configured in same context as GGSN service:

```bash
default dns-client context
```
**echo-interval**

Configures the rate at which GPRS Tunneling Protocol (GTP) v1-C Echo packets are sent from the GGSN service to the SGSN.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

`configure > context context_name > ggsn-service service_name`

Entering the above command sequence results in the following prompt:

`(context_name)host_name(config-ggsn-service)#`

**Syntax Description**

`echo-interval seconds [ dynamic [ smooth-factor multiplier ] ]`

{ default | no } `echo-interval`

- **default**
  
  Configures the default value (60 seconds) for echo interval.

- **no**

  Disables the sending of GTPv1-C Echo packets.

- **seconds**

  Default: 60

  Specifies the frequency at which the GGSN service sends GTPv1-C Echo packets to the SGSN(s) it is configured to communicate with.

  `seconds` is measured in seconds and can be configured to an integer from 60 through 3600.

- **dynamic | smooth-factor multiplier |**

  Enables the dynamic echo timer for the GTP-U service.

  **smooth-factor multiplier**: Introduces a multiplier into the dynamic echo timer as an integer from 1 through 5. Default: 2
Usage Guidelines

Use this command to adjust the rate at which the GGSN sends these packets. GTPv1-C Echo packets are used to detect whether SGSNs that the GGSN service is communicating with, has become unresponsive or has rebooted.

The system initiates this protocol for each of the following scenarios:

- Upon system boot
- Upon the configuration of a new SGSN on the system using the `sgsn address` command as described in this chapter
- Upon the execution of the path failure detection policy as described in the `path-failure` command of this chapter

The echo-interval command is used in conjunction with the `max-retransmissions` and `retransmission-timeout` commands as described in this chapter.

In addition to receiving an echo response for this echo protocol, if GGSN receives a Node Alive Request message or a Echo Request message from a presumed dead SGSN, it will immediately assume the SGSN is active again.

If the GGSN discovers that an SGSN has become unresponsive, it will terminate all PDP contexts that had been established with the SGSN.

Examples

The following command configures the GGSN service to send GTP Echo packets every 120 seconds:

```
  echo-interval 120
```
**echo-retransmission-timeout**

Configures the timeout for GTPv1 echo message retransmissions for this service.

**Product**

GGSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-ggsn-service)#
```

**Syntax Description**

```
echo-retransmission-timeout seconds
default echo-retransmission-timeout
```

default

Returns the command to its default setting of 3.

```
seconds
```

Default: 5

Configures the echo retransmission timeout, in seconds, for the GTPv1 service as an integer ranging from 1 to 20.

**Usage Guidelines**

Use this command to configure the amount of time, in seconds, before the GTPv1 service transmits another echo request message. The value set in this command is used, as is, for the default echo. If dynamic echo is enabled (echo-interval dynamic) the value set in this command serves as the dynamic minimum (if the RTT multiplied by the smooth factor is less than the value set in this command, the service uses this value).

**Examples**

The following command sets the retransmission timeout for echo messages to 2 seconds:

```
echo-retransmission-timeout 2
```
**end**

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax Description**
end

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

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

exit

**Usage Guidelines**

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

This command defines Fully Qualified Domain Name (FQDN) which would be used for authorization over S6b interface between GGSN and 3GPP AAA/HSS.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax Description**

```
fqdn host host_name realm realm_id
{ no | default } fqdn

no

Removes the configured FQDN host name and realm ID from the GGSN service.

default

Sets the system to default mode for this command and configures the host and realm ID value to NULL.

host host_name

Specifies the name of the host to be used for authorization over an S6b interface to a 3GPP AAA server/HSS from the GGSN service.

*host_name* is a unique node name for authorization over the S6b interface from this GGSN service.

*host_name* must be an alphanumeric string of 1 through 127 characters. Punctuation marks are allowed.

realm realm_id

Specifies the realm as an FQDN to be used for authorization over S6b interface with 3GPP AAA server/HSS from GGSN service. The realm may typically be a company or service name.

*realm_id* is a unique identifier configured for the authorization over S6b interface from this GGSN service, expressed as an alphanumeric string of 1 through 127 characters. Punctuation marks are allowed.

*host_name*
Usage Guidelines

Use this command to define host and realm as the FQDN for a 3GPP AAA server/HSS that would be used for authorization over an S6b interface with the GGSN. The realm specified as an FQDN may typically be a company or service name.

By default the FQDN host and realm will be NULL

---

Important

This command is a license-enabled feature.

---

Examples

The following configures the hss1 as host name and xyz.com as realm to support authorization over an S6b from this GGSN service:

```
fqdn host hss1 realm xyz.com
```
gtpc allow-on-congestion

This command enables the prioritized handling for VoLTE/Emergency calls for the current GGSN service. This is a license-controlled feature under the license introduced for VoLTE.

**Product**
GGSN

**Privilege**
Administrator, Config Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax Description**

```
[ no ] gtpc allow-on-congestion { apn-name | apn_name | arp | priority | rel99arp | priority }
```

- **no**
  Removes the default configuration.

- **apn-name**
  Configures the GW to allow calls for this APN even under congestion. *apn_name* is the access point name to be prioritized. It is a string of size 1 to 64.

- **arp priority**
  Configures the GW to allow calls for this ARP even under congestion. *priority* is the ARP Priority Level, ranging integer 1..15

- **rel99arp priority**
  Configures the GW to allow calls for the Rel99 ARP under congestion. Rel99arp is ignored in case EARP is received. *priority* is the REL99ARP priority, ranging from integer 1..3

**Usage Guidelines**

For VoLTE and Emergency calls there are certain scenarios where-in prioritized handling is needed as compared to non-VoLTE calls

When CLI is enabled:

- Under congestion scenarios, emergency calls are given priority and are accepted as much as possible
• Only 3 or less APN and ARP values can be configured for prioritized handling in congestion situation.
• Gn CPCReq calls having the Release 99 bearer parameter ARP (not EARP) are allowed under congestion.

**Examples**

The following command ignores the congestion situation for apn name "intershat":

```
gtpc allow-on-congestion apn intershat
```
gtpc decode-as-hex

This command configures the GGSN to decode the MCC-MNC parameters from the User Location Information (ULI) to hexadecimal digits.

Product GGSN

Privilege Administrator, Config Administrator

Command Modes Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:
[context_name]host_name(config-ggsn-service)#

Syntax Description [ default | no ] gtpc decode-as-hex

default
This CLI is disabled by default. The received MCC-MNC parameters of ULI are decoded assuming that, it contains decimal digits only.

no
Removes the default configuration.

Usage Guidelines The GTP parameter ULI contains encoded MCC-MNC digits. This new CLI configures GGSN to decode this MCC-MNC into hexadecimal digits. When CLI is disabled, current behavior is in effect - The received MCC-MNC is decoded assuming that, it contains decimal digits only. When CLI is enabled and if the received MCC-MNC is valid, it is decoded into decimal digits. If the received MCC-MNC is invalid, all digits are decoded into hexadecimal digits, including filler digits, if any. Hexadecimal digits are represented using Upper Case ASCII characters (A, B, C, D, E, F).

Examples The following command decodes MCC-MNC as hexadecimal:
gtpc decode-as-hex
This command maps the Maximum Bit Rate AVP received in Update PDP Context QoS message from SGSN to Aggregate Maximum Bit Rate attribute value (AMBR), if AMBR is not received in Update PDP Context QoS message from SGSN. This command is applicable for Gn-Gp GGSN mode only and not applicable to standalone GGSN. By default this command is disabled.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-ggsn-service)#
```

**Syntax Description**

```
[ default | no ] gtpc map-mbr-ambr
```

- **default**

  Sets the default mode to map the Maximum Bit Rate AVP received in Update PDP Context QoS message from SGSN to Aggregate Maximum Bit Rate attribute value (AMBR), if AMBR is not received in Update PDP Context QoS message from SGSN.

- **no**

  Removes the configured mapping of the MBR AVP received in Update PDP Context message from SGSN to AMBR attribute value.

**Usage Guidelines**

Use this command to map the Maximum Bit Rate AVP received in Update PDP Context QoS message from SGSN to Aggregate Maximum Bit Rate attribute value (AMBR), if AMBR is not received in Update PDP Context QoS message from SGSN.

**Important**

To use this command event trigger for QoS-Change for session must be provisioned on PCRF.
The following command configures the GGSN service to map the MBR received in Update PDP Context QoS message from SGSN to Aggregate Maximum Bit Rate attribute value (AMBR):

gtpc map-mbr-ambr
gtpc nsapi-in-create-pdp-response

This command excludes or includes the optional information element (IE) Network Service Access Point Identifier (NSAPI) within "Create PDP Context Response" messages in GTP-C.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
/context_name/host_name(config-ggsn-service)#
```

**Syntax Description**

```
[ default | no ] gtpc nsapi-in-create-pdp-response
```

- **default**
  
  Sets the default mode for GTP-C messages not to include the NSAPI IE in "Create PDP Context Response" messages.

- **no**
  
  Removes the preconfigured mode for GTP-C messages; the GTP-C message will not include the NSAPI IE in "Create PDP Context Response" messages. By default it is disabled.

**Usage Guidelines**

Use this command to exclude or include the NSAPI IE in "Create PDP Context Response" GTP-C messages received from the SGSN.

**Examples**

The following command configures the GGSN service to include the optional NSAPI IE in "Create PDP Context Response" messages:

```
gtpc nsapi-in-create-pdp-response
```
operator-del-cause

Enables or disables the Cause-IE feature for Delete PDP Context Request in GGSN. This CLI is disabled by default.

Important
This command is license dependent. For more information please contact your Cisco account representative.

Product
GGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ggsn-service)#

Syntax Description
| default | no | gtpc operator-del-cause

default
Sets the default mode for Operator Cause-IE behavior feature. By default, it is disabled.

no
Disables Operator Cause-IE behavior feature.

operator-del-cause
Enables Operator Cause-IE behavior feature for Delete PDP Context Request sent to delete the last PDP Context of the PDN connection.

Usage Guidelines
This command enables or disables the Cause-IE feature for Delete PDP Context Request in GGSN.

The Cause-IE configuration for Delete PDP Context Request is given in the APN configuration and is also available in the clear subscribers CLI command. When this command is enabled, the feature will be applied to GGSN based on the APN configuration or the clear subscribers command. This command is disabled by default.
Examples

The following command enables the Cause-IE feature.

gtpc operator-del-cause
gtpc private-extension

This command includes customer-specific private extensions in GTP-C messages.

Product
GGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > GGSN Service Configuration
configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ggsn-service)#

Syntax Description

Syntax Description

gtpc private-extension { {focs | odb} access-list acl_name in disconnect-on-violation | ggsn-preservation-mode | loss-of-radio-coverage | none }
default gtpc private-extension
no gtpc private-extension {focs | ggsn-preservation-mode | loss-of-radio-coverage }

default
Sets the default mode for GTP-C messages. By default it is disabled.

no
Disables the configured private extensions for GTP-C messages.

{focs | odb} access-list acl_name in disconnect-on-violation

Configures the Free-Of-Charge-Service (FOCS) and Operator Determined Barring (ODB) extensions for all packet-oriented services as defined by operators.

focs: Enables or disables Free of Charge Services for the subscriber who has no credit, and also takes the access-list acl_name to be applied for FOCS.

odb: Enables or disables "all packet oriented service barred" for the subscriber, and also takes the access-list acl_name to be applied for ODB.

acl_name is the name of a configured access control list (ACL) for this service.

Important
These are the customer-specific keywords and need customer-specific license to use them.
**ggsn-preservation-mode**

Enables the processing of customer-specific private extension in Update PDP Context requests. This extension indicates whether the subscriber is active or idle, and whether RAN resources have been released. It also indicates the desired "type" of preservation mode behavior.

When **ggsn-preservation-mode** is configured, different types of accounting records are generated based on the "type" of mode. To enable the generation of different accounting records, the trigger for preservation mode must be configured for RADIUS or GTPP for that accounting protocol. If that trigger is not configured, there will be no change in the generation of accounting records.

**Important**  This is a customer-specific keyword and needs customer-specific license to use this feature.

**loss-of-radio-coverage**

Enables the protection against overcharging a subscriber due to loss of radio coverage (LORC) in a GGSN service. It also enables the system to understand the private extension for LORC) in GTP-C Update PDP Context messages from the SGSN.

**Important**  This is a license enabled keyword and need feature-specific license to use it.

**none**

Removes the private extensions from record which are from GTP-C messages received from the SGSN.

**Usage Guidelines**

Use this command to configure the processing of private extensions within GTP-C messages received from the SGSN. It also configures the customer specific features, such as preservation mode for GGSN service. Overcharging protection (LORC) is a solution which provides the ability to accurately bill customers.

This implementation is based on Cisco-specific private extension to GTP messages and/or any co-relation of G-CDRs and S-CDRs. It also does not modify any RANAP messages.

**Important**  This is a license enabled command that requires installation of feature-specific licenses to use this command.

**Examples**

The following command configures the GGSN service to record the private extension for protecting the subscribers from overcharging during loss of radio coverage:

```
gtpc private-extension loss-of-radio-coverage
```
gtpc ran-procedure-ready-delay

This command configures the GGSN to enable the RAN Procedure Ready feature for the particular GGSN service and specify the timeout period for the RAN procedure timer in the GGSN. This timer starts on arrival of every secondary Create PDP Context request.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-ggsn-service)#
```

**Syntax Description**

```
gtpc ran-procedure-ready-delay [ timeout dur ]
{ default | no } gtpc ran-procedure-ready-delay
```

- **default**
  Sets the default mode of RAN Procedure Ready feature for this GGSN service. By default it is disabled.

- **no**
  Disables the RAN Procedure Ready feature for this GGSN service. By default it is disabled.

- **timeout dur**
  Default: 10
  Specifies the timeout duration (in seconds) for the RAN procedure timer. This timer starts on the arrival of every secondary "Create PDP Context Request" message.

  This is an optional keyword. If no timeout period is specified, the default value is 10 seconds.

  `dur` must be an integer from 1 through 40.

**Usage Guidelines**

Use this command to enable the RAN Procedure Ready feature for this GGSN service and specify the timeout period for the RAN procedure timer. This timer starts on the arrival of every secondary "Create PDP Context Request" message.
The GGSN waits until the Radio Access Bearer setup is completed and "Update PDP Context Request" is sent by the SGSN. If any downlink data is received before arrival of the "Update PDP Context Request" or before timer expiry, the downlink packets will be queued or buffered.

If the buffer becomes full (total buffer limit is of 1024 packets), all newly arriving packets are dropped.

The RAN Procedure Ready feature supports the following scenarios when RAB setup timer starts at the GGSN:

- If the GGSN receives the "Update PDP Context Request" before timer expiry, the GGSN stops the timer, sends all the queued/buffered packets in 'first-in first-out' manner and disables buffering of subsequent downlink data.

- If the GGSN receives the "Update PDP Context Request" before the timer expires, it processes the "Update PDP Context Request" as usual, but does not disable the buffering of downlink data. It then waits for another "Update PDP Context Request" to come with the RAN Procedure Ready set, or waits for timer to expire.

- If the GGSN does not receive the "Update PDP Context Request" with RAN Procedure Ready set before timer expiry, the timer is fired and the GGSN starts sending all queued packets and disables buffering of subsequent downlink data (assuming that the corresponding SGSN does not support this feature).

- If the timer has expired and the GGSN receives an "Update PDP Context Request" for a secondary PDP context with or without RAN Procedure Ready bit set, the UPC will be processed normally without buffering the packets.

---

**Important**

This feature does not affect the Enhanced Charging Service or deep packet inspection (DPI) since the buffering of downlink data is done before sending it to an ACSMgr.

---

**Important**

During an SGSN handoff scenario all packets are processed normally and the downlink packets are buffered until the timer expires.

---

**Examples**

The following command configures the GGSN service to enable the RAN Procedure Ready feature and specify the timeout period as 20 seconds for the RAN Procedure timer in GGSN:

```
gtpc ran-procedure-ready-delay timeout 20
```
gtpc support-access-side

This command allows MS to change QoS parameters when Bearer Control Mode (BCM) is set as mixed for Gn-Gp GGSN.

Important
This is a customer-specific implementation to meet the 3GPP TS 23.060 (Rel 11) Section 9.2 compliance requirements. For more information please contact your Cisco account representative.

Product
GGSN

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

Syntax Description
[ default | no ] gtpc support-access-side { traffic-class { downgrade } }

default
Restores the default setting. That is, for Gn-Gp GGSN, the MS will not be allowed to change the QCI when BCM is set as mixed.

no
Disables the configuration.

support-access-side
Allows the MS to change the QoS for Gn-Gp GGSN when BCM is mixed. This functionality is disabled by default.

traffic-class
Allows Traffic Class to be changed by the MS for Gn-Gp GGSN when BCM is set as mixed. This functionality is disabled by default.

downgrade
Allows Traffic Class to be downgraded by the MS for Gn-Gp GGSN when BCM is set as mixed. This functionality is disabled by default.
Usage Guidelines

Use this command to allow MS to change QoS parameters when BCM is set as mixed for Gn-Gp GGSN.

Examples

The following example disables the configuration:

```
no gtpc support-access-side traffic-class downgrade
```
**gtpc support-earp**

Enables Evolved ARP (e-ARP) support for GGSN service on Gn-Gp interface.

**Product**
GGSN

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

**Syntax Description**

```
[default | no] gtpc support-earp
```

- **no**
  Ignores E-ARP IE received in CPC/UPC Messages.

- **default**
  Sets the E-ARP support behavior to default, or disables the support.

**Usage Guidelines**
This command enables Evolved ARP support for GGSN service on Gn-Gp interface. Changing E-ARP support for GGSN service can impact existing bearers. By default E-ARP support is disabled.

**Caution**
Changing the E-ARP support status from "disable" (default) to "enable" will have less or no impact on existing calls; whereas, changing the E-ARP support status from "enable" to "disable" will have more impact on existing calls.

**Examples**
The following example disables the e-ARP support:
```
default gtpc support-earp
```
gtpc suppress-nrupc

This command helps enabling as well as disabling the NRUPC suppression.

Product
GGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

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

Syntax Description
| no | gtpc suppress-nrupc { cpc | upc } { qos-change }

no
Disables the NRUPC suppression.

Usage Guidelines
This command is used to enable or disable the NRUPC suppression caused by QoS change. NRUPC initiated by GGSN/P-GW is not responded to by the SGSNs of some vendors where behavior of SGSN is not compliant to standards. To accommodate SGSN non-compliance, the GGSN/P-GW software has been enhanced with CLI-controlled behavior to suppress sending of the GGSN/P-GW-initiated UPC only if SGSN requested values are less than PCRF authorized bit rates and if the values of the "No QoS Negotiation" and "Upgrade QoS Supported" flags received in the SGSN-initiated Update Request does not allow change/upgrade in QoS values in Update Response. By default, this behavior is disabled and it should be enabled if interoperability issues are seen with the SGSN.

When SGSN informs GGSN that, for a transaction either for Create PDP context Request or Update PDP Context Request, it(SGSN) does not support QoS-Upgrade and/or QoS-Negotiation, and if GGSN has to modify(either upgrade or degrade), QoS, then GGSN sends SGSN a response with unchanged QoS. Followed by the response, GGSN initiates a NRUPC with modified QoS. This is NRUPC for QoS-Change. To honor common flags suppress NRUPC CLIs are introduced.

This command suppress NRUPC (for qos-change) sent from GGSN to SGSN under following condition:

- When SGSN sends Create PDP Context Request with UQS=0. If Upgrade QoS Supported bit of the Common Flags IE is set to 0 or the Common Flags IE is absent then the SGSN does not support QoS upgrade in Response message functionality.
- When SGSN sends Update PDP Context Request with NQN flag = 1.
• When SGSN sends Update PDP Context Request QoS Update Support flag = 0

This suppression feature works with a limited functionality as follows:

• It works only on MBR and def-eps-qos.
• It holds if MBR in CPC/ UPC Request < AMBR authorized by (PCRF/MME).
• AMBR is not related to common flags hence no suppression on modification of AMBR.
• It doesn't hold if MBR in CPC/ UPC Request > AMBR authorized by (PCRF/MME). NRUPC will be generated to equalize the value of MBR to AMBR.

Examples

The following example disables the NRUPC suppression using "upc" as GTP procedure:

```plaintext
no gtpc suppress-nrupc upc qos-change
```
gtpu echo-interval

This command is obsolete and now available for configuration in GTP-U service configuration mode.
guard-interval

Configures the time period after which a redundant PDP context request received from an SGSN is treated as a new request rather than a re-send of a previous request.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

\[(context_name)host_name(config-ggsn-service)\#

**Syntax Description**

- `guard-interval guard_time`
  - `{ default | no } guard-interval`

  **default**
  
  Restores the GGSN guard-interval parameter to its default setting of 100.

  **no**
  
  Disables the guard-interval function for the GGSN service.

  **guard_time**
  
  Default: 100
  
  Specifies the amount of time that must pass before a GGSN service treats a redundant PDP context request as a new request instead of a re-send of a previous request.
  
  `guard_time` is measured in seconds and can be configured to an integer from 10 through 3600.

**Usage Guidelines**

The guard interval is used to protect against replay attacks. Without a guard interval configured, information from a valid PDP context request could be used to gain un-authorized network access.

If the GGSN service receives a PDP context request in which the International Mobile Subscriber Identity (IMSI), the Network Service Access Point Identifier (NSAPI), the end user IP address, and the GTP sequence number are identical to those received in a previous request, the GGSN treats the new request as a re-send of the original. Therefore, information from a valid PDP context request could be collected and re-sent at a later time by an un-authorized user to gain network access.
Configuring a guard interval limits the amount of time that the information contained within a PDP context request remains valid.

**Examples**

The following command configures the GGSN service with a guard interval of 60 seconds:

```
guard-interval 60
```
ip local-port

Configures the local User Datagram Protocol (UDP) port for the Gn interfaces' GTP-C socket for GTPv1.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration
```
configure > context context_name > ggsn-service service_name
```
Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-ggsn-service)#
```

**Syntax Description**
```
ip local-port gtpc-v1 port_number
```
```
default ip local-port gtpc-v1
```
```
default
```
Default

Configures the default value for the local UDP port for GTP Version 1 control messaging for this GGSN service.

```
gtpc-v1 port_number
```
Default: 2123

Specifies the UDP port number for GTPv1 GTPC sockets.

`port_number` can be configured to an integer from 1 through 65535.

**Usage Guidelines**
By default, the GGSN service attempts to use GTPv1 when communicating with SGSNs. This parameter configures the UDP port over which the GTP control (GTP-C) sockets are sent.

If an SGSN only supports GTPv0, the GGSN service automatically switches to GTPv0 when communicating with this SGSN. In the scenario, the GGSN service communicates with the SGSN on UDP port 3386 and does not have a GTP-C socket.

**Important**
The UDP port setting on the SGSN must match the local-port setting for the GGSN service on the system in order for the two devices to communicate.
Examples

The following command configures the GGSN service to use UDP port 2500 for exchanging GTPC sockets with SGSNs when using GTPv1:

```
ip local-port gtpc-v1 2500
```
**ip qos-dscp**

Configures the quality of service (QoS) differentiated service code point (DSCP) used when sending data packets over the Gn interface.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

\[context_name\]host_name(config-ggsn-service)#

**Syntax Description**

```
ip qos-dscp \{ gtpc dscp \{ 1|2|3|4|9 dscp \} | qci \{ 1|2|3|4|9 dscp \} \} +
default ip qos-dscp
no ip qos-dscp \{ gtpc | qci \{ 1|2|3|4|9 \} | qci \{ 5|6|7|8 \} allocation-retention-priority \{ 1|2|3 \} \} +
```

default

Restores the GGSN IP parameters to the default settings.

Default GTP-C DSCP: be

Default QCI/DSCP:

- 1: ef
- 2: ef
- 3: af11
- 4: af11
- 5: ef
- 6: ef
- 7: af21
- 8: af21
- 9: be
no
Removes a specified QoS setting and returns it to its default setting.

gtpc
Configures the DSCP marking to be used for GTP-C messages. Must be followed by a DSCP marking.
Default GTP-C DSCP: be

dscp
Specifies the DSCP for the specified traffic pattern. dscp can be configured to any one of the following:

- **af11**: Assured Forwarding 11 per-hop-behavior (PHB)
- **af12**: Assured Forwarding 12 PHB
- **af13**: Assured Forwarding 13 PHB
- **af21**: Assured Forwarding 21 PHB
- **af22**: Assured Forwarding 22 PHB
- **af23**: Assured Forwarding 23 PHB
- **af31**: Assured Forwarding 31 PHB
- **af32**: Assured Forwarding 32 PHB
- **af33**: Assured Forwarding 33 PHB
- **af41**: Assured Forwarding 41 PHB
- **af42**: Assured Forwarding 42 PHB
- **af43**: Assured Forwarding 43 PHB
- **be**: Best effort forwarding PHB
- **ef**: Expedited forwarding PHB

qci { 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 }
Configures the QoS Class Identifier (QCI) attribute of QoS. Here the QCI value is the QCI for which the negotiate limit is being set; it ranges from 1 to 9.

allocation-retention-priority { 1 | 2 | 3 }
Specifies the DSCP for interactive class if the allocation priority is present in the QoS profile. Priority can be the integer 1, 2, or 3.

DSCP values use the following matrix to map based on traffic handling priority and allocation retention priority if the allocation priority is present in the QoS profile.

The following table shows the DSCP value matrix for allocation-retention-priority.
**Table 1: Default DSCP Value Matrix**

<table>
<thead>
<tr>
<th>Allocation Priority</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Handling Priority</td>
<td>ef</td>
<td>ef</td>
<td>ef</td>
</tr>
<tr>
<td>1</td>
<td>ef</td>
<td>ef</td>
<td>ef</td>
</tr>
<tr>
<td>2</td>
<td>ef</td>
<td>ef</td>
<td>ef</td>
</tr>
<tr>
<td>3</td>
<td>af21</td>
<td>af21</td>
<td>af21</td>
</tr>
<tr>
<td></td>
<td>af21</td>
<td>af21</td>
<td>af21</td>
</tr>
</tbody>
</table>

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

**Usage Guidelines**

DSCP levels can be assigned to specific traffic patterns in order to ensure that data packets are delivered according to the precedence with which they are tagged. The diffserv markings are applied to the outer IP header of every GTP data packet. The diffserv marking of the inner IP header is not modified.

The traffic patterns are defined by QCI (1 to 9). Data packets falling under the category of each of the traffic patterns are tagged with a DSCP that further indicate their precedence as shown in the following tables:

**Table 2: Class structure for assured forwarding (af) levels**

<table>
<thead>
<tr>
<th>Drop Precedence</th>
<th>Class 1</th>
<th>Class 2</th>
<th>Class 3</th>
<th>Class 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>af11</td>
<td>af21</td>
<td>af31</td>
<td>af41</td>
</tr>
<tr>
<td>Medium</td>
<td>af12</td>
<td>af22</td>
<td>af32</td>
<td>af41</td>
</tr>
<tr>
<td>High</td>
<td>af13</td>
<td>af23</td>
<td>af33</td>
<td>af43</td>
</tr>
</tbody>
</table>

**Table 3: DSCP Precedence**

<table>
<thead>
<tr>
<th>Precedence (low to high)</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Best Effort (be)</td>
</tr>
<tr>
<td>1</td>
<td>Class 1</td>
</tr>
<tr>
<td>2</td>
<td>Class 2</td>
</tr>
<tr>
<td>3</td>
<td>Class 3</td>
</tr>
<tr>
<td>4</td>
<td>Class 4</td>
</tr>
</tbody>
</table>
The DSCP level can be configured for multiple traffic patterns within a single instance of this command. The **no ip qos-dscp** command can be issued to remove a QoS setting and return it to its default setting.

**Examples**

The following command configures the DSCP level for QCI to be Expedited Forwarding, ef:

```
ip qos-dscp qci 1 ef
```
max-contexts

Configures the maximum Primary, Secondary per Primary, and PPP context limits for the GGSN service.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

`configure > context context_name > ggsn-service service_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ggsn-service)#`

**Syntax Description**

```
max-contexts { max-primary max_pri_number | max-sec-per-primary max_sec_number | ppp-pdp-contexts context_number } +
default max-contexts
```

`default`

Configures the default value for maximum contexts for the GGSN service.

`max-primary max_pri_number`

Configures maximum primary PDP context allowed for this service. This includes PPP contexts also.

`max_pri_number` can be configured to an integer from 0 through 120000.

`max-sec-per-primary max_sec_number`

Default: 10

Indicates the maximum number of times that GTP control packets are retransmitted.

`max_sec_number` can be configured to an integer from 0 through 10.

`ppp-pdp-contexts context_number`

Configures maximum PPP pdp context allowed for this service.

`context_number` can be configured to an integer from 0 through 120000.

`+`

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

Usage Guidelines  This command is used to limit the number of primary contexts including PPP contexts, number of secondary contexts per primary context, and PPP contexts per GGSN service.

Examples  The following command configures the limits for primary, secondary contexts per primary, as well as the PPP contexts for a GGSN service:

```
max-contexts max-primary 40000 max-sec-per-primary 10 ppp-pdp-contexts 50000
```
max-retransmissions

Configures the maximum number of times that GTP control packets are retransmitted to an SGSN before it marks it unreachable.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
<context_name>@host_name(config-ggsn-service)#
```

**Syntax Description**

```
max-retransmissions max_number
default max-retransmissions
```

**default**

Restores the GGSN max-retransmissions parameter to its default setting of 4.

**max_number**

Default: 4

Indicates the maximum number of times that GTP control packets are retransmitted.

max_number can be configured to an integer from 0 through 15.

**Usage Guidelines**

This command is used in conjunction with the timeout command to control the retransmission of GTP control packets when no response is received from an SGSN. It is equivalent to the N3-REQUESTS parameter discussed in 3GPP TS 29.060.

If no response is received from the SGSN prior to the expiration of the timeout value, the GTP control packets are re-sent by the GGSN. This process occurs as many times as allowed by the configuration of this command.

If the max-retransmissions value is exceeded, the GGSN records a "Path Failure" for that SGSN and releases all PDP contexts associated with it.

**Examples**

The following command configures the maximum number of retransmissions to 8:

```
max-retransmissions 8
```
mbms policy

This command enables/disables the Multimedia Broadcast Multicast Services (MBMS) user service support for multicast and/or broadcast mode. It also specifies the policy for MBMS user service mode.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-ggsn-service)#

**Syntax Description**
mbms policy { multicast broadcast | none }

{ default | no } mbms policy

default
Restores the default mode of MBMS support in this GGSN service.

no
Removes or disables the configured MBMS support for multicast and/or broadcast mode in this GGSN service.

multicast broadcast
Enables the MBMS support and configures the policy for multicast and broadcast of user service.

none
Disables MBMS user service support.

**Usage Guidelines**
Use this command to enable/disable the MBMS user service support for Multicast and/or Broadcast mode. It also specifies the policy for MBMS user service mode.

**Examples**
The following command enables MBMS support in this GGSN service:

mbms policy multicast broadcast
newcall

This command enables or disables the new call related behavior of this GGSN service when duplicate sessions with the same IP address request are received. This feature is required to support interworking with P-GW and HA.

Product
GGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

(context_name) host_name(config-ggsn-service)#

Syntax Description
newcall | duplicate-subscriber-requested-address { accept | reject } |
duplicate-subscriber-requested-v6-address { accept | reject } |
default newcall | duplicate-subscriber-requested-address | duplicate-subscriber-requested-v6-address |
{ accept | reject } |

default
Restores the default mode for new call session with the same address request received in this GGSN service. It rejects calls with duplicate address requests.

duplicate-subscriber-requested-address
Configures how duplicate sessions with same IP address request are handled.

duplicate-subscriber-requested-v6-address
Configures how duplicate sessions with same IPv6 address request are handled.

accept
Sets the system to "accept" another session using the same IP address for a new call. The new session will be created and the old session will be torn down.
Default: Disabled
reject

Rejects new calls with duplicate address requests. This is the default behavior.

Default: Enabled

Usage Guidelines

Use this command to enable or disable new call connections when the UE is not able to gracefully disconnect from the Enterprise PDN before attempting to reconnect via another access method. When enabled this command tears down the old session in order to accept the new connection with the same IP or IPv6 address assignment.

This feature also allows the GGSN to accept a request for a static subscriber address, even if the address is already used by another session. If this feature is not enabled, a new request with the same IP address for another session will be rejected.

Important

This command is a license-enabled feature.

Examples

The following command allows the GGSN to accept the duplicate call session request with the same IP address:

newcall duplicate-subscriber-requested-address accept
**path-failure**

Determines the GTP path-failure behavior on echo/non-echo messages.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```bash
configure context context_name ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```bash
[context_name]host_name(config-ggsn-service)#
```

**Syntax Description**

```bash
path-failure detection-policy gtp { echo | non-echo } | non-echo | echo }
{ no | default } path-failure detection-policy
```

- **no**
  
  No defined detection policy means path-failures are not detected.

- **default**

  Sets the path-failure detection-policy to GTP in echo mode.

  ```bash
detection-policy gtp {echo | non-echo } | non-echo | echo }
```

Detection-policy is the policy to be used when path-failure is in active state. GTP messages are either gtp(u) (user) or gtp(c) (control) type, and the gtp keyword takes either echo or non-echo as message type.

- **echo**
  gtp(u) or gtp(c) message.

- **non-echo**
  a message type other than gtp(u) or gtp(c).

**Usage Guidelines**

Under current circumstances, a GGSN shuts down the GTP tunnel if the associated SGSN does not respond to multiple retries of an echo or non-echo message from the GGSN. In this way, a single call failure could be responsible for the loss of all active calls in the tunnel.

This is also an issue when echo is disabled, or when there is very little traffic on the SGSN and the GGSN is configured with large echo intervals.

This behavior adversely impacts the user experience because the customer has to reconnect every time this happens with their SGSN.
The following example detects path failures when the SGSN fails to respond to multiple echo message retries:

```
pool-failure detection-policy gtp echo
```

The following example turns off path-failure detection. On timeout of gtp(c) message retries, the particular context will be purged:

```
no path-failure detection-policy
```
plmn id

Configures the GGSN's Public Land Mobile Network (PLMN) identifiers used to determine if a mobile station is visiting, roaming, or belongs to a network. Up to 512 PLMN IDs can be configured for each GGSN service.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

`configure > context context_name > ggsn-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax Description**

```
plmn id mcc mcc_value | mnc mnc_value | | primary |
no plmn id mcc mcc_value | mnc mnc_value |
```

**no**

Removes a previously configured PLMN identifier for the GGSN service.

**mcc mcc_value**

Specifies the mobile country code (MCC) portion of the PLMN's identifier.

`mcc_value` is the PLMN MCC identifier and can be configured to an integer between 100 and 999.

**mnc mnc_value**

Specifies the mobile network code (MNC) portion of the PLMN's identifier. This option is optional.

`mnc_value` is the PLMN MNC identifier and can be configured to any 2- or 3-digit integer from 00 through 999.

**primary**

When multiple PLMN IDs are configured, the `primary` keyword can be used to designate one of the PLMN IDs to be used for the AAA attribute (3GPP-GGSN-MCC-MNC).
Usage Guidelines

The PLMN identifier is used by the GGSN service to determine whether or not a mobile station is visiting, roaming, or home. Multiple GGSN services can be configured with the same PLMN identifier. Up to 512 PLMN IDs can be configured for each GGSN Service.

Important

The number of supported PLMN IDs was increased from 5 to 512 in StarOS Release 17.1. In addition, the MNC portion of the PLMN ID became optional.

If the MNC portion of a PLMN ID is not specified, home PLMN qualification will be done based solely on the MCC value and the MNC portion will be ignored for these particular MCCs.

Examples

The following command configures the PLMN identifier with an MCC of 462 and MNC of 2:

```
plmn id mcc 462 mnc 02
```
plmn unlisted-sgsn

Configures the GGSN's policy for handling communications from SGSNs with which it is not configured to communicate.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

`configure > context context_name > ggsn-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax Description**
```
plmn unlisted-sgsn [ foreign | disable-gtpc-echo | rat-type { GAN | GERAN | HSPA | UTRAN | WLAN } | reject-foreign-subscriber ] | home [ foreign | disable-gtpc-echo | rat-type { GAN | GERAN | HSPA | UTRAN | WLAN } ] | mcc mcc_value mnc mnc_value | disable-gtpc-echo | rat-type { GAN | GERAN | HSPA | UTRAN | WLAN } | reject-foreign-subscriber ] | reject ]
default plmn unlisted-sgsn
```

default
Resets configured parameters to their default settings.

**foreign**
Default: Disabled

Specifies that the GGSN service accepts messages from SGSNs that are not configured within the service using the `sgsn address` command.

This keyword also dictates that unlisted SGSNs are treated as if they belong to a foreign PLMN. Therefore, PDP contexts originating from them are treated as visiting or roaming.

**home**
Default: Disabled

Specifies that the GGSN service accepts messages from SGSNs that are not configured within the service using the `sgsn address` command.

This keyword also dictates that unlisted SGSNs are treated as if they belong to the GGSN service's home PLMN.
**mcc mcc_value**
Specifies the mobile country code (MCC) portion of the PLMN's identifier. 
*mcc_value* is the PLMN MCC identifier and can be configured to an integer from 100 through 999.

**mnc mnc_value**
Specifies the mobile network code (MNC) portion of the PLMN's identifier. 
*mnc_value* is the PLMN MNC identifier and can be configured to a 2- or 3-digit integer from 00 through 999.

**reject**
Default: Enabled
Specifies that the GGSN service rejects messages from SGSNs that are not configured within the service using the *sgsn address* command.
When the GGSN service rejects the message(s), it returns a cause code of No Resources 199 (C7H, No resources available).

**disable-gtpc-echo**
Default: Send GTPC Echo messages to unlisted SGSNs.
When this keyword is specified, GTPC echo messages are not sent to unlisted SGSNs.

**rat-type { GAN | GERAN | HSPA | UTRAN | WLAN }**
This keyword configures the type of radio access technology.
GERAN: Specifies the GSM EDGE Radio Access Network type of RAT.
HSPA: Specifies the High Speed Packet Access type of RAT.
UTRAN: Specifies the UMTS Terrestrial Radio Access Network type of RAT.
WLAN: Specifies the Wireless Local Access Network type of RAT.

**reject-foreign-subscriber**
Default: Disabled
Specifies that incoming calls from foreign subscribers are rejected.

**Usage Guidelines**
This command works in conjunction with the *sgsn* command that configures the GGSN service to communicate with specific SGSNs. Any messages received from SGSNs not configured in that list are subject to the rules dictated by the *unlisted-sgsn* policy.

**Examples**
The following command configures the GGSN service to accept messages from unlisted SGSNs and treat the SGSN as if it is on the GGSN's home network:

`plmn unlisted-sgsn home`
policy

Specifies the reject code to be used in the "Create PDP Context" response message when a RADIUS server timeouts.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ggsn-service)#

Syntax Description

policy { accounting-server-timeout use-reject-code \{ system-failure | no-resources \} | authentication-server-timeout use-reject-code \{ system-failure | user-authentication-failure \} }
default policy { authentication-server-timeout | accounting-server-timeout }

default

Restores the specified parameter to its default setting.

accounting-server-timeout use-reject-code \{ system-failure | no-resources \}

Default: no-resources

Specifies the reject code used by the GGSN if communication with an accounting server times out. The possible reject codes are:

- system-failure (204 (CCH))
- no-resources (199 (C7H))

authentication-server-timeout use-reject-code \{ system-failure | user-authentication-failure \}

Default: user-authentication-failure

Specifies the reject code used by the GGSN if communication with an authentication server times out. The possible reject codes are:

- system-failure (204 (CCH))
- user-authentication-failure (209 (D1H))

Command Line Interface Reference, Modes G - H, StarOS Release 19
Usage Guidelines  
This command is used to configure the cause code used by the GGSN if communication with either a RADIUS authentication or accounting server times out.

When this parameter is used in conjunction with Radius accounting servers, the response is only set if a flag is configured in the APN Delay GTP Response, only after getting a response to the Accounting Start.

Examples  
The following command configures the GGSN response to a RADIUS authentication server timeout to be system-failure:

```
policy authentication-server-timeout use-reject-code system-failure
```
retransmission-timeout

Configures the timeout period in between retransmissions of GTP control packets. This timeout configuration is not applicable on Echo Request retransmission.

| Important | In 17.3 and later releases, this command has been deprecated. |

Product GGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

\[(context_name)host_name(config-ggsn-service)#\]

Syntax Description retransmission-timeout retransmit_time
default retransmission-timeout
default

Configures the default time interval that must pass without an SGSN response before the GGSN service retransmits GTP control packets.

retransmit_time

Default: 5

Specifies the amount of time that must pass without an SGSN response before the GGSN service retransmits GTP control packets.

retransmit_time is measured in seconds and can be configured to an integer from 1 through 20.

Usage Guidelines This command is used in conjunction with the **max-retransmissions** command to control the retransmission of GTP control packets when no response is received from an SGSN.

If no response is received from the SGSN prior to the expiration of the timeout value, the GTP control packets are re-sent by the GGSN. This process occurs as many times as allowed by the configuration of the **max-retransmissions** command.
If the max-retransmissions value is exceeded within the retransmission-timeout period, the GGSN records a "Path Failure" for that SGSN and releases all PDP contexts associated with it.

**Important**
This retransmission timeout configuration is not applicable for Echo Requests message retransmission. Echo are sent/retransmitted every echo interval, which can be configured separately.

**Examples**
The following command configures a timeout value of 20 seconds:

```plaintext
retransmission-timeout 20
```
retransmission-timeout-ms

Configures the timeout period in between retransmissions of GTP control packets. This timeout configuration is not applicable on Echo Request retransmission.

Product

GGSN

Privilege

privilege

Command Modes

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-ggsn-service)#

Syntax Description

retransmission-timeout-ms retransmit_time
default retransmission-timeout-ms

default

Configures the default time interval that must pass without an SGSN response before the GGSN service retransmits GTP control packets.

retransmit_time

Default: 5000

Specifies the amount of time that must pass without an SGSN response before the GGSN service retransmits GTP control packets.

retransmit_time is measured in milliseconds and can be configured to an integer from 1000 through 20000, with a granularity of 100 milliseconds.

Usage Guidelines

This command is used in conjunction with the max-retransmissions command to control the retransmission of GTP control packets when no response is received from an SGSN.

If no response is received from the SGSN prior to the expiration of the timeout value, the GTP control packets are re-sent by the GGSN. This process occurs as many times as allowed by the configuration of the max-retransmissions command.

If the max-retransmissions value is exceeded within the retransmission-timeout period, the GGSN records a "Path Failure" for that SGSN and releases all PDP contexts associated with it.
This retransmission timeout configuration is not applicable for Echo Requests message retransmission. Echo are sent/retransmitted every echo interval, which can be configured separately.

Examples

The following command configures a timeout value of 2000 milliseconds:

gerestransmission-timeout-ms 2000
setup-timeout

Configures the maximum amount of time the GGSN service allows for the setting up of PDP contexts.

Product
GGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ggsn-service)#

Syntax Description

setup-timeout setup_time
default setup-timeout

default
Restores the command to its default setting of 60.

setup_time
Default: 60
Specifies the maximum amount of time the GGSN service allows for the setting up of PDP contexts. setup_time is measured in seconds and can be configured to an integer from 1 through 6000.

Usage Guidelines
Use this command to limit the amount of time allowed for setting up PDP contexts. If the PDP context is not setup within the configured time frame, the GGSN service rejects the PDP context with a cause code of 199 (C7H, No resources available).

Examples
The following command allows a maximum of 120 seconds for the setting up of PDP contexts:

setup-timeout 120
sgsn address

Configures the SGSNs that this GGSN service is allowed to communicate with.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```
configure > context context_name > ggsn-service service_name
```

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

**Syntax Description**
```
sgsn address {ipv4/ipv6_address | ipv4/ipv6_address/netmask} | plmn-foreign | reject-foreign-subscriber
| mcc mcc_code mnc mnc_code | reject-foreign-subscriber | rat-type {GAN | GERAN | HSPA | UTRAN | WLAN} | description description | disable-gtpc-echo
no sgsn address {ipv4/ipv6_address | ipv4/ipv6_address/netmask}
```

**no**
Removes a specific SGSN from the list or all configured SGSNs.

**address**
Configures the IP address of the SGSN.

*ipv4/ipv6_address* must be specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation and can be followed by the subnetmask of the address.

**plmn-foreign**
Indicates whether or not the SGSN belongs to a foreign public land mobile network (PLMN).

**reject-foreign-subscriber**
Default: Disabled
Specifies that incoming calls from foreign subscribers are rejected.

**mcc mcc_code**
Specifies the mobile country code (MCC) portion of the PLMN's identifier.
mcc_code is the PLMN MCC identifier and configured as an integer from 100 through 999.

mnc mnc_code
Specifies the mobile network code (MNC) portion of the PLMN's identifier.
mnc_code is the PLMN MNC identifier and configured as a 2- or 3-digit integer from 00 through 999.

rat-type {GAN | GERAN | HSPA | UTRAN | WLAN }
This keyword configures the type of radio access technology.
GERAN: Specifies the GSM EDGE Radio Access Network type of RAT.
HSPA: Specifies the High Speed Packet Access type of RAT.
UTRAN: Specifies the UMTS Terrestrial Radio Access Network type of RAT.
WLAN: Specifies the Wireless Local Access Network type of RAT.

description description
Add description field to the SGSN entry in GGSN service.
description is an alphanumeric string of 1 through 63 characters.

disable-gtpc-echo
Default: Send GTPC Echo messages to unlisted SGSNs.
When this keyword is specified, GTPC echo messages are not sent to unlisted SGSNs.

Usage Guidelines
Use this command to configure a list of SGSNs that the GGSN service is to communicate with. This command can be entered multiple times to configure multiple SGSNs.

Important
The GGSN only communicates with the SGSNs configured using this command unless a plmn-policy is enabled to allow communication with unconfigured SGSNs. PLMN policies are configured using the plmn unlisted-sgsn command.

Examples
The following command configures the GGSN to communicate with an SGSN on a foreign PLMN with an IP address of 192.168.1.100:
sgsn address 192.168.1.100 plmn-foreign
sgsn define-multiple-address-group

This command defines an SGSN Multiple Address Group and enters SGSN Multiple Address Group Configuration mode. Whenever there is a change in the control address in a GTPC UPC message, it is treated as an inter-SGSN handoff because an SGSN is usually identified uniquely by a single IP-address. This command supports a multiple address group feature which allows you to specify a set of addresses that specify a single SGSN. When a UPC handoff is received from any address in the group, it is treated as an intra-SGSN handoff.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ggsn-service)#

Syntax Description

sgsn define-multiple-address-group grp_name [-noconfirm]

no sgsn define-multiple-address-group grp_name

no

Removes a specific SGSN Multiple Address Group from the list GGSN service configuration.

grp_name

Specifies the name of an SGSN multiple address group to create or configure.

 grp_name is an alphanumeric string from 1 through 63 characters.

-noconfirm

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

Usage Guidelines

Use this command to create or configure an SGSN Multiple Address Group that the GGSN service is to communicate with. This command can be entered multiple times to configure multiple SGSN Multiple Address Groups.
Examples

The following command creates an SGSN Multiple Address Group named `sgsngrp1` and enters SGSN Multiple Address Group Configuration mode:

```
sgsn define-multiple-address-group sgsngrp1
```
**sgsn multiple-address-group**

Configures the SGSN multiple address groups that this GGSN service is allowed to communicate with.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```plaintext
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```plaintext
[context_name]host_name(config-ggsn-service)#
```

**Syntax Description**

```plaintext
sgsn multiple-address-group grp_name [ disable-gtpc-echo ] [ mcc mcc_code mnc mnc_code [ reject-foreign-subscriber ] ] [ plmn-foreign [ reject-foreign-subscriber ] [ rat-type { GAN | GERAN | HSPA | UTRAN | WLAN } ] [ description description ]
no sgsn multiple-address-group grp_name
```

**no**

Removes a specific SGSN multiple address group from the list of configured SGSN multiple address groups.

**grp_name**

Specifies the name of a configured SGSN multiple address group to use.

**disable-gtpc-echo**

Default: Send GTPC Echo messages to unlisted SGSNs.

When this keyword is specified, GTPC echo messages are not sent to unlisted SGSNs.

**plmn-foreign**

Indicates whether or not the SGSN multiple address group belongs to a foreign public land mobile network (PLMN).

**reject-foreign-subscriber**

Default: Disabled

Specifies that incoming calls from foreign subscribers are rejected.
**mcc mcc_code**
Specifies the mobile country code (MCC) portion of the PLMN's identifier.
*mcc_code* is the PLMN MCC identifier and can be configured to an integer from 100 through 999.

**mnc mnc_code**
Specifies the mobile network code (MNC) portion of the PLMN's identifier.
*mnc_code* is the PLMN MNC identifier configured as a 2- or 3-digit integer from 00 through 999.

**rat-type { GAN | GERAN | HSPA | UTRAN | WLAN }**
This keyword configures the type of radio access technology.
GERAN: Specifies the GSM EDGE Radio Access Network type of RAT.
HSPA: Specifies the High Speed Packet Access type of RAT.
UTRAN: Specifies the UMTS Terrestrial Radio Access Network type of RAT.
WLAN: Specifies the Wireless Local Access Network type of RAT.

**description description**
Add a description field to the SGSN multiple address group entry in the GGSN service configuration.
*description* must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**
Use this command to configure a list of SGSN multiple address groups with which the GGSN service is to communicate. This command can be entered multiple times to configure multiple SGSN multiple address groups.

**Important**
The GGSN only communicates with the SGSN multiple address groups configured using this command unless a plmn-policy is enabled to allow communication with unconfigured SGSNs. PLMN policies are configured using the `plmn unlisted-sgsn` command.

**Examples**
The following command configures the GGSN to communicate with an SGSN with multiple address that is defined by an SGSN multiple address group named `sgsngrp1` that is on a foreign PLMN:
```
sgsn multiple-address-group sgsngrp1 plmn-foreign
```
sgsn mcc-mnc

This command configures sgsn mcc-mnc for this GGSN service.

Product  GGSN

Privilege  Security Administrator, Administrator

Command Modes  Exec > Global Configuration > Context Configuration > GGSN Service Configuration
  configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

{context_name} host_name (config-ggsn-service)#

Syntax Description  sgsn mcc-mnc { prefer-rai | prefer-uli }
  default sgsn mcc-mnc

  default
  Configures the default option for sgsn mcc-mnc. Default is 'prefer-uli'.

  prefer-rai
  Configures sgsn mcc-mnc using rai.

  prefer-uli
  Configures sgsn mcc-mnc using uli.

Usage Guidelines  Use this command to configure the sgsn mcc-mnc.

Examples  The following command configures the sgsn mcc-mnc to 'prefer-rai':
  sgsn mcc-mnc prefer-rai
trace-collection-entity

This command configures the trace collection entity IP address. Trace collection entity is the destination node to which trace files are transferred and stored.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

`configure > context context_name > ggsn-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax Description**

- `trace-collection-entity ipv4_addr`
- `no trace-collection-entity`
- `ipv4_addr`

Specifies the IP address in IPv4 dotted-decimal notation.

**Usage Guidelines**

Use this command to configure the trace collection entity IP address. This configuration is required because during signaling session trace activation, CPC REQ and UPC REQ do not provide the IP address for the trace collection entity.

**Examples**

The following command configures the trace collection entity IP address with this GGSN service:

```
trace-collection-entity 192.36.56.56
```
Global Configuration Mode Commands (A-K)

The Global Configuration Mode is used to configure basic system-wide parameters.

This section includes the commands `aaa accounting-overload-protection` through `imei-profile`.

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Important**

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

- `aaa accounting-overload-protection`, page 85
- `aaa default-domain`, page 86
- `aaa domain-matching ignore-case`, page 88
- `aaa domain-matching imsi-prefix`, page 89
- `aaa large-configuration`, page 91
- `aaa last-resort`, page 93
- `aaa tacacs+`, page 95
- `aaa username-format`, page 96
- `active-charging service`, page 98
- `alarm`, page 100
- `apn-profile`, page 101
- `apn-remap-table`, page 102
- `arp`, page 103
- autoconfirm, page 104
- autoless, page 105
- banner, page 106
- bearer-control-profile, page 108
- boot delay, page 109
- boot interface, page 110
- boot nameserver, page 112
- boot networkconfig, page 113
- boot system priority, page 115
- bulkstats, page 118
- ca-certificate, page 120
- ca-crl, page 122
- call-control-profile, page 124
- card, page 125
- card-standby-priority, page 126
- cdr-multi-mode, page 127
- certificate, page 128
- cli, page 130
- cli-encrypt-algorithm, page 133
- clock, page 135
- cmp auto-fetch, page 138
- cmp cert-store location, page 140
- cmp cert-trap time, page 142
- commandguard, page 143
- congestion-control, page 145
- congestion-control overload-disconnect, page 147
- congestion-control policy, page 149
- congestion-control threshold, page 156
- congestion-control threshold license-utilization, page 160
- congestion-control threshold max-sessions-per-service-utilization, page 162
- congestion-control threshold message-queue-utilization, page 164
- congestion-control threshold message-queue-wait-time, page 166
- congestion-control threshold mmemgr-average-cpu-utilization, page 168
• congestion-control threshold port-rx-utilization, page 170
• congestion-control threshold port-specific, page 172
• congestion-control threshold port-rx-utilization, page 174
• congestion-control threshold port-tx-utilization, page 176
• congestion-control threshold service-control-cpu-utilization, page 178
• congestion-control threshold system-cpu-utilization, page 180
• congestion-control threshold system-memory-utilization, page 182
• congestion-control threshold tolerance, page 184
• connectedapps, page 186
• content-filtering category database directory, page 187
• content-filtering category database max-versions, page 188
• content-filtering category database override, page 189
• context, page 190
• crash enable, page 192
• crypto blacklist file, page 195
• crypto peer-list, page 197
• crypto remote-secret-list, page 199
• crypto whitelist file, page 201
• cs-network, page 203
• css acsmgr-selection-attempts, page 205
• css delivery-sequence, page 206
• css service, page 207
• diameter dynamic-dictionary, page 208
• diameter-host-template, page 210
• diameter-proxy ram-disk, page 212
• ecmp-lag hash, page 213
• end, page 214
• enforce imsi-min equivalence, page 215
• exit, page 217
• fa-spi-list, page 218
• fabric egress drop-threshold, page 219
• fabric fsc-auto-recovery, page 221
• failure-handling-template, page 222
• global-title-translation address-map, page 224
• global-title-translation association, page 225
• gtpc-load-control-profile, page 226
• gtpc-overload-control-profile, page 227
• gtppcr compression-process, page 228
• gtppcr push-to-active, page 229
• gtppcr ram-disk-limit, page 231
• gtppcr single-source, page 232
• ha-spi-list, page 234
• hd raid, page 235
• hd storage-policy, page 238
• high-availability, page 240
• hybrid-mode, page 242
• imei-profile, page 243
aaa accounting-overload-protection

This command configures Overload Protection Policy for accounting requests.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```aaa accounting-overload-protection prioritize-gtpp
{ default | no } aaa accounting-overload-protection
```

**default**

Configures the default setting.

Default: no priority assigned

**no**

Disables the Overload Protection configuration.

**prioritize-gtpp**

Gives higher priority to GTPP requests among the other outstanding requests. So while purging the lower priority requests will be selected first.

**Usage Guidelines**

Use this command to configure Overload Protection Policy for accounting requests.

**Examples**

The following command prioritizes GTPP requests among the other outstanding requests:

```aaa accounting-overload-protection prioritize-gtpp```
aaa default-domain

Configure global accounting and authentication default domain for subscriber and context-level administrative user sessions.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local] `host_name (config)#`

**Syntax Description**

```
aaa default-domain { administrator | subscriber } domain_name
no aaa default-domain { administrator | subscriber }
```

- **no**
  Removes all or only the specified configured domain.

- **administrator | subscriber**
  - **administrator**: Configures the default domain for context-level administrative users.
  - **subscriber**: Configures the default domain for subscribers.

- **domain_name**
  Sets the default context.
  - `domain_name` must be an alphanumeric string of 1 through 79 characters.

**Usage Guidelines**
This command configures the default domain which is used when accounting and authentication services are required for context-level administrative user and subscriber sessions whose user name does not include a domain.
Examples

The following commands configure the default domains for context-level administrative users and subscribers, respectively:

```
aaa default-domain administrator sampleAdministratorDomain
aaa default-domain subscriber sampleSubscriberDomain
```
aaa domain-matching ignore-case

This command disables case sensitivity when performing domain matching. When this command is enabled, the system disregard case when matching domains.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]\host_name(config)#
```

**Syntax Description**

<table>
<thead>
<tr>
<th>no</th>
<th>aaa domain-matching ignore-case</th>
</tr>
</thead>
<tbody>
<tr>
<td>default aaa domain-matching</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use this command to configure the system to ignore case when matching domains.

**Examples**
The following command configures the system to ignore case when matching domains:

```
aaa domain-matching ignore-case
```
aaa domain-matching imsi-prefix

Enables domain lookup for session based on the International Mobile Subscriber Identity (IMSI) prefix length. Default: Disabled

| Important | This command is only available in 8.3 and later releases. |

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

Syntax Description

aaa domain-matching imsi-prefix prefix-length prefix_length
no aaa domain-matching imsi-prefix
default aaa domain-matching

no

Specifies the system must not consider imsi-prefix domain matching method.

prefix-length

Specifies the IMSI length to be matched with the domain.

prefix_length must be an integer from 1 through 15.

Usage Guidelines

Use this command to configure the IMSI-prefix method of domain matching. This command enables domain lookup for the session based on the IMSI prefix length. If there is a domain configured with the matching IMSI prefix, the associated configuration is used.

This feature does not support partial matches.
aaa domain-matching imsi-prefix

**Examples**

The following command configures the IMSI prefix method for domain matching setting the prefix length to 10.

```bash
aaa domain-matching imsi-prefix prefix-length 10
```
aaa large-configuration

This command enables or disables the system to accept a large number of RADIUS configurations to be defined and stored.

**Important**
For this command to take affect, after entering the command the configuration must be saved and reloaded.

When aaa large-configuration is disabled, the following restrictions are in place:

- Only one (1) NAS IP address can be defined per context with the `radius` attribute command.
- The RADIUS attribute `nas-ip-address` can only be configured if the RADIUS group is `default`.
- Only 320 RADIUS servers can be configured system-wide.
- Only 64 RADIUS groups can be configured system-wide.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
| no | aaa large-configuration
```

- `no`
  Disables AAA large configuration support.

**Usage Guidelines**
When aaa large-configuration is enabled, the system provides the ability to configure multiple NAS IP addresses in a single context to used with different radius groups. As well, the command allows support for up to 1,600 RADIUS server configurations and for a PDSN a maximum of 400 or for a GGSN a maximum of 800 RADIUS server group configurations system-wide.
Examples

To enable the definition of a large number of RADIUS configurations, enter the following commands in the following order:

In APN Configuration mode, enter:
`default aaa group`

In Global Configuration mode, enter:
`aaa large-configuration`

In Exec mode, use the `save configuration` command and then the `reload` command.
aaa last-resort

Configure global accounting and authentication last resort domain for subscriber and context-level administrative user sessions.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

aaa last-resort context { administrator | subscriber context_name }

no aaa last-resort context { administrator | subscriber }

no

Removes all or only the specified previously configured authentication last resort domain name.

administrator | subscriber

administrator: Configures the last resort domain for context-level administrative.

subscriber: Configures the last resort domain for the subscribers.

context_name

Specifies the context which is to be set as the last resort. context_name must be an alphanumeric string of 1 to 79 characters.

Usage Guidelines

Set the last resort context which is used when there is no applicable default domain (context) and there is no domain provided with the subscriber's or context-level administrative user's name for use in the AAA functions.

Examples

The following commands configure the last resort domains for context-level administrative user and subscribers, respectively:

aaa last-resort administrator sampleAdministratorDomain
aaa last-resort subscriber sampleSubscriberDomain
The following command removes the previously configured domain called *sampleAdministratorDomain*:

```bash
no aaa last-resort administrator sampleAdministratorDomain
```
aaa tacacs+

Enables or disables system-wide TACACS+ AAA (authentication, authorization and accounting) services for administrative users. This command is valid only if TACACS+ servers and related services have been configured in TACACS Configuration Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no ] aaa tacacs+
```

- **no**
  Enables or disables the use of TACACS+ AAA services for administrative users.
  Disables TACACS+ AAA authentication.

**Usage Guidelines**

```
aaa tacacs+
no aaa tacacs+
```
aaa username-format

Configure global accounting and authentication user name formats for AAA (authentication, authorization and accounting) functions. Up to six formats may be configured.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
| no | aaa username-format { domain | username } separator

default aaa username-format
```

- **no**
  Removes the specified user name format from the configuration.

- **domain | username**
  Default: username @

  - **domain**: indicates the left side of the string from the separator character is a domain name and the right side is the user name.
  - **username**: indicates the left side of the string from the separator character is a user name and the right side is the domain name.

**Important**
The user name string is always searched from right to left for the first occurrence of the separator character.

**separator**

Specifies the character to use to delimit the domain from the user name for global AAA functions. Permitted characters include: @, %, -, #, or /. To specify a back slash (\) as the separator, you must enter a double back slash (\\) on the command line.
**Usage Guidelines**

Define the formats for user name delimiting if certain domains or groups of users are to be authenticated based upon their user name versus domain name.

**Examples**

aaa username-format domain @

aaa username-format username %

no aaa username-format username %
active-charging service

This command allows you to create/configure/delete the Active Charging Service (ACS)/Enhanced Charging Service (ECS).

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
active-chargingservice acs_service_name [-noconfirm ]
no active-chargingservice acs_service_name
```

**no**
Deletes the specified Active Charging Service.

**acs_service_name**
Specifies name of the Active Charging Service.

*acs_service_name* must be the name of an Active Charging Service, and must be an alphanumeric string of 1 through 15 characters.

If the named Active Charging Service does not exist, it is created, and the CLI mode changes to the ACS Configuration Mode wherein the service can be configured. If the named Active Charging Service already exists, the CLI mode changes to the ACS Configuration Mode.

**-noconfirm**
Specifies that the command must execute without any additional prompt and confirmation from the user.

**Usage Guidelines**
Use this command to create/configure/delete an Active Charging Service in the system. Note that, in this release, only one Active Charging Service can be created in the system.

Use this command after enabling ACS using the **require active-charging** command. This command allows administrative users to configure the ACS functionality.
On entering this command, the CLI prompt changes to:

`[context_name]hostname(config-acs)#`

**Examples**

The following command creates an ACS service named *test*:

`active-charging service test`
alarm

Enables or disables alarming options for the SPIO card or the SSC internal alarms and the central-office external alarms. To verify the state of the alarms, refer to the `show alarm` command.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
| no | alarm  | audible | central-office |
```

`no`

Disables the option specified.

`audible`

Enables the internal audible alarm on ASR 5000 SPIO cards or ASR 5500 SSCs.

`central-office`

Enables the central office (external relay) alarms.

Usage Guidelines

Use this command to enable or disable audible and external relay alarms on ASR 5000 SPIO cards or ASR 5500 SSCs.

Examples

The following commands enable the audible alarms:

```
alarm audible
```
apn-profile

Creates an instance of an Access Point Name (APN) profile.

**Product**
MME
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no ] apn-profile apn_profile_name
```

- **no**
  Deletes the APN profile instance from the configuration.

- **apn_profile_name**
  Specifies the name of the APN profile. Enter an alphanumeric string of 1 through 64 characters.

**Usage Guidelines**
Use this command to create an instance of an APN profile and to enter the APN profile configuration mode. An APN profile is a template which groups a set of APN-specific commands that may be applicable to one or more APNs. See the *APN Profile Configuration Mode Commands* chapter for information regarding the definition of the rules contained within the profile and the use of the profile.

---

**Important**
An APN profile is a key element of the Operator Policy feature and is only valid when associated with at least one operator policy.

To see what APN profiles have already been created, return to the Exec mode and enter the `show apn-profile all` command.

**Examples**
The following command creates a configuration instance of an APN profile:
```
apn-profile apnprof27
```
apn-remap-table

Creates an instance of an Access Point Name (APN) remap table.

Product

MME
SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name(config) #

Syntax Description

| no | apn-remap-table apn_remap_table_name |

no

Deletes the APN remap table instance from the configuration.

apn_remap_table_name

Specifies the name of the APN remap table. Enter an alphanumeric string of 1 through 65 characters.

Usage Guidelines

Use this command to create an instance of an APN remap table and to enter the APN remap table configuration mode. An APN remap table includes entries that define how an incoming APN, or the lack on one, will be handled. See the APN Remap Table Configuration Mode Commands chapter for information regarding the definition of the entries contained within the table and the use of the table.

Important

An APN remap table is a key element of the Operator Policy feature and is only valid when associated with at least one operator policy.

To see what APN remap tables have already been created, return to the Exec mode and enter the show apn-remap-table all command.

Examples

The following command creates a configuration instance of an APN remap table:

apn-remap-table pnremap-USorigins-table1
arp

Configures a system-wide time interval for performing Address Resolution Protocol (ARP) refresh.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

ARP base-reachable-time time
default ARP base-reachable-time

default

Restores the parameter to its default setting.

time

Default: 30

Specifies the ARP refresh interval (in seconds) as an integer from 30 through 86400.

**Usage Guidelines**

Use this command to configure a system-wide ARP refresh interval. Once a neighbor is found, the entry is considered valid for at least a random value between the time/2 and the time*1.5.

**Examples**

The following command configures an ARP refresh interval of 1 hour:

arp base-reachable-time 3600
autoconfirm

This command disables or enables confirmation for certain commands. This command affects all future CLI sessions and users.

To change the behavior for the current CLI session only, use the autoconfirm command in the Exec Mode.

Important

Product

All

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config) #

Syntax Description

| no | autoconfirm

no

Disables the autoconfirm feature.

Usage Guidelines

When autoconfirm is enabled, certain commands ask you to answer yes or no to confirm that you want to execute the command. When autoconfirm is disabled the confirmation prompts never appear. Disabling autoconfirm disables command confirmation for all future CLI sessions.

By default autoconfirm is enabled.

Important

If autoconfirm is enabled, commandguard will not take effect until autoconfirm is disabled in both Exec and Global Configuration modes.

Examples

The following command enables command confirmation for all future CLI sessions and users:

autoconfirm
autoless

This command is obsolete. It is included in the CLI for backward compatibility with older configuration files. When executed, this command issues a warning and performs no function.
banner

Configures the CLI banner which is displayed upon the start of a CLI session.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

- `banner { charging-service | lawful-intercept | motd | pre-login } string`
- `no banner { charging-service | lawful-intercept | motd | pre-login }

**no**
Removes the banner message by setting it to be a string of zero length.

**charging-service**
Specifies the Active Charging Service banner message. The banner is displayed upon initialization of an SSH CLI session with ACS-admin privileges (whenever anyone with the CLI privilege bit for ACS logs on).

**lawful-intercept**
Refer to the *Lawful Intercept Configuration Guide* for a description of this parameter.

**motd**
Configures the CLI banner message of the day which is displayed upon the initialization of any CLI session.

**pre-login**
Configures the CLI banner displayed before a CLI user logs in.

**Important**
This banner is displayed only for serial port and telnet log ins. It is not supported in ssh and, therefore, will not be displayed before ssh log ins.
**string**

Specifies the banner or message to be displayed at session initialization. *string* may be an alphanumeric string of 0 through 2048 characters. The string must be enclosed in double quotation marks if the banner or message is to include spaces.

**Usage Guidelines**

Set the message of the day banner when an important system wide message is needed. For example, in preparation for removing a chassis from service, set the banner 1 or more days in advance to notify administrative users of the pending maintenance.

**Examples**

The following command creates a message of the day with the text *Have a nice day.*

`banner motd "Have a nice day."`
bearer-control-profile

This command creates an instance of a Bearer Control profile, a key element of the MME QoS Profile feature.

**Product**
MME

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration
  
  ```
  configure
  ```
  Entering the above command sequence results in the following prompt:
  ```
  [local]host_name(config)#
  ```

**Syntax Description**
```
[no] bearer-control-profile bcprofile_name
```

- **no**
  Including this command prefix causes the MME to delete the named instance of the bearer control profile from the MME's configuration.

- **bcprofile_name**
  Enter an alphanumeric string of 1 through 64 characters to identify a specific bearer control profile.

**Usage Guidelines**
Entering this command provides access to the configuration commands of the Bearer Control Profile Configuration Mode to configure QoS parameters for dedicated-bearers and for default-bearers. Bearer level parameters such as ARP-PL, ARP-PVI, ARP-PCI, MBR, GBR, remap QCI value can be configured here independently for default/dedicated bearer along with the action to be taken, such as prefer-as-cap or pgw-upgrade. Bearer Control profile can be applied for specific QCIs or range of QCIs.

**Examples**
The following sample command creates an instance of a bearer control profile named **BCProf**:
```
bearer-control-profile BCProf
```
**boot delay**

Configures the delay period, in seconds, before attempting to boot the system from a software image file residing on an external network server.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```bash
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

- `boot delay time`  
- `no boot delay`

- `no`

Deletes the setting for the boot delay. The boot process executes immediately.

- `time`

Specifies the amount of time (in seconds) to delay prior to requesting the software image from the external network server as an integer from 1 through 300.

**Usage Guidelines**

Useful when booting from the network when connection delays may cause timeouts. Such as when the Spanning Tree Protocol is used on network equipment.

---

**Important**
The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

**Examples**
The following sets the boot delay to 10 seconds:

```
boot delay 10
```
**boot interface**

Configures Ethernet network interfaces for obtaining a system software image during the system boot process.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

**Syntax Description**

Releases prior to 12.2:

```
boot interface { spio-eth1 | spio-eth2 } [ medium { auto | speed medium_speed duplex medium_duplex } ]
no boot interface
```

Release 12.2 and after:

```
boot interface { local-eth1 | local-eth2 } [ medium { auto | speed medium_speed duplex medium_duplex } ]
no boot interface
```

**no**

Removes the boot interface configuration from the boot.sys file. Only files from the local file system can be loaded.

**spio-eth1 | spio-eth2**

Specifies the network interface to be configured where `spio-eth1` is the primary interface on the SPIO (slot 24 interface 1 or slot 25 interface 1) and `spio-eth2` is the secondary interface on the SPIO (slot 24 interface 2 or slot 25 interface 2). The interfaces are either RJ-45 if for speeds of 10, 100, or 1000 megabits per second (Mbps), or SFP for the optical Gigabit (1000 Mbps).

**local-eth1 | local-eth2**

Specifies the network interface to be configured where `local-eth1` is the primary ethernet interface and `local-eth2` is the secondary ethernet interface.
For the ASR 5000, the primary is interface 1 on the SPIO and the secondary is interface 2 on the SPIO. The interfaces are either RJ-45 if for speeds of 10, 100, or 1000 megabits per second (Mbps), or SFP for optical Gigabit (1000 Mbps).

For the ASR 5500, the primary is port 1 (1000Base-T) on the MIO and the secondary interface is port 2 (1000Base-T) on the MIO.

```
medium { auto | speed medium_speed duplex medium_duplex }
```

Default: auto

- **auto**: configures the interface to auto-negotiate the interface speed and duplex.

- **speed medium_speed duplex medium_duplex**: specifies the speed to use at all times where medium_speed must be one of:
  - 10
  - 100
  - 1000

The keyword **duplex** is used to set the communication mode of the interface where medium_duplex must be one of:

- full
- half

```
media medium_media
```

Default: rj45

Optionally sets the physical interface where medium_media must be either rj45 or sfp.

**Usage Guidelines**

Modify the boot interface settings to ensure the system is able to obtain a software image from an external network server.

**Important**

The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

**Examples**

The following configures the primary interface to auto-negotiate the speed.

```
boot interface spio-eth1 medium auto
boot interface local-eth1 medium auto
```

The following command configures the secondary interface to a fixed gigabit speed at full duplex using RJ45 connectors for the physical interface.

```
boot interface spio-eth2 medium speed 1000 duplex full medium rj45
boot interface local-eth2 medium speed 1000 duplex full medium rj45
```

The following restores the defaults for the boot interface.

```
no boot interface
```
boot nameserver

Configures the IP address of the DNS (Domain Name Service) server to use when looking up hostnames in URLs for network booting.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

boot nameserver  ip_address

no boot nameserver

no

Removes the network boot nameserver information from the boot.sys file.

ip_address

IPv4 dotted-decimal address of the DNS server the system uses to lookup hostnames in URLs for a software image from the network during the system boot process.

Usage Guidelines

Use this command to identify the DNS server to use to lookup hostnames in a software image URL.

Important

The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

Examples

The following configures the system to communicate with a DNS nameserver with the IP address of 10.2.3.4:

boot nameserver 10.2.3.4
**boot networkconfig**

Configures the networking parameters for the Switch Processor I/O card network interfaces to use when obtaining a software image from an external network server during the system boot process.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
boot networkconfig { dhcp | { dhcp-static-fallback | static } ip address spio24 ip_address | spio25 ip_address | netmask ip_mask | gateway gw_address | } }
```

**no boot networkconfig**

Removes the network configuration information from the boot.sys file.

**dhcp**

Indicates that a Dynamic Host Control Protocol (DHCP) server is used for communicating with the external network server.

**dhcp-static-fallback | static**

**dhcp-static-fallback**: provides static IP address fallback network option when a DHCP server is unavailable.

**static**: specifies a fixed network IP address for the external network server that hosts the software image.

**spio24 ip_address [ spio25 ip_address ] netmask ip_mask [ gateway gw_address ]**

**spio24 ip_address [ spio25 ip_address ]**: the IP address to use for the SPIO in slot 24 and optionally the SPIO in slot 25 for network booting. `ip_address` must be specified using IPv4 dotted-decimal notation.

**netmask ip_mask**: the network mask to use in conjunction with the IP address(es) specified for network booting. `ip_mask` must be specified using IPv4 dotted-decimal notation.

**gateway gw_address**: the IP address of a network gateway to use in conjunction with the IP address(es) specified for network booting. `gw_address` must be entered using IPv4 dotted-decimal notation.
If gw_address is not specified, the network server must be on the same LAN as the system. Since both SPIOs must be in the same network, the netmask and gateway settings are shared.

**Important**

Configure the network parameters for the ports on the SPIO cards to use to communicate with an external network server that hosts software images.

**Important**

The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

**Important**

When configuring static addresses both SPIOs must have different IP addresses. Neither address can be the same as the local context IP address.

**Examples**

The following configures the system to communicate with the external network server via DHCP with a fallback to IP address 192.168.100.10, respectively.

```
boot networkconfig dhcp-static-fallback ip address spio24 192.168.100.10 netmask 255.255.255.0
```

The following command configures the system to communicate with an external network server using the fixed (static) IP address 192.168.100.10 with a network mask of 255.255.255.0.

```
boot networkconfig static ip address spio24 192.168.100.10 netmask 255.255.255.0
```

The following restores the system default for the network boot configuration options.

```
no boot networkconfig
```
**boot system priority**

Specifies the priority of a boot stack entry to use when the system first initializes or restarts. Up to 10 boot system priorities (entries in the boot.sys file located in the /flash device in the SPC, SMC or MIO) can be configured.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
boot system priority number image image_url config config_path
no boot system priority number
```

**no**
Remove a boot stack entry at the priority specified from the boot stack when it is no longer used.

**priority number**

Specifies the priority for the file group (consisting of an image (.bin) and its corresponding configuration (.cfg) file) specified in the boot stack. The value must be in the range from 1 through 100 where a priority of 1 is the highest. Up to 10 boot system priorities (boot stack entries) can be configured.

**Important**
When performing a software upgrade it is important that the new file group have the highest priority (lowest number) configured.

**Important**
To ensure that higher priority numbers remain open, use an "N-1" priority numbering methodology, where "N" is the first priority in the current boot stack.
image image_url

Specifies the location of an image file to use for system startup. The URL may refer to a local or a remote file. The URL must be formatted according to the following format:

For the ASR 5000:

- [ file: ] { /flash | /pcmcia1 | /hd } [ /directory ]/filename
- [ http: | tftp: ] [ /host ]:port [ /directory ]/filename

Important

Use of the SMC hard drive is not supported in this release.

For the ASR 5500:

- [ file: ] { /flash | /usb1 | /hd } [ /directory ]/filename
- [ http: | tftp: ] [ /host ]:port [ /directory ]/filename

Important

Do not use the following characters when entering a string for the field names below: "/" (forward slash), ":" (colon) or "@" (at sign).

directory is the directory name.
filename is the actual file of interest.
host is the IP address or host name of the server.
port# is the logical port number that the communication protocol is to use.

Important

A file intended for use on an ASR 5000 uses the convention xxxx.asr5000.bin, where xxxx is the software build number.

Important

A file intended for use on an ASR 5500 uses the convention xxxx.asr5500.bin, where xxxx is the software build number.

Important

When using the TFTP, it is advisable to use a server that supports large blocks, per RFC 2348. This can be implemented by using the "block size option" to ensure that the TFTP service does not restrict the file size of the transfer to 32MB.

config config_path

Specifies the location of a configuration file to use for system startup. This must be formatted according to the following format:

For the ASR 5000:

- [ file: ] { /flash | /pcmcia1 | /hd } [ /path ]/filename
Use of the SMC hard drive is not supported in this release.

For the ASR 5500:

\[
\text{\{file:\{/flash|/usb1|/hd\}/path/filename}\}
\]

Where \text{path} is the directory structure to the file of interest, and \text{filename} is the name of the configuration file. This file typically has a \text{.cfg} extension.

**Usage Guidelines**

This command is useful in prioritizing boot stack entries in the boot.sys file, typically located on the /flash device of the Active SPC, SMC, or MIO, for automatic recovery in case of a failure of a primary boot file group.

**Important**

The configuration file must reside on the SPC's, SMC's, or MIO's local filesystem, stored on one of its local devices (/flash, or /pcmcia1, or /hd-raid/pcmcia1, or /pcmcia2, or /usb1, or /hd-raid). Attempts to load the configuration file from an external network server will result in a failure to load that image and configuration file group, causing the system to load the image and configuration file group with the next highest priority in the boot stack.

**Important**

Configuration changes do not take effect until the system is reloaded.

**Important**

The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

**Examples**

The following commands set up two locations from which to obtain a boot file group.

\[
\text{boot system priority 1 image tftp://remoteABC/pub/2012jan.bin config /flash/pub/data/2012feb.cfg}
\]

\[
\text{boot system priority 2 image /flash/pub/data/2002jun.bin config /pcmcia1/pub/data/2012feb.cfg}
\]

The following removes the current priority 1 boot entry from the boot.sys file.

\[
\text{no boot system priority 1}
\]
bulkstats

Enables the collection of bulk statistics and/or enters the bulk statistics configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]<host_name>(config)#

Syntax Description

bulkstats { collection | historical collection | mode }
no bulkstats { collection | historical }

no

Disables the collection of bulk statistics.

collection

Enables the statistics collection process. Collects a periodic snapshot of activity and performance data as configured via the Bulk Statistics Configuration mode.

historical collection

Enables the collection of historical bulk statistics.
If enabled, StarOS tracks activities that require the storing of more data, such as "the highest value that's been seen over the last 24 hours".

mode

Enters the Bulk Statistics Configuration mode. The resulting command-line prompt will look similar to:

[<context-name>]<asr5000>(config-bulkstats)#

Usage Guidelines

The Bulk Statistics Configuration mode consists of commands for configuring bulk statistic properties, such as the periodicity of collection. Detailed command descriptions appear in the Bulk Statistics Configuration Mode Commands chapter.
The collected bulk statistics are sent to a collection server (called a receiver). Bulk statistics are statistics that are collected in a group or schema, for example, system statistics, port statistics, RADIUS statistics.

Once the receiver, schema, and collection properties are configured, the `bulkstats collection` command enables or disables the collection of the data.

To collect a sample that will provide an average, for example, an average of CPU counters, the "historical" features must be enabled with the `bulkstats historical collection` command.

Since bulk statistics are collected at regular, user-defined intervals, the Exec mode `bulkstats force` command can be used to manually initiate the immediate collection of statistics.

**Examples**

The following command enables the collection of bulk statistics:

`bulkstats collection`
ca-certificate

Configures and selects an X.509 CA certificate to enable a security gateway to perform certificate-based peer (client) authentication. StarOS supports a maximum of 16 certificates and 16 CA (Certificate Authority) root certificates. A maximum of four CA root certificates can be bound to a crypto or SSL (Secure Sockets Layer) template.

**Product**
All IPSec-related products

**Privilege**
Administrator, Security Administrator, Operator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
ca-certificate name name \{ der url url_format | pem \{ data pemdata | url url_format | cert-enc | [ cert-hash-url url url_format ] \}\}
no ca-certificate name name

no
Disables ca-certificate.
```

**Note**
If the CA-CERT is mandatory for the service to be up and running, then the removal of that CA-CERT is not allowed.

**name name**
Specifies the name the CA certificate as an alphanumeric string of 1 through 128 characters.

**der url**
Specifies the use of the Distinguished Encoding Rules (DER) binary format.

**url** is the Universal Reosurce Locator of the file containing certificate in der format.
pem
Specifies that the Privacy-enhanced Electronic Mail (PEM) format is to be used.

data pemdata
Indicates that the CA certificate data will be in PEM format. pemdata must be an alphanumeric string of 1 through 4095 characters.

cert-enc
Specifies a certificate encoding type other than default encoding type.

cert-hash-url
Specifies a hash of X.509 Certificate.

url
Specifies the Universal Resource Locator of the file containing the CA certificate.

url_format
Specifies an existing URL expressed in one of the following formats:
  - [file:][/flash | /pcmcia1 | /hd-raid][/directory]<filename
  - tftp://<host>[:<port>]/<directory>/<filename
  - ftp://<username>[:<password>@]<host>[:<port>]/<directory>/<filename
  - sftp://<username>[:<password>@]<host>[:<port>]/<directory>/<filename
  - http://<username>[:<password>@]<host>[:<port>]/<directory>/<filename

When read via a file, note that show configuration will not contain the URL reference, but will instead output the data via data pemdata, such that the configuration file is self-contained.

Usage Guidelines
Use this command to configure and select an X.509 CA certificate to enable a security gateway or SCM to perform certificate-based peer (client) authentication.

Examples
Use the following command to remove a certificate named fap1:
no ca-certificate fap1
configure the name and URL path of a Certificate Authority-Certificate Revocation List (CA-CRL).

**Product**
All IPSec-related products

**Privilege**
Operator

**Command Modes**
Exec > Global Configuration

```bash
configure
```
Entering the above command sequence results in the following prompt:

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

**Syntax Description**
```bash
crl name \{der | pem\} \{url url\}
no crl name name
```

- **no**
  Removes the named CA-CRL.

- **name**
  Provides a name of the CA-CRL. `name` must be an alphanumeric string of 1 through 128 characters.

- **der**
  Specifies that Distinguished Encoding Rules (DER) format is to be used for the source format.

- **pem**
  Specifies that Privacy-enhanced Electronic Mail (PEM) format is to be used for the source format.

- **url url**
  Specifies the URL where the CA-CRL is to be fetched. `url` must be an existing URL expressed as an alphanumeric string of 1 through 1023 characters in one of the following formats:
  ```
  • [file:]\[/flash | /pmcia | /hd-raid]\[/directory]/<filename
  • tftp://<host>:<port>[/<directory>]/<filename
  • ftp://[<username>:[<password>]<@]<host>:<port>[/<directory>]/<filename
  ```
Usage Guidelines

Use this command to name and fetch a CA-CRL from a specified location.

Without additional information from the CA, an issued certificate remains valid to any verifier until it expires. To revoke certificates, the CA publishes a CRL periodically to provide an updated list of certificates revoked, but not yet expired. Like a certificate, a CRL is a digital document signed by the CA. In addition to a list of serial numbers of revoked certificates, the CRL includes attributes such as issuer name (same as the issuer name in the certificate), signature (signed by the issuer using the same key that signs certificates), last update (the time this CRL was issued), and next update (the time next CRL will be available).

Examples

The following command fetches a CA-CRL named list1.pem from a host.com/CRLs location and names the list CRL5:

crclamation CRL5 pem urllhttp://host.com/CRLs/list1.pem
call-control-profile

Creates an instance of a call-control profile.

Product
- MME
- SGSN

Privilege
- Security Administrator, Administrator

Command Modes
- Exec > Global Configuration
  - configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

| no | call-control-profile cc_profile_name |

no

Deletes the Call-Control Profile instance from the configuration.

cc_profile_name

Specifies the name of the call-control profile. Enter an alphanumeric string of 1 through 64 characters.

Usage Guidelines

Use this command to create an instance of a call-control profile and to enter the call-control profile configuration mode. A call-control profile is a template which groups a set of call-handling instructions that may be applicable to one or more incoming calls. See the Call-Control Profile Configuration Mode Commands chapter for information regarding the definition of the rules contained within the profile and the use of the profile.

Important

A call-control profile is a key element of the Operator Policy feature and is only valid when associated with at least one operator policy.

To see what call-control profiles have already been created, return to the Exec mode and enter the show call-control-profile all command.

Examples

The following command creates a configuration instance of an call-control profile:

call-control-profile ccprof1
**card**

Enters the Card Configuration mode for the specified card. (ASR 5x00 only)

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`card slot_number`

- **slot_number**

  Specifies the slot number of the card for which the card configuration mode is to be entered. `slot_number` must be an integer from 1 through 48 (on the ASR 5000) or 1 through 20 (on the ASR 5500).

**Usage Guidelines**

Enter the configuration mode for a specific card when changes are required.

---

**Important**

This command is not supported on virtual platforms.

**Examples**

The following command enters Card Configuration mode for the card in slot 8 of the chassis:

`card 8`
**card-standby-priority**

Configures the redundancy priorities for packet processing cards by specifying the slot number search order for a standby card when needed.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`card-standby-priority slot_num+`

- `slot_num`
  
  Specifies the slot of the card for the order of the standby cards. `slot_num` must be in the range from 1 through 16 excluding slots 8 and 9 (on the ASR 5000) or 1 through 10 excluding slots 5 and 6 (on the ASR 5500). `+` indicates that you may enter as many slot numbers (separated by a space) as necessary to indicate the complete search order.

**Usage Guidelines**

Set the standby order of the redundant cards when multiple standby cards are available.

Questionable hardware should be placed lower in the priority list.

- **Important**
  
  This command replaces the `pac-standby-priority` command.

- **Important**
  
  This command is not supported on all platforms.

**Examples**

The following command configures the redundancy priority to use the standby cards in slots 16, 14, and 12 in that order:

```
card-standby-priority 16 14 12
```
**cdr-multi-mode**

This command enables multiple instances of CDRMOD, one per packet processing card.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

**Syntax Description**

\[ default | cdr-multi-mode\]

**default**

Configures this command with its default setting.
Default: Single-CDRMOD mode

**Usage Guidelines**

Use this command to enable the multi-CDRMOD mode, wherein there will be one instance of CDRMOD per packet processing card. All the SessMgr instances that are running on a packet processing card will send the records to the CDRMOD instance running on that card.

By default, CDRMOD runs in single mode, wherein there will be only one instance of CDRMOD running for the entire chassis. All the SessMgr instances that are running on a packet processing card will send the records to the CDRMOD instance.

---

**Important**
For changes to this command to take effect, save the configuration and reboot the system.

---

**Important**
In multi-CDRMOD mode, you should enable hard-disk usage.
**certificate**

Configures and selects an X.509 Trusted Author certificate.

**Product**

All IPSec-related products

**Privilege**

Administrator, Security Administrator, Operator

**Command Modes**

Exec > Global Configuration

**Syntax Description**

```
certificate name name  { der url url | pem { data pemdata | url url } private-key pem { [ encrypted ] data pemdata | url url [cert-enc] [cert-hash-url url url ] } }  
no certificate name name
```

- **no**
  Disables certificate.

- **name name**
  Names the certificate. name must be from 1 to 128 alphanumeric characters.

- **der url**
  Specifies that the Distinguished Encoding Rules (DER) binary format is to be used.

- **pem**
  Specifies that the Privacy-enhanced Electronic Mail (PEM) format is to be used.

- **data pemdata**
  Certificate/private key data in PEM format. pemdata must be an alphanumeric string of 1 through 4095 (if private key is not implemented) or 1 through 8191 (if private key is implemented) characters.

- **cert-enc**
  Specifies a certificate encoding type other than default encoding type.
**cert-hash-url**
Specifies a hash and URL of the X.509 Certificate.

**url**
Specifies the Universal Resource Locator (URL) of the file containing certificate/private key.

**url_format**
Specifies an existing URL expressed in one of the following formats:

- [file://]{/flash | /pcmcia1 | /hd-raid}[/directory]/<filename>
- tftp://<host>[:<port>]/<directory>/<filename>
- ftp://<username>[:<password>@]<host>[:<port>]/<directory>/<filename>
- sftp://<username>[:<password>@]<host>[:<port>]/<directory>/<filename>
- http://<username>[:<password>@]<host>[:<port>]/<directory>/<filename>

When read via a file, **show configuration** will not contain the URL reference, but instead outputs the data via **data pemdata**, such that the configuration file is self-contained.

**private-key pem**
Specifies use of private key PEM data.

**encrypted**
Specifies the use of encrypted private key data.

**Usage Guidelines**
Use this command to Configures and selects an X.509 Trusted Author certificate.

**Examples**
Use the following command to remove a certificate named *box1*:

```plaintext
no certificate data box1
```
cli

Configures global Command Line Interface (CLI) parameters.

Product  All

Privilege  Security Administrator, Administrator

Command Modes  Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

cli { access { monitor-protocol | monitor-subscriber | show-configuration } { administrator | operator } } | configuration-monitor | hidden | login-failure-delay number | max-sessions number | operator clear-subscriber-one-only | test-commands [encrypted] password password | trap config-mode }

no cli { configuration-monitor | hidden | login-failure-delay number | max-sessions | operator clear-subscriber-one-only | trap config-mode }

default cli { access { monitor-protocol | monitor-subscriber | show-configuration } { administrator | operator } }

default

Removes the specified option.

default

Resets the keywords to their default values.

access { monitor-protocol | monitor-subscriber | show-configuration } { operator | administrator }

Sets access privileges on the monitor protocol and monitor subscriber commands:

monitor-protocol: Selects privileges for the monitor protocol command.

monitor-subscriber: Selects privileges for the monitor subscriber command.

show-configuration: Selects privileges for the show-configuration command. However the default access level for this command is the user with operator privileges.

operator: Sets the privileges for the selected command to allow use by users with operator privileges.

administrator: Restricts use of the selected command to administrators only.
configuration-monitor

When this keyword is enabled, the system executes a `show configuration checksum` command every 15-minutes. The resulting checksum is compared with the previous checksum.

When a configuration change is detected, a log message and SNMP notification are generated. The SNMP notification only indicates that a change has occurred without identifying what change had been made.

The 15-minute interval is fixed and cannot be configured. By default configuration monitoring is disabled.

hidden

Allows a Security Administrator to enable access to hidden cli test-commands command.

The `no cli hidden` command disables access to the `cli test-commands` command. This is the default mode. Refer to the description of the `test-commands` keyword below for additional information.

login-failure-delay number

Specifies the time to wait before a login failure is returned and another login may be attempted. Default is five seconds.

max-sessions number

Sets the number of allowed simultaneous CLI sessions on the system. If this value is set to a number below the current number of open CLI sessions, the open sessions will continue until closed. `number` must be an integer from 2 through 100.

Caution

Use caution when setting this command. Limiting simultaneous CLI sessions prevents authorized users from accessing the system if the maximum number allowed has been reached. The system already limits CLI sessions based on available resources. Additional limitation could have adverse effects.

operator clear-subscriber-one-only

Restricts Operator to clearing only one subscriber session at a time.

test-commands [encrypted] password password_string

Enables access to the CLI test-commands. The commands and keywords made available under this mode are for internal testing and debugging.

Caution

CLI test-commands are intended for diagnostic use only. Access to these commands is not required during normal system operation. These command are intended for use only by Cisco TAC personnel. Some of these commands can slow system performance, drop subscribers, and/or render the system inoperable.

Important

An SNMP trap is generated when a user enables `cli test-commands` (starTestModeEntered). Refer to the `SNMP MIB Reference` for additional information.

encrypted: Specifies that the system will save the password in an encrypted format in the configuration file. The system displays the encrypted keyword in the configuration file as a flag indicating 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_string**: Prompts for the password required to access CLI test-commands. This password must have been previously configured by a Security Administrator via the **tech-support test-commands password** command. The password is an alphanumeric string of 1 through 64 characters (plain text password) or 1 through 524 characters (encrypted password).

If the **password** keyword is not entered, the user is prompted (no-echo) to enter the password. If **tech-support test-commands password** has not been enabled, you will be unable to execute **cli test-commands**.

Once this test mode is entered under Global Configuration mode, CLI test-commands become part of the current configuration. Therefore, any generated configuration file will contain the **cli test-commands** command as the first configuration command.

---

**Caution**

Use of CLI test-commands may cause significant service interruption. Contact Cisco TAC before executing any commands while in this mode.

The **no cli test-commands** command disables access to the CLI test-commands mode.

**trap config-mode**

Enables sending an SNMP trap (starCLICfgMode) when a CLI user enters the configuration mode.

---

**Usage Guidelines**

This command sets access parameters and enables several operational parameters for the system's command line interface.

---

**Important**

The maximum number of multiple CLI sessions that can be supported is based on the amount of available memory. A minimum of 15 CLI sessions are supported on the ASR 5x00. One of the CLI sessions is reserved for use exclusively by a CLI session on a serial console interface. Additional CLI sessions beyond the pre-reserved set are permitted if sufficient management card resources are available. If the Resource Manager is unable to reserve resources for a CLI session beyond those that are pre-reserved, administrative users are prompted as to whether or not the system should attempt to create the new CLI session even without reserved resources.

---

**Examples**

The following command sets the number of allowed simultaneous CLI sessions to 5.

`cli max-sessions 5`

The following command sets the command **monitor protocol** to administrator-only

`cli access monitor-protocol administrator`
**cli-encrypt-algorithm**

Specifies the type of encryption algorithm to be used for passwords and secrets.

**Product**
All

**Privilege**
Security Administrator

**Command Modes**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config) #

**Syntax Description**

```
cli-encrypt-algorithm { A | B | C }
default cli-encrypt-algorithm
```

default

Resets the encryption algorithm to "A".

A

Specifies MD5-based cipher encryption algorithm. This is the default. Passwords encrypted with this key will have "+A" prefixes in the configuration file.

B

Specifies the AES-CTR-128 cipher algorithm for encryption and the HMAC-SHA1 cipher algorithm for authentication. Passwords encrypted with this key will have "+B" prefixes in the configuration file.

C

Specifies HMAC-SHA512 cipher algorithm for encryption and authentication. Passwords encrypted with this key will have "+C" prefixes in the configuration file.

**Usage Guidelines**

Use this command to specify the types of cipher algorithm(s) to be used as encryption and authentication keys for passwords.

The encryption key protects the confidentiality of passwords, while the authentication key protects their integrity.
Examples

The following command sets the encryption key to C:

\texttt{cli-encrypt-algorithm C}
**clock**

Configures system clock timezone and what local time zone to use.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

clock timezone tz | local |

no clock timezone

no

Resets the system timezone to the system default UTC.

**tz**

Specifies the system time zone to use as one of:

- america-buenos-aires (GMT-3:00; Buenos Aires)
- america-caracas (GMT-4:00) Caracas
- america-guatemala (GMT-6:00; Guatemala, Guatemala)
- america-la_paz (GMT-4:00; La Paz)
- america-lima (GMT-5:00; Lima, Peru)
- america-puerto-rico (GMT-4:00; Puerto Rico)
- america-sao-paulo (GMT-3:00; Brazil)
- america-tijuana (GMT-8:00; Tijuana)
- asia-almaty (GMT+6.00; Almaty, Kazakhstan)
- asia-baghdad (GMT+3:00; Baghdad, Russia Zone 2, Kuwait, Nairobi, Riyadh, Moscow, Tehran)
- asia-bangkok (GMT+7:00; Bangkok)
• asia-calcutta (GMT+5:30; Calcutta, Mumbai, New Delhi)
• asia-dhaka (GMT+6:00; Dhaka)
• asia-hong-kong (GMT+8:00; Hong_Kong)
• asia-irkutsk (GMT+9:30; Irkutsk)
• asia-kabul (GMT+4:30; Kabul)
• asia-karachi (GMT+5:00; Karachi)
• asia-katmandu (GMT+5:45; Kathmandu)
• asia-magadan (GMT+11:00; Magadan)
• asia-muscat (GMT+4:00; Abu Dhabi, UAE, Muscat, Tblisi, Volgograd, Kabul)
• asia-rangoon (GMT+6:30; Rangoon)
• asia-seoul (GMT+9:00) Seoul
• asia-tehran (GMT+3:30; Tehran)
• asia-tokyo (GMT+9:00; Tokyo, Russia Zone 8)
• atlantic-azores (GMT-2:00; Azores)
• atlantic-cape-verde (GMT-1:00; Cape Verde Islands)
• australia-perth (GMT+8:00) Perth
• australia-darwin (GMT+9:30) Northern Territory - Alice Springs, Darwin, Uluru
• australia-adelaide (GMT+9:30) Southern Territory - Adelaide
• australia-melbourne (GMT+10:00) Victoria - Ballarat, Melbourne
• australia-sydney (GMT+10:00) New South Wales - Newcastle, Sydney, Wollongong
• australia-hobart (GMT+10:00) Tasmania - Hobart, Launceston
• australia-brisbane (GMT+10:00) Queensland - Brisbane, Cairns, Toowoomba, Townsville
• australia-lordhowe (GMT+10:30) Lord Howe Island
• canada-newfoundland (GMT-3:30; Newfoundland)
• canada-saskatchewan (GMT-6:00; Saskatchewan)
• europe-central (GMT+1:00; Paris, Berlin, Amsterdam, Brussels, Vienna, Madrid, Rome, Bern, Stockholm, Oslo)
• europe-dublin (GMT+0:00) Dublin, Ireland
• europe-eastern (GMT+2:00; Russia Zone 1, Athens, Helsinki, Istanbul, Jerusalem, Harare)
• newzealand-auckland (GMT+12:00; Auckland, Wellington)
• newzealand-chatham (GMT+12:45; Chatham)
• nuku (GMT-13:00; Nuku'alofa)
• pacific-fiji (GMT+12:00; Wellington, Fiji, Marshall Islands)
• pacific-guam (GMT+10:00; Brisbane, Cairns, Sydney, Guam)
• pacific-kwajalein (GMT-12:00; Kwajalein)
• pacific-norfolk - (GMT+11:30) Norfolk Island
• pacific-samoa (GMT-11:00; Samoa)
• us-alaska (GMT-9:00; Alaska)
• us-arizona (GMT-7:00; Arizona)
• us-central (GMT-6:00; Chicago, Mexico City, Saint Louis)
• us-eastern (GMT-5:00; Bogota, Lima, New York City)
• us-hawaii (GMT-10:00; Hawaii)
• us-indiana (GMT-6:00; Indiana)
• us-mountain (GMT-7:00; Cheyenne, Denver, Las Vegas)
• us-pacific (GMT-8:00) San Francisco, LA, Seattle
• utc (GMT; Universal Time Coordinated: London, Dublin, Edinburgh, Lisbon, Reykjavik, Casablanca)

local
Indicates the timezone specified by tz is to be considered the local time zone for local time display and conversion.

Usage Guidelines
Clock and timezone management is necessary for proper accounting records. The chassis may be set to display a different local time than that of the system clock which allows accounting records to use the system time but to display the proper local time for users.

Examples
The following command sets the clock time zone to UTC (Universal Time Coordinated):
clock timezone utc
cmp auto-fetch

Use this command to add a fetch configuration for each certificate for which automatic update is required. This is a Certificate Management Protocol v2 command.

**Product**

All products supporting IPSec CMPv2 features

**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

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
cmp auto-fetch current-name cert_name ca-root ca_name time days
no auto-fetch current-name cert_name
```

**no**

Removes auto-fetch configuration for a certificate.

**current-name cert-name**

Specifies a valid security gateway certificate as an alphanumeric string of 1 through 129 characters.

**ca-root ca_name**

Specifies the filename of the root certificate of the CA server. ca_name is an alphanumeric string of 1 through 129 characters.

**time days**

Specifies the number of days before the certificate expires as the time when the auto fetch should be triggered. days is specified as an integer from 1 through 256.
Usage Guidelines

Use this command to specify when a current certificate should be automatically fetched.

Examples

The following command automatically fetches the current certificate (aqaw12345) 10 days before it is to expire:

```
cmp fetch current-name aqaw12345 ca-root ca001 time 10
```
**cmp cert-store location**

Use this command to add a file location on /flash disk where the certificates and private keys will be stored. This is a Certificate Management Protocol v2 command.

**Product**

All products supporting IPSec CMPv2 features

---

**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

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
cmp cert-store location  pathname  |  key reuse |
no  cmp cert-store
```

**no**

Removes the certificate storage location configuration.

**pathname**

Specifies the storage location of the certificates and key files in the following formats:

- `file://[/flash | /usb1 | /hd-raid ][/directory]/<filename>`
- `tftp://<host>[:<port>]/<directory>/<filename>`
- `ftp://[<username>[:<password>]@]<host>[:<port>]/<directory>/<filename>`
- `sftp://[<username>[:<password>]@]<host>[:<port>]/<directory>/<filename>`
- `http://[<username>[:<password>]@]<host>[:<port>]/<directory>/<filename>`

**Usage Guidelines**

Use this command to specify where certificates and key files should be stored.
The following command stores certificates and key files in a location different from the default location:
```
cmp cert-store location file:///certificates
```
**cmp cert-trap time**

Defines when an SNMP MIB certificate expiry trap should be sent as the number of hours before expiration.

**Product**
All products supporting IPSec CMPv2 features

**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

```plaintext
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
- `cmp cert-trap time hours`
- `no cmp cert-trap time`

`no`
Removes the certificate expiry MIB trap notification.

`time hours`
Specifies the number of hours before certificate expiry when a MIB trap should be sent. `hours` is an integer from 1 through 1024.

**Usage Guidelines**
Use this command to set when an SNMP MIB certificate expiry trap should be sent.

**Examples**
The following command specifies that an SNMP MIB certificate expiry trap should be sent 48 hours prior to expiration:

```
cmp cert-trap time 48
```
**commandguard**

Forces mandatory confirmation prompting for the **autoconfirm** (Exec mode and Global Configuration mode) and **configure** (Exec mode).

**Product**
All products

**Privilege**
Security Administrator, Administrator, Operator

**Command Modes**
Exec > Global Configuration
 configure

Entering the above command sequence results in the following prompt:

```bash
[local]\host_name(config)#
```

**Syntax Description**

```
[ no ] commandguard  [ exec-command  exec_mode_category  ]
```

- **no**
  
  Disables commandguard functionality if enabled.

- **exec-command exec_mode_category**

  Applies mandatory prompting for specified categories of Exec mode configuration commands, even when **autoconfirm** is enabled.

  **exec_mode_category** specifies one of the following categories of Exec mode configuration commands:
  
  - card
  - clear
  - copy
  - debug
  - delete
  - filesystem
  - hd
  - reload
  - rename
You can enter multiple `commandguard exec-command exec_mode_category` commands.

**Usage Guidelines**

Use this command to force mandatory confirmation prompting for the `autoconfirm` (Exec mode and Global Configuration mode) and `configure` (Exec mode). This command prevents users from accidentally entering Global Configuration mode, or to prevent file replay (most commonly caused by a cut and paste error in the configuration file). By default this command is disabled.

The status of `commandguard` is output in `show configuration` commands.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>If <code>autoconfirm</code> is enabled, <code>commandguard</code> will not take effect until <code>autoconfirm</code> is disabled in both Exec and Global Configuration modes.</td>
</tr>
</tbody>
</table>

Use the `commandguard` command to apply mandatory prompting for specified categories of Exec mode configuration commands, even when `autoconfirm` is enabled.

- All Exec mode commands beginning with the specified category word will prompt for confirmation, regardless if `autoconfirm` is enabled.
- You can turn off confirmation prompting for a specific category using `no commandguard exec-command exec_mode_category`.
- If `autoconfirm` is overridden by `commandguard exec-command` for an Exec mode command, StarOS displays an informational message indicating why `autoconfirm` is being overridden when you attempt to execute the command.
- Users may selectively override confirmation prompting for any Exec mode configuration command that supports the `-noconfirm` keyword.

**Examples**

The following command enables confirmation prompting for all configuration commands:

`commandguard`
congestion-control

This command enables and disables the congestion control functionality on the system.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
{ default | no | congestion-control

default
Sets the congestion control to its default value.

no
Disables the congestion control functionality. This is the default behavior.
```

**Usage Guidelines**

Congestion control on the system is used to monitor the system for conditions that could potentially degrade performance when the system is under heavy load. Typically, these conditions are temporary (i.e. high CPU or memory utilization) and are quickly resolved. However, continuous or large numbers of these conditions within a specific time interval may impact the system's ability to service subscriber sessions. The purpose of congestion control is to aid in the identification of such conditions and invoke policies for addressing the situation.

Congestion control operation is based on the configuration of the following:

- **Call disconnections on overload**: With this functionality, the system enables and disables the policy for disconnecting passive calls (chassis-wide) during an overload situation. It also configures and fine-tunes the overload-disconnect congestion control policy for an entire chassis.

- **Congestion condition thresholds**: Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). These thresholds function in a similar fashion to the operation thresholds that can be configured for the system (as described in later in this chapter). The primary difference is that when these thresholds are reached, not only is an SNMP trap generated (starCongestion), but a service congestion policy is invoked as well.
A threshold tolerance is configured to dictate the percentage under the configured threshold that must be reached in order for the condition to be considered "cleared". An SNMP trap (starCongestionClear) is then triggered.

- **Service congestion policies**: Congestion policies are configurable for each service (e.g., PDSN, GGSN, P-GW, SGSN, etc.). These policies dictate how services respond should the system detect that a congestion condition threshold has been crossed.

Since the congestion control functionality on the system is disabled by default, this command should be executed once congestion-control thresholds and policies have been configured. (Refer to the other congestion-control related commands for more information.)

**Examples**

The following command enables the congestion control functionality on the system.

```
congestion-control
```
congestion-control overload-disconnect

This command enables and disables the policy for disconnecting passive calls (chassis-wide) during an overload situation. It also configures and fine-tunes the overload-disconnect congestion control policy for an entire chassis.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local] host_name (config) #

Syntax Description
congestion-control overload-disconnect [ iterations-per-stage integer | percent percentage_value | threshold { license-utilization percentage_value | max-sessions-per-service-utilization percentage_value | tolerance number } ]
default congestion-control overload-disconnect [ iterations-per-stage | percent | threshold { license-utilization | max-sessions-per-service-utilization | tolerance } ]
no congestion-control overload-disconnect

default
When "default" and one of the keywords is added to the command, the policy remains in its current state and the value for the specified keyword is reset to its default value.
When "default" and the command are entered without keywords, the overload-disconnect policy for congestion control is disabled.

no
Disables the overload-disconnect policy for congestion control.

iterations-per-stage integer
Specifies the number of calls to be disconnected during the defined number of seconds. integer is a value from 2 through 8. The default value is 8.
percent percentage_value
Specifies the percentage of calls to be disconnected, in stages, during an overload situation. percentage_value is an integer from 1 through 100. The default value is 5.

threshold

license-utilization: Specifies the license-utilization percentage threshold for overload situations. If candidates are available, passive calls are disconnected when this threshold is exceeded. percentage_value is an integer from 1 through 100. The default value is 80.

max-sessions-per-service-utilization: Specifies a percentage of the maximum sessions per service. If candidates are available, passive calls are disconnected when this threshold is exceeded. percentage_value is an integer from 1 through 100. The default value is 80.

tolerance: Specifies the percentage of calls the system disconnects below the values set for the other two thresholds. In either case, a Clear Traps message is sent after the number of calls goes below the corresponding threshold value. number is an integer from 1 through 25. The default value is 10.

Usage Guidelines
Use this command to set the policy for call disconnects when the chassis experiences call overload.

To verify the congestion-control configuration use show congestion-control configuration from the Exec mode.

To set overload-disconnect policies for individual subscribers., see overload-disconnect in Subscriber Configuration Mode Commands.

Examples
The following command sets an overload-disconnect policy for the chassis in which 5 calls would be disconnected very 5 seconds during an overload situation.

congestion-control overload-disconnect interactions-per-stage 5

Both of the following commands disable the overload-disconnect policy without changing the policy configuration.

default congestion-control overload-disconnect

or

no congestion-control overload-disconnect

To instruct the system to stop call disconnects when the number of calls goes down 85% of the total allowed calls for that service, enter both of the following commands to set the max-sessions-per-service-utilization value to 90% and the tolerance value to 5%:

congestion-control overload-disconnect threshold max-sessions-per-service-utilization 90
congestion-control overload-disconnect threshold tolerance 5
congestion-control policy

Configures congestion control policies.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
congestion-control policy { asngw-service | asnpc-service | epdg-service fng-service | ggsn-service | ha-service | hnbgw-service | hsgw-service | ipsg-service | lma-service | lns-service | mipv6ha-service | pcc-af-service | pcc-policy-service | pdg-service | pdif-service | pdsn-service | pdsnclsdbr-service | pgw-service | phsgw-service | phspc-service | saegw-service | samog-service | sgxn-service | sgw-service | wsg-service} action {drop | none | redirect | reject} congestion-control policy mme-service action {drop | none | reject | report-overload {permit-emergency-sessions | reject-new-sessions | reject-non-emergency-sessions} enodeb-percentage percentage} congestion-control policy {critical mme-service action-profile action_profile_name | major mme-service action-profile action_profile_name | minor mme-service action-profile action_profile_name} congestion-control policy {critical | major | minor} sgxn-service action-profile action_profile_name no congestion-control policy {critical | major | minor} sgxn-service default congestion-control policy { asngw-service | asnpc-service | epdg-service | fng-service | ggsn-service | ha-service | hnbgw-service | hsgw-service | ipsg-service | lma-service | lns-service | mipv6ha-service | mme-service | pcc-af-service | pcc-policy-service | pdg-service | pdif-service | pdsn-service | pdsnclsdbr-service | pgw-service | phsgw-service | phspc-service | saegw-service samog-service | sgxn-service | sgw-service | wsg-service }

```

default

Specifies the Congestion Control policy action for the selected service to its default value.

**asngw-service**

Specifies the Congestion Control policy action for the ASN-GW service.

**asnpc-service**

Specifies the Congestion Control policy action for the ASN PC-LR service.
**critical**

For MME (starting with Release 14.0), or ePDG (starting with Release 14.1), or for SGSN (starting with Release 17.0), this keyword associates the action-profile to be used for critical congestion thresholds for the MME or SGSN's service.

**epdg-service action**

Specifies the Congestion Control policy action for the ePDG service.

Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

For ePDG type of session/calls, **redirect** action is not supported.

**fng-service**

Specifies the Congestion Control policy action for the FNG service.

**ggsn-service**

Specifies the Congestion Control policy action for the GGSN service.

**ha-service**

Specifies the Congestion Control policy action for the HA service.

**hnbgw-service**

Specifies the Congestion Control policy action for the HNB-GW service.

Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

**hsgw-service**

Specifies the Congestion Control policy action for the HSGW service.

Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **redirect**: Specifies that the system should redirect new session requests to an alternate device.
If this option is used, the IP address of the alternate device must be configured using the **policy overload redirect** command that is part of the HSGW service configuration.

- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

**ipsg-service**

Specifies the Congestion Control Policy action for the IPSG service. The policy specifies how the IPSG service will respond when the system detects that a congestion condition threshold has been crossed.

Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.

**Default**: none

**lma-service**

Specifies the Congestion Control policy action for the LMA service

**lns-service**

Specifies the Congestion Control policy action for the LNS service.

**mipv6ha-service**

Specifies the Congestion Control policy action for the MIPv6-HA service.

**major**

For MME (starting with Release 14.0), or ePDG (starting with Release 14.1), or for SGSN (starting with Release 17.0), this keyword associates the action-profile to be used for major congestion thresholds for the MME or SGSN's service.

**minor**

For MME (starting with Release 14.0), or ePDG (starting with Release 14.1), or for SGSN (starting with Release 17.0), this keyword associates the action-profile to be used for minor congestion thresholds for the MME or SGSN's service.

**mme-service**

Sets the congestion control policy for action to take when subscriber sessions exceeds the defined threshold limit.

For MME type of session/calls, **redirect** action is not supported.
The **mme-service** keyword option is available only in releases prior to 14.0. In 14.0 and higher, you must first select either the critical, major or minor policy level first. Refer to the **congestion-action-profile** command in the LTE Policy Configuration mode to create action-profiles which in turn define the actions to be taken when thresholds are exceeded in Release 14.0 and higher for MME.

**Important**

**pcc-af-service**

Specifies the Congestion Control policy action for the PCC Application Function (AF) service.

Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

**pcc-policy-service**

Specifies the Congestion Control policy action for the PCC Policy service.

Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

**pcc-quota-service**

Specifies the Congestion Control policy action for the PCC Quota service.

Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

**pdg-service**

Specifies the Congestion Control policy action for the PDG service.

**pdif-service**

Specifies the Congestion Control policy action for the PDIF service.

**pdsn-service**

Specifies the Congestion Control policy action for the PDSN service.
**pdsnclosedrp-service**

Specifies the Congestion Control policy action for the PDSN Closed R-P service.

**pgw-service**

Specifies the Congestion Control policy action for the P-GW service.

Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

For P-GW sessions/calls, **redirect** action is not supported.

**saegw-service**

Specifies the Congestion Control policy action for the SAEGW service.

Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

For SAEGW sessions/calls, **redirect** action is not supported.

**samog-service**

Specifies the Congestion Control policy action for the SaMOG service.

Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

**sgsn-service**

Specifies the Congestion Control policy - the congestion response actions for the SGSN service.

Prior to Release 17.0, the supported policy actions in this command are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.
With Release 17.0 and higher, to define a policy you must first select one of the three congestion levels: critical, major or minor. Next select the service with the \texttt{sgsn-service} keyword and then associate a congestion-action-profile. Refer to the \texttt{congestion-action-profile} command in the SGSN-Global Configuration mode to create the congestion-action-profiles which define the congestion response actions to be taken when thresholds are exceeded for the SGSN.

\textbf{sgw-service}

Specifies the Congestion Control policy action for the S-GW service.

Supported policy actions are:

- \textbf{drop}: Specifies that the system should drop incoming packets containing new session requests.
- \textbf{none}: Specifies that the system should take no action.
- \textbf{reject}: Specifies that the system processes new session request messages and responds with a reject message.

For S-GW sessions/calls, \texttt{redirect} action is not supported.

\textbf{wsg-service}

Specifies the Congestion Control policy action for the WSG service.

Supported policy actions are:

- \textbf{drop}: Specifies that the system should drop incoming packets containing new session requests.
- \textbf{none}: Specifies that the system should take no action.
- \textbf{reject}: Specifies that the system processes new session request messages and responds with a reject message.

\textbf{action \{ drop | none | redirect | reject \}}

Specifies the policy action:

- \textbf{drop}: Specifies that the system should drop incoming packets containing new session requests.
- \textbf{none}: Specifies that the system should take no action. This is the default for PDIF-service.
- \textbf{redirect}: Specifies that the system should redirect new session requests to an alternate device. (HA, HSGW, and PDSN only)

\begin{itemize}
  \item \textbf{reject}: Specifies that the system processes new session request messages and responds with a reject message.
\end{itemize}

(For PDSN and HA, the reply code is 130, "insufficient resources". For the GGSN, the reply code is 199, "no resources available".)
**report-overload** {permit-emergency-sessions | reject-new-sessions | reject-non-emergency-sessions }

**enodeb-percentage** percentage

---

**Important**

This set of keywords is supported only by the MME.

Enables the MME to report overload conditions to eNodeBs and take additional action to alleviate congestion situations.

**permit-emergency-sessions**: Specifies that only emergency sessions are allowed to access the MME during the overload period.

**reject-new-sessions**: Specifies that all new sessions destined for the MME will be rejected during the overload period.

**reject-non-emergency-sessions**: Specifies 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 to 100.

---

**Usage Guidelines**

Congestion policies can be configured for each service. When congestion control functionality is enabled, these policies dictate how services respond should the system detect that a congestion condition threshold has been crossed.

---

**Examples**

The following command configures a congestion control policy of reject for PDSN services:

```
congestion-control policy pdsn-service action reject
```

The following command configures a congestion control policy of reject for MME services:

```
congestion-control policy mme-service action reject
```
congestion-control threshold

Configures the congestion control threshold values that are to be monitored.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
```
congestion-control threshold { license-utilization percent | max-sessions-per-service-utilization percent |
message-queue-utilization percent | message-queue-wait-time time | port-rx-utilization percent |
port-specific { slot/port | all } [ tx-utilization percent ] [ rx-utilization percent ] port-specific-rx-utilization critical |
port-specific-tx-utilization critical | port-tx-utilization percent | service-control-cpu-utilization percent |
system-cpu-utilization percent | system-memory-utilization percent | tolerance percent }
default congestion-control threshold { license-utilization | max-sessions-per-service-utilization |
message-queue-utilization | message-queue-wait-time | port-rx-utilization | port-specific | tx-utilization |
| rx-utilization | port-tx-utilization | service-control-cpu-utilization | system-cpu-utilization |
| system-memory-utilization | tolerance }
no congestion-control threshold port-specific { slot/port | all }
no congestion-control threshold port-specific { slot/port | all } [ rx-utilization percent ] [ tx-utilization percent ]
no congestion-control threshold port-specific-rx-utilization critical
no congestion-control threshold port-specific-tx-utilization critical
no congestion-control threshold { message-queue-utilization | message-queue-wait-time |
port-rx-utilization percent | port-tx-utilization percent | service-control-cpu-utilization |
| system-cpu-utilization | system-memory-utilization }

**default congestion-control threshold** keyword

Sets the threshold keyword to its default value.

**no congestion-control threshold port-specific { slot/port | all }
**

This command disables port specific threshold monitoring on the specified port or on all ports.

*slot/port*: Specifies the port for which port specific threshold monitoring is being configured. The slot and
port must refer to an installed card and port.

*all*: Set port specific threshold monitoring for all ports on all cards.
**no congestion-control threshold port-specific-rx-utilization critical**

This command disables specific receive port utilization.

**no congestion-control threshold port-specific-tx-utilization critical**

This command disables specific transmit port utilization.

**license-utilization** `<percent>`

Default: 100

The percent utilization of licensed session capacity as measured in 10 second intervals. `<percent>` can be configured to any integer value from 0 to 100.

**max-sessions-per-service-utilization** `<percent>`

Default: 80

The percent utilization of the maximum sessions allowed per service as measured in real-time. This threshold is based on the maximum number of sessions or PDP contexts configured for the a particular service. (Refer to the `bind` command for the PDSN, GGSN, SGSN, or HA services.) `<percent>` can be an integer from 0 through 100.

**message-queue-utilization** `<percent>`

Default: 80

The percent utilization of the Demux Manager software task's message queue as measured in 10 second intervals. The queue is capable of storing a maximum of 10000 messages. `<percent>` can be an integer from 0 through 100.

**message-queue-wait-time** `<time>`

Default: 5

The maximum time (in seconds) messages can be held in queue as measured by packet time stamps. `<time>` is measured in seconds and can be an integer from 1 through 30.

---

### Important

In the event that this threshold is crossed, an SNMP trap is not triggered. The service congestion policy invocation resulting from the crossing of this threshold is enforced only for the packet that triggered the action.

---

**[ no ] port-rx-utilization** `<percent>`

Default: 80

The average percent utilization of port resources for all ports by received data as measured in 5-minute intervals. `<percent>` can be an integer from 0 through 100.
congestion-control threshold

[ no | port-specific { slot/port | all } ] [ rx-utilization percent ] [ tx-utilization percent ]

Default: Disabled
Sets port-specific thresholds. If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is applied system-wide.

*slot/port*: Specifies the port for which port-specific threshold monitoring is being configured. The slot and port must refer to an installed card and port.

*all*: Set port specific threshold monitoring for all ports on all cards.

*rx-utilization percent*: Default 80%. The average percent utilization of port resources for the specified port by received data as measured in 5-minute intervals. *percent* must an integer from 0 through 100.

*tx-utilization percent*: Default 80%. The average percent utilization of port resources for the specified port by transmitted data as measured in 5-minute intervals. *percent* must be an integer from 0 through 100.

[ no | port-tx-utilization percent ]

Default: 80
The average percent utilization of port resources for all ports by transmitted data as measured in 5-minute intervals.

*percent* can be an integer from 0 through 100.

*service-control-cpu-utilization percent*

Default: 80
The average percent utilization of CPUs on which a Demux Manager software task instance is running as measured in 10-second intervals.

*percent* can be an integer from 0 through 100.

*system-cpu-utilization percent*

Default: 80
The average percent utilization for all PAC/PSC/PSC2 CPUs available to the system as measured in 10-second intervals.

*percent* can be an integer from 0 through 100.

This threshold setting can be disabled with *no congestion-control threshold system-cpu-utilization* command. In case later you want to enable the same threshold setting *congestion-control threshold system-cpu-utilization* command will enable the CPU utilization threshold to preconfigured level.

*system-memory-utilization percent*

Default: 80
The average percent utilization of all CPU memory available to the system as measured in 10-second intervals.

*percent* can be an integer from 0 through 100.

*tolerance percent*

Default: 10
The percentage under a configured threshold that dictates the point at which the condition is cleared.
percent can be an integer from 0 through 100.

**Usage Guidelines**

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). These thresholds function in a similar fashion to the operation thresholds that can be configured for the system (as described in later in this chapter). The primary difference is that when these thresholds are reached, not only is an SNMP trap generated (starCongestion), but a service congestion policy is invoked as well.

The tolerance parameter establishes the threshold at which the condition is cleared. An SNMP trap (starCongestionClear) is generated for the clear condition, as well.

---

**Important**

The MME (version 14.0 and higher) supports three levels of thresholds – critical, major and minor – for each condition. Refer to the `congestion-control threshold` commands immediately following this command for information specific to the MME.

---

**Examples**

The following command configures a system CPU utilization threshold of 75%.

```
congestion-control threshold system-cpu-utilization 75
```

This setting will remain in configuration unless you specify another threshold value in place of 75. This threshold setting can be disabled with `no congestion-control threshold system-cpu-utilization` command but cannot be removed from configuration. Later if you want to enable the previously configured threshold value of 75 percent, you only need to enter the `congestion-control threshold system-cpu-utilization` command without specifying any threshold value. It will enable the CPU utilization threshold to preconfigured level of 75 percent.

For example, `no congestion-control threshold system-cpu-utilization` disables the configured threshold setting and `congestion-control threshold system-cpu-utilization` again enables the threshold setting of 75%.

The following command configures a threshold tolerance of 5%:

```
congestion-control threshold license-utilization tolerance 5
```

In the above examples, the starCongestion trap gets triggered if the license utilization goes above 75% and the starCongestionClear trap gets triggered if it reaches or goes below 70%.
congestion-control threshold license-utilization

Configures the congestion threshold levels for license utilization on the system.

Important

This command applies to MME (version 14.0 and higher) and ePDG (version 14.1 and higher).

Product

MME
ePDG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config) #

Syntax Description

congestion-control threshold license-utilization { critical percent | major percent | minor percent }

default congestion-control threshold license-utilization

Sets all license-utilization thresholds to the default values.

critical percent

Default: 100

The critical threshold value for percent utilization of licensed session capacity, measured in 10-second intervals. percent can be configured to any integer value from 0 to 100.

major percent

Default: 0

The major threshold value for percent utilization of licensed session capacity, measured in 10-second intervals. percent can be configured to any integer value from 0 to 100.
**minor percent**

Default: 0

The minor threshold value for percent utilization of licensed session capacity, measured in 10-second intervals. *percent* can be configured to any integer value from 0 to 100.

**Usage Guidelines**

Use this command to set the critical, major and minor threshold levels of licensed session capacity as a percentage as measured in 10-second intervals.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

This command requires a valid product license.

**Examples**

The following command configures a minor threshold level for license utilization of 25%.

```
congestion-control threshold license-utilization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25.

The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold license-utilization
```
congestion-control threshold max-sessions-per-service-utilization

Configures the congestion thresholds for the maximum sessions allowed per service.

**Important**
This command applies to MME (version 14.0 and higher) and ePDG (version 14.1 and higher).

**Product**
- MME
- ePDG

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
```
congestion-control threshold max-sessions-per-service-utilization { critical percent | major percent | minor percent }
default congestion-control threshold max-sessions-per-service-utilization

default congestion-control threshold max-sessions-per-service-utilization
Sets all max-sessions-per-service-utilization thresholds to the default values.

**critical percent**
Default: 80
The critical threshold value for percent utilization of the maximum sessions allowed per service.
percent can be configured to any integer value from 0 to 100.

**major percent**
Default: 0
The major threshold value for percent utilization of the maximum sessions allowed per service.
percent can be configured to any integer value from 0 to 100.
**Usage Guidelines**

Use this command to set the critical, major and minor threshold levels of maximum sessions per service as a percentage measured in real-time. This threshold is based on the maximum number of sessions or PDP contexts configured for the a particular service. (Refer to the `bind` command for the PDSN, GGSN, SGSN, or HA services.)

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

This command requires a valid product license.

**Examples**

The following command configures a minor threshold level of 25%.

```
congestion-control threshold max-sessions-per-service-utilization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25.

The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold max-sessions-per-service-utilization
```
congestion-control threshold message-queue-utilization

Configures the congestion thresholds for the percent utilization of the Demux Manager software task's message queue.

**Important**

This command applies to ePDG (version 14.1 and higher).

**Product**

ePDG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] *host_name*(config)#

**Syntax Description**

congestion-control threshold message-queue-utilization { critical *percent* | major *percent* | minor *percent* }

default congestion-control threshold message-queue-utilization

default congestion-control threshold message-queue-utilization

Sets all max-sessions-per-service-utilization thresholds to the default values.

critical *percent*

Default: 80

The critical threshold value for percent utilization of the Demux Manager software task's message queue as measured in 10-second intervals.

*percent* can be configured to any integer value from 0 to 100.

major *percent*

Default: 0

The major threshold value for percent utilization of the Demux Manager software task's message queue as measured in 10-second intervals.

*percent* can be configured to any integer value from 0 to 100.
**minor percent**

Default: 0

The minor threshold value for percent utilization of the Demux Manager software task's message queue as measured in 10-second intervals.

*percent* can be configured to any integer value from 0 to 100.

### Usage Guidelines

Use this command to set the critical, major and minor threshold levels of percent utilization of the Demux Manager software task's message queue as measured in 10-second intervals.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

This command requires a valid product license.

### Examples

The following command configures a minor threshold level of 25%.

```
congestion-control threshold message-queue-utilization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25.

The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold message-queue-utilization
```
congestion-control threshold message-queue-wait-time

Configures the congestion thresholds for the maximum time (in seconds) messages can be held in queue as measured by packet time stamps.

**Important**

This command applies to ePDG (version 14.1 and higher).

**Product**
ePDG

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```bash
configure
```

Entering the above command sequence results in the following prompt:

```bash
[local]host_name(config)#
```

**Syntax Description**

- `congestion-control threshold message-queue-wait-time { critical time | major time | minor time }
- default congestion-control threshold message-queue-wait-time

Sets all max-queue-wait-time thresholds to the default values.

- **critical time**
  Default: 5
  The critical threshold value for the maximum time (in seconds) that messages can be held in queue as measured by packet time stamps.
  
  *time* is measured in seconds and can be an integer from 1 through 30.

- **major time**
  Default: 0
  The major threshold value for the maximum time (in seconds) that messages can be held in queue as measured by packet time stamps.
  
  *time* is measured in seconds and can be an integer from 1 through 30.
**minor time**

Default: 0

The minor threshold value for the maximum time (in seconds) that messages can be held in queue as measured by packet timestamps.

*time* is measured in seconds and can be an integer from 1 through 30.

**Usage Guidelines**

Use this command to set the critical, major and minor threshold levels for the maximum time (in seconds) messages can be held in queue.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed a congestion action-profile is invoked, if configured.

This command requires a valid product license.

**Examples**

The following command configures a major threshold level of 4 seconds.

```
congestion-control threshold message-queue-wait-time major 4
```

This setting will remain in configuration unless you specify another minor threshold level in place of 4.

The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold message-queue-wait-time
```
congestion-control threshold mmemgr-average-cpu-utilization

Configures MMEMgr-specific thresholds to monitor the MMEMgrs' average CPU utilization.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
congestion-control threshold mmemgr-average-cpu-utilization { critical percent | major percent | minor percent }
| default | no | congestion-control threshold mmemgr-average-cpu-utilization { critical | major | minor }
```

default
- Resets the configured thresholds to the system defaults.

no
- Disables the configured thresholds and removes them from the MME's configuration.

critical percent
- Default: 80
- The critical threshold value for the average percent utilization of all the CPU memory available to the MMEMgr measured in 10-second intervals.
- percent can be configured to any integer value from 1 to 100.

major percent
- Default: 0
- The major threshold value for the average percent utilization of all the CPU memory available to the MMEMgr measured in 10-second intervals.
- percent can be configured to any integer value from 0 to 100.
**minor percent**

Default: 0

The minor threshold value for the average percent utilization of the all the CPU memory available to the MMemgr measured in 10-second intervals.

*percent* can be configured to any integer value from 1 to 100.

**Usage Guidelines**

Use this command to set the critical, major and minor threshold levels of average percent utilization of all CPU memory available to the MMemgrs as measured in 10-second intervals.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked.

The most commonly recommended threshold for the MMemgr is the service CPU utilization. This is reflective of the MMemgr's CPU usage since all MMemgrs are located on demux cards.

**Examples**

Use a command similar to the following to set a critical threshold of 89% for MMemgr CPU usage:

`congestion-control threshold mmemgr-average-cpu-utilization critical 89`
congestion-control threshold port-rx-utilization

Configures the congestion thresholds for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

Important
This command applies to ePDG (version 14.1 and higher).

Product  ePDG

Privilege  Security Administrator, Administrator

Command Modes  Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local] host_name(config) #

Syntax Description
congestion-control threshold port-rx-utilization { critical percent | major percent | minor percent }
default congestion-control threshold port-rx-utilization

default congestion-control threshold port-rx-utilization
Sets all port-rx-utilization thresholds to the default values.

critical percent
Default: 80
The critical threshold value for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.
percent can be configured to any integer value from 0 to 100.

major percent
Default: 0
The major threshold value for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.
percent can be configured to any integer value from 0 to 100.
**minor percent**

Default: 0

The minor threshold value for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

*percent* can be configured to any integer value from 0 to 100.

**Usage Guidelines**

Use this command to set the critical, major and minor threshold levels of average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

This command requires a valid product license.

**Examples**

The following command configures a minor threshold level of 25%.

```
congestion-control threshold port-rx-utilization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25.

The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold port-rx-utilization
```
congestion-control threshold port-specific

Configures the congestion thresholds for specific port utilization.

---

**Important**

This command applies to ePDG (version 14.1 and higher).

---

**Product**

ePDG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] \*host_name*(config)#

**Syntax Description**

congestion-control threshold port-specific { slot/port [ tx-utilization { critical percent | major percent | minor percent | rx-utilization { critical percent | major percent | minor percent } | all { critical percent | major percent | minor percent } ] }

no congestion-control threshold port-specific { slot/port { critical | major | minor } | all { critical | major | minor } }

Sets all port-specific utilization thresholds to the default values.

**slot/port**

Default: Disabled

Specifies the port for which port specific threshold monitoring is being configured. The slot and port must refer to an installed card and port. If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is applied system-wide.

**all**

Set threshold monitoring for all ports on all cards.
rx-utilization
Set threshold monitoring for received data only.

tx-utilization
Set threshold monitoring for transmitted data only.

critical percent
Default: 80
The critical threshold value for average percent utilization of the specified port resources as measured in 5-minute intervals.
_percent can be configured to any integer value from 0 to 100.

major percent
Default: 0
The major threshold value for average percent utilization of the specified port resources as measured in 5-minute intervals.
_percent can be configured to any integer value from 0 to 100.

minor percent
Default: 0
The minor threshold value for average percent utilization of the specified port resources as measured in 5-minute intervals.
_percent can be configured to any integer value from 0 to 100.

Usage Guidelines
Use this command to set the critical, major and minor threshold levels of average percent utilization of specified resources for all ports by transmitted data as measured in 5-minute intervals.
Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.
This command requires a valid product license.

Examples
The following command configures a minor threshold level of 5% for received data on port 1 of the card in slot 17.
congestion-control threshold port-specific 17/1 rx-utilization minor 5
This setting will remain in configuration unless you specify another minor threshold level in place of 5.
congestion-control threshold port-rx-utilization

Configures the congestion thresholds for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

Important

This command applies to ePDG (version 14.1 and higher).

Product  
ePDG

Privilege  
Security Administrator, Administrator

Command Modes  
Exec > Global Configuration  
configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

Syntax Description

congestion-control threshold port-rx-utilization { critical percent | major percent | minor percent }

default congestion-control threshold port-rx-utilization

Sets all port-rx-utilization thresholds to the default values.

critical percent

Default: 80

The critical threshold value for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

percent can be configured to any integer value from 0 to 100.

major percent

Default: 0

The major threshold value for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

percent can be configured to any integer value from 0 to 100.
**minor percent**

Default: 0

The minor threshold value for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

*percent* can be configured to any integer value from 0 to 100.

**Usage Guidelines**

Use this command to set the critical, major and minor threshold levels of average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

This command requires a valid product license.

**Examples**

The following command configures a minor threshold level of 25%.

```
congestion-control threshold port-rx-utilization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25.

The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold port-rx-utilization
```
congestion-control threshold port-tx-utilization

Configures the congestion thresholds for average percent utilization of port resources for all ports by transmitted data as measured in 5-minute intervals.

---

**Important**

This command applies to ePDG (version 14.1 and higher).

---

**Product**

ePDG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

- `congestion-control threshold port-tx-utilization { critical percent | major percent | minor percent }`
- `default congestion-control threshold port-tx-utilization`

Sets all port-tx-utilization thresholds to the default values.

- `critical percent`
  
  Default: 80
  
  The critical threshold value for average percent utilization of port resources for all ports by transmitted data as measured in 5-minute intervals.
  
  `percent` can be configured to any integer value from 0 to 100.

- `major percent`
  
  Default: 0
  
  The major threshold value for average percent utilization of port resources for all ports by transmitted data as measured in 5-minute intervals.
  
  `percent` can be configured to any integer value from 0 to 100.
**minor percent**
Default: 0
The minor threshold value for average percent utilization of port resources for all ports by transmitted data as measured in 5-minute intervals.

*percent* can be configured to any integer value from 0 to 100.

**Usage Guidelines**
Use this command to set the critical, major and minor threshold levels of average percent utilization of port resources for all ports by transmitted data as measured in 5-minute intervals.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

This command requires a valid product license.

**Examples**
The following command configures a minor threshold level of 25%.

```
congestion-control threshold port-tx-utilization minor 25
```
This setting will remain in configuration unless you specify another minor threshold level in place of 25.

The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold port-tx-utilization
```
congestion-control threshold service-control-cpu-utilization

Configures the congestion thresholds for average percent utilization of CPUs on which a Demux Manager software task instance is running as measured in 10-second intervals.

Important

This command applies to MME (version 14.0 and higher) and ePDG (version 14.1 and higher).

Product

MME
ePDG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local]\host_name(config)#

Syntax Description

congestion-control threshold service-control-cpu-utilization { critical percent | major percent | minor percent }
default congestion-control threshold service-control-cpu-utilization
default congestion-control threshold service-control-cpu-utilization

Sets all service-control-cpu-utilization thresholds to the default values.

critical percent

Default: 80
The critical threshold value for average percent utilization of CPUs on which a Demux Manager software task instance is running as measured in 10-second intervals.

percent can be configured to any integer value from 0 to 100.

major percent

Default: 0
The major threshold value for average percent utilization of CPUs on which a Demux Manager software task instance is running as measured in 10-second intervals.
percent can be configured to any integer value from 0 to 100.

**minor percent**

Default: 0

The minor threshold value for average percent utilization of CPUs on which a Demux Manager software task instance is running as measured in 10-second intervals.

percent can be configured to any integer value from 0 to 100.

**Usage Guidelines**

Use this command to set the critical, major and minor threshold levels of average percent utilization of CPUs on which a Demux Manager software task instance is running as measured in 10-second intervals.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

When the service-control-cpu-utilization critical threshold setting is exceeded, ipsecmgrs running in the congested CPU are notified of the congestion. The ipsecmgrs raise traps for service-congestion exceeded and update the NPU so that no new calls are sent to those ipsecmgrs. The NPU does not send any new calls to the congested ipsecmgrs. However, if all ipsecmgrs are congested the action is always drop regardless of the setting for congestion policy action. The packet drops are silently done by the NPU.

When ipsecmgrs are congested and an NPU receives a packet whose Security Parameter Index, Initiator (SPIi) in IKE_SA_INIT matches that of a currently established session, the packet is classified as belonging to the existing session. Since congestion action is applied only on new sessions, such IKE_SA_INIT packets are allowed to create sessions. If the IKE_SA_INIT uses an SPIi which does not match any of the existing sessions, it is processed according to the congestion policy action.

This command requires a valid product license.

**Examples**

The following command configures a minor threshold level of 25%.

```congestion-control threshold service-control-cpu-utilization minor 25```

This setting will remain in configuration unless you specify another minor threshold level in place of 25.

The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold service-control-cpu-utilization```


congestion-control threshold system-cpu-utilization

Configures the congestion thresholds for average percent CPU utilization of all packet processing cards available to the system as measured in 10-second intervals.

**Important**

This command applies to MME (version 14.0 and higher) and ePDG (version 14.1 and higher).

**Product**

MME

ePDG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
congestion-control threshold system-cpu-utilization { critical percent | major percent | minor percent }
default congestion-control threshold system-cpu-utilization
```

**default congestion-control threshold system-cpu-utilization**

Sets all system-cpu-utilization thresholds to the default values.

**critical percent**

Default: 80

The critical threshold value for average percent CPU utilization of all packet processing cards available to the system.

percent can be configured to any integer value from 0 to 100.

**major percent**

Default: 0

The major threshold value for average percent CPU utilization of all packet processing cards available to the system.

percent can be configured to any integer value from 0 to 100.
**minor percent**

Default: 0

The minor threshold value for average percent CPU utilization of all packet processing cards available to the system.

*percent* can be configured to any integer value from 0 to 100.

**Usage Guidelines**

Use this command to set the critical, major and minor threshold levels of average percent CPU utilization of all packet processing cards available to the system as measured in 10-second intervals.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

This command requires a valid product license.

**Examples**

The following command configures a minor threshold level of 25%.

```
congestion-control threshold system-cpu-utilization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25.

The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold system-cpu-utilization
```
congestion-control threshold system-memory-utilization

Configures the congestion thresholds for the average percent utilization of all CPU memory available to the system as measured in 10-second intervals.

Important
This command applies to MME (version 14.0 and higher) and ePDG (version 14.1 and higher).

Product
MME
ePDG

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local]host_name(config)#

Syntax Description
congestion-control threshold system-memory-utilization { critical percent | major percent | minor percent }
default congestion-control threshold system-memory-utilization
default congestion-control threshold system-memory-utilization
Sets all system-memory-utilization thresholds to the default values.

critical percent
Default: 80
The critical threshold value for the average percent utilization of all CPU memory available to the system as measured in 10-second intervals.
percent can be configured to any integer value from 0 to 100.

major percent
Default: 0
The major threshold value for the average percent utilization of all CPU memory available to the system as measured in 10-second intervals.
percent can be configured to any integer value from 0 to 100.

**minor percent**

Default: 0

The minor threshold value for the average percent utilization of all CPU memory available to the system as measured in 10-second intervals.

percent can be configured to any integer value from 0 to 100.

**Usage Guidelines**

Use this command to set the critical, major and minor threshold levels of average percent utilization of all CPU memory available to the system as measured in 10-second intervals.

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

This command requires a valid product license.

**Examples**

The following command configures a minor threshold level of 25%.

```
congestion-control threshold system-memory-utilization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25.

The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold system-memory-utilization
```
congestion-control threshold tolerance

Configures the percentage under a configured threshold value that dictates the point at which the condition is cleared.

Important
This command applies to MME (version 14.0 and higher) and ePDG (version 14.1 and higher).

Product
MME
ePDG

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local]host_name(config)#

Syntax Description
congestion-control threshold tolerance { critical percent | major percent | minor percent }
default congestion-control threshold system-cpu-utilization

default congestion-control threshold tolerance
Sets all threshold tolerances to the default values.

critical percent
Default: 10
The tolerance percentage for critical thresholds. When a critical threshold drops below this level, the condition is cleared.
percent can be configured to any integer value from 0 to 100.

major percent
Default: 0
The tolerance percentage for major thresholds. When a major threshold drops below this level, the condition is cleared.
percent can be configured to any integer value from 0 to 100.
**minor percent**

Default: 0

The tolerance percentage for minor thresholds. When a minor threshold drops below this level, the condition is cleared.

`percent` can be configured to any integer value from 0 to 100.

**Usage Guidelines**

Use this command to set the tolerance limits for critical, major and minor thresholds.

The tolerance parameter establishes the threshold at which the condition is cleared. An SNMP trap (starCongestionClear) is generated for the clear condition.

This command requires a valid product license.

**Examples**

The following command configures the tolerance level of 5% for minor thresholds.

```
congestion-control threshold tolerance minor 5
```

This setting will remain in configuration unless you specify another tolerance for minor thresholds in place of 5.

The following command returns the critical, major, and minor threshold tolerance levels to their default values:

```
default congestion-control threshold tolerance
```
connectedapps

Enables the configuration of Connected Apps (CA) client communication with the IOS-XR CA server on an ASR 9000. This command sends you to the Connected Apps Configuration mode.

**Product**
SecGW (WSG)

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
`connectedapps`

**Usage Guidelines**
Use this command to go to the Connected Apps Configuration mode. In this mode you can set CA client session parameters and ASR 9000 VSM High Availability (HA) chassis and network modes.

**Examples**
The following command sends you to the Connected Apps Configuration mode:

```
connectedapps
```
content-filtering category database directory

This command configures the base directory to be used for storing all content-rating databases that are required for Category-based Content Filtering application.

**Product** CF

**Privilege** Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration
- `configure`

Entering the above command sequence results in the following prompt:

```
[local]/host_name(config)>
```

**Syntax Description**
- `content-filtering category database directory path directory_path`
- `default content-filtering category database directory path`

- `default`
  Specifies the default base directory and directory path for Category-based Content Filtering application.

- `directory_path`
  Default: `/pcmcia1/cf`
  Specifies the base directory and its path to store all of the full or incremental content rating databases for the Category-based Content Filtering application. `directory_path` must be an alphanumeric string of 1 through 255 characters.

**Usage Guidelines**
Use this command to specify the directory and its path to download all full or incremental category-rating databases to be used for the Category-based Content Filtering application.

Merging of incremental database can be done as part of the database upgrade process performed with `upgrade content-filtering category database` command in the Executive Mode.

**Examples**
The following command configures the `/flash/cf_temp/DB` as the base directory to download all full and incremental content-rating databases for content filtering application.

```
content-filtering category database directory path /flash/cf_temp/DB
```
content-filtering category database max-versions

This command configures the number of full content-rating databases to maintain/archive in the base directory for category-based content filtering application.

Product

CF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

content-filtering category database max-versions num_archive
default content-filtering category database max-versions

default
Sets the default number of full databases for specified directory path/location.

num_archive
Default: 2
Specifies the maximum number of database to be archived or maintained in the specific location.
num_archive must be an integer from 1 through 3.

Usage Guidelines

Use this command to set the number of full content-rating database to be maintained in the specified directory path with the base file name specified using the content-filtering database override file command. The specified directory path is the location specified using the content-filtering category database directory path command.

Examples

The following command configures the system to maintain 3 full content-rating databases for category-based content filtering application.
content-filtering category database max-versions 3
content-filtering category database override

This command specifies the name of a file to be used by the category-rating database load process for category-based content filtering application.

**Product**

CF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

`content-filtering category database override file file_name.extension`

default

`content-filtering category database override file`

default

Sets the default content rating database file name; for example, optcmd.bin.

`file file_name.extension`

Specifies the header of the file in the database directory path location to determine the newest full database.

`file_name` must be an alphanumeric string of up to 10 characters with an extension of 3 characters after a period (.) as `extension`.

**Usage Guidelines**

Use this command to configure the category-rating database file name to determine the newest version of full database. A process called "LOAD_DATABASE" invokes during the system startup or the database upgrade process by `upgrade content-filtering category database` command in Executive Mode. This process examines the header of each of the files in the database folder specified by `content-filtering category directory path` command in this mode.

Note that by default system examines the header of those files only which begins with the string "OPTCMDB" and having extension ".bin".

**Examples**

The following command configures the system to examine the header of files that begins with `CF_sta.DB` only for content filtering application.

`content-filtering category database override file CF_sta.DB`
context

Creates or specifies an existing StarOS context and enters the Context Configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local]/host_name(config)#

Syntax Description
context context_name | -noconfirm |
no context context_name

no
Removes the specified context from the configuration.

name
Specifies the name of a context to enter, add, or remove. When creating a new context, the context name must be unique.

Important
When creating a new context, the context_name specified must not conflict with the name of any existing context or domain names.

-noconfirm
Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage Guidelines
Use this command to create or remove a specified context and enter the COntext configuration mode.

Important
You can create a maximum of 64 contexts.
Examples

The following command creates a context named sampleContext:

```
context sampleContext
```
**crash enable**

Enables or disables the copying of crash data to a specified location.

**Product**  
All

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**  
```
crash enable { async-core-transfer | [ encrypted ] url crash_url ] | filename-pattern pattern | [ restrict mbyte ]
```

**no**

Disables the specified option.

**Important**  
System crash information is generated and stored in the crash list even when the `no` keyword is specified. The information maintained in the crash lists is minimal crash information when the `no` keyword has been specified.

**async-core-transfer**  
Maintains the transfer of the core dump to the management card while asynchronously beginning proclet recovery which can reduce the total outage. This feature is enabled by default.

**Important**  
When a proclet crashes, a minimum 10% of the available total memory must be free in the CPU to start a new or rename the standby proclet.

**encrypted**  
Indicates that the URL is encrypted for security reasons.
filename-pattern pattern

The filename-pattern is an alphanumeric string containing any or all of the following variables:

- `%hostname%` - The system hostname.
- `%ip%` - A SPIO IP address
- `%cpu%` - CPU number
- `%card%` - Card number
- `%time%` - POSIX timestamp in hexadecimal notation
- `%filename%` - Alias for crash-%card%-%cpu%-%time-core%
- `%%` - A single % sign

If no pattern is specified, the result is the same as the pattern filename.

Use '/' characters in the filename pattern part to store crashes in per-system subdirectories.

url crash_url

Specifies the location to store crash files. crash_url may refer to a local or a remote file. crash_url must be entered using the following format:

For the ASR 5000:

- [file:] {/flash|/pcmcia1|/hd}[/directory]/
- [tftp://{host[:port#]}/][directory]/
- [ftp: | sftp://][username[:password]@[host]:port#]/[directory]/

For the ASR 5500:

- [file:] {/flash|/usb1|/hd}[/directory]/
- [tftp://{host[:port#]}/][directory]/
- [ftp: | sftp://][username[:password]@[host]:port#]/[directory]/

Important Use of the ASR 5000 SMC hard drive is not supported in this release.

Important Do not use the following characters when entering a string for the field names below: "/" (forward slash), ":" (colon) or "@" (at sign).

directory is the directory name.
filename is the actual file of interest.
username is the user to be authenticated.
password is the password to use for authentication.
host is the IP address or host name of the server.
**port#** is the logical port number that the communication protocol is to use.

**restrict mbyte**
Specifies a maximum amount of memory (in megabytes) to use for storing crash files as an integer from 1 through 128. Default: 128

The **restrict** keyword is only applicable to local URLs.

**Usage Guidelines**
Enable crashes if there are systems that are not stable and the crash information will be useful for troubleshooting. The remote storage of the crash file reduces the memory utilized on the chassis.

**Examples**
The following command saves a maximum of 64 megabytes of crash data to the /flash drive:
```
crash enable url /flash/pub/data/crash.dmp restrict 64
```
crypto blacklist file

Configures a blacklist (access denied) file to be used by a Wireless Security Gateway (WSG).

**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

---

**Command Modes**

Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description**

```
crypto blacklist file pathname
no crypto blacklist file

no
```

Removes the blacklist file from the system.

```
pathname
```

Specifies the location of the blacklist file as:

- `| file: {[/flash|/usb1|/hd-raid]}/[directory]/<filename>
- `| tftp://[/host[/port]]/[directory]/<filename>
- `| ftp: | sftp: //[/username[/password[@]] [/host[/port]]/[directory]/<filename>
- `| http://[/<username>[<password>@] ][/host[/port]]/[directory]/<filename>

---

**Usage Guidelines**

Use this command to configure the location of the blacklist file to be used by a WSG.

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*.

**Important**

Either a blacklist, a whitelist or none is configured. Both listing techniques cannot be used simultaneously on the system.

**Examples**

The following command specifies the use of a crypto backlist file on the /flash drive:

```
crypto blacklist file /flash/pub/data/blacklist.txt
```
crypto peer-list

Enables an SecGW to initiate an IKEv2 session setup request when the peer does not initiate a setup request within a specified time interval. Executing this command moves you to the Peer List Configuration mode. This functionality is only applicable for site-to-site (S2S) based tunnels within a WSG service. For remote access tunnels the peer is always the initiator. (VPC-VSM only)

Product
SecGW (WSG)

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

| no | crypto peer-list {ipv4 | ipv6} peer_list_name |

no
Disables the specified crypto peer list.

peer_list_name
Specifies the name of the peer list as an alphanumeric string of one through 32 characters.

Usage Guidelines
Use this command to enable an SecGW to initiate an IKEv2 session setup request when the peer does not initiate a setup request within a specified time interval. Executing this command moves you to the Peer List Configuration mode. This functionality is only applicable for site-to-site (S2S) based tunnels within a WSG service. For remote access tunnels the peer is always the initiator. (VPC-VSM only)

The following restrictions apply when configuring an SecGW as an Initiator:

• The peer-list peer_list_name command is only executed if the deployment mode for WSG service is site-to-site, and the bind address type matches with the peer list address type (IPv4 or IPv6).

• You cannot change the WSG service deployment-mode if peer-list peer_list_name is enabled under the service. You will be prompted to remove the peer list before changing the mode.

• A maximum of 1,000 peer IP addresses can be added to the peer list via the Peer List Configuration mode address command.
• WSG service address binding is not allowed if a peer list is configured and both address types do not match. An error message is generated if they do not match.

• An IPv4 or IPv6 peer list cannot be modified if peer-list peer_list_name is enabled under the WSG service.

When a peer list has been configured in the WSG service, the initiator and responder mode timer intervals each default to 10 seconds. The SecGW will wait for 10 seconds in the responder mode for a peer session initiation request before switching to the initiator mode and waiting 10 seconds for a peer response.

You can change the default settings for the initiator and/or responder mode intervals using the WSG Service Configuration mode initiator-mode-duration and responder-mode-duration commands.

For additional information, refer to the Peer List Configuration Mode Commands and WSG Service Configuration Mode Commands chapters of this guide. Also see the Security Gateway as Initiator chapter in the IPSec Reference.

Examples

The following command enables SecGW as an Initiator functionality and creates an IPv4 peer list named peer1.

crypto peer-list ipv4 peer1
**crypto remote-secret-list**

Specifies the remote secret list for storing remote secrets based on the ID type. This command sends you to the Remote Secret List Configuration mode. Only one active remote-secret-list is supported per system.

**Product**

All products supporting IPSec remote secrets

---

**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

`configure`

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description**

```
| no | crypto remote-secret-list  listname
```

- **no**
  
  Deletes the remote-secret-list file from the system.

---

**Important**

You must unbind the remote-secret-list from any crypto maps or templates before it can be deleted.

---

- **listname**
  
  Specifies the name of the remote secret list as an alphanumeric string from 1 to 127 characters.

---

**Usage Guidelines**

Use this command to specify the remote secret list for storing remote secrets based on the ID type. Only one remote-secret-list can be configured per system. Executing this command places you in the Remote Secret List Configuration mode.

This list of remote pre-shared keys is based on the remote ID type. The remote secret list can contain up to 1000 entries.
For additional information, refer to the *Remote Secret List Configuration Commands* chapter and the *System Administration Guide*.

**Examples**

The following command creates a remote-secret-list named *rs-list*:

```
crypto remote-secret-list rs-list
```
crypto whitelist file

Configures a whitelist (access permitted) file to be used by a Wireless Security Gateway (WSG).

**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

**Command Modes**

Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
crypto whitelist file pathname [-noconfirm ]
no crypto whitelist file

no

Removes the blacklist file from the system.

pathname

Specifies the location of the whitelist file as:

- `| file: ||[/flash|/usb1[/hd-raid]][/directory]/<filename>
- `tftp://[host[:port#]][/directory]/<filename>
- `ftp:|sftp://[username[:password[@]] [host[[:port#]][/directory]/<filename>
- `http://[<username>@]<host[[:port#]][/directory]/<filename>

**Usage Guidelines**

Use this command to configure the location of the white file to be used by a WSG.

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*.

**Important**

Usually either a blacklist, a whitelist or none is configured. Both listing techniques cannot be used simultaneously on the system.

**Examples**

The following command specifies the use of a crypto whitelist stored on the /flash drive.

```plaintext
crypto whitelist file /flash/pub/data/whitelist.txt
```
This command creates/removes an HNB-CS network configuration instance for Famed UMTS access over Iu-CS/Iu-Flex interface between Home NodeB Gateway (HNB-GW) service and CS networks elements; i.e. MSC/VLR. This command also configures an existing HNB-CS network instance and enters the HNB-CS Network Configuration mode on a system.

**Product**

HNBGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`cs-network cs_instance [-noconfirm]`

`no cs-network cs_instance`

`no`

Removes the specified HNB-CS network instance from the system.

**Caution**

Removing the HNB-CS network instance is a disruptive operation and it will affect all UEs accessing MSC(s) configured in specific CS core network through the HNB-GW service.

**Caution**

If any HNB-CS Network instance is removed from system all parameters configured in that mode will be deleted and Iu-CS/Iu-Flex interface will be disabled.

**cs_instance**

Specifies the name of the Circuit Switched Core Networks instance which needs to be associated with the HNB Radio Network PLMN via the HNB RN-PLMN Configuration mode. If `cs_instance` does not refer to an existing HNB-PS network instance, the new HNB-CS network instance is created.

`cs_instance` must be an alphanumeric string of 1 through 63 characters.
-noconfirm
Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage Guidelines
Use this command to enter the HNB-CS Network Configuration mode for an existing CS network instance or for a newly defined HNB-CS network instance. This command is also used to remove an existing HNB-CS network instance.

This configuration enables/disables the Iu-CS/Iu-Flex interface on HNB-GW service with CS core network elements; i.e. MSC/VLR.

A maximum of one HNB-CS network instance per HNB-GW service instance which is further limited to a maximum of 256 services (regardless of type) can be configured per system.

Caution
This is a critical configuration. The HNBs cannot access MSC(s) in CS core network without this configuration. Any change to this configuration would lead to disruption in HNB access to CS core network.

Entering this command results in the following prompt:

```
{context_name}@hostname(config-cs-network)#
```

The various parameters available for configuration of an HNB-CS network instance are defined in the HNB-CS Network Configuration Mode Commands chapter.

Examples
The following command enters the existing HNB-CS Network configuration mode (or creates it if it does not already exist) for the instance named hnb-cs1:

```
cs-network hnb-cs1
```

The following command will remove HNB-CS network instance hnb-cs1 from the system without any warning to operator:

```
no cs-network hnb-cs1
```
css acsmgr-selection-attempts

This is a restricted command. In 9.0 and later releases this command is obsolete.
css delivery-sequence

This is a restricted command. In 9.0 and later releases this command is obsolete.
css service

This is a restricted command. In 9.0 and later releases this command is obsolete.
**diameter dynamic-dictionary**

This command allows configuring a Diameter dictionary dynamically at run time, and then loading the dynamic dictionary into the system.

---

**Important**

The maximum number of dynamic dictionaries that can be loaded into the system is 10.

---

**Product**

- GGSN
- HA
- HSGW
- IPSG
- PDSN
- P-GW
- SAEGW
- S-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

- `diameter dynamic-dictionary name url`
- `no diameter dynamic-dictionary name`

**no**

Unloads the specified dynamic Diameter dictionary from the system.

**name**

Specifies the name of the dynamic Diameter dictionary as an alphanumeric string of 1 through 15 characters.
url

Specifies the URL of the Diameter dictionary to be loaded into the system. The input must be an alphanumeric string of 1 through 127 characters.

Usage Guidelines

This command is used to define a new Diameter dictionary on the fly, and load the dynamic dictionary in to the system.

To perform this configuration, you should first create a text file in ABNF format and configure all the required Diameter AVPs and command codes in the file. Then, save the file in flash or some URL that will be accessible by the system.

Now, configure a dynamic dictionary with an unique name and map it to the URL of the file to be loaded dynamically in to the system at the global configuration level.

When the names of the dynamic dictionaries and their URLs are configured, the corresponding files at the respective URLs are parsed and populated in all SessMgr and AAAMgr facilities as new dictionaries and kept available to be used when these dictionary names are configured under any Diameter application level or AAA group.

When a dynamic dictionary name is configured under an application such as IMS authorization service or in a AAA group, the corresponding dictionary (which is already loaded in SessMgrs and AAAMgrs) entry will be used.

There will be only one instance of a dynamic dictionary loaded in to a task for one dynamic dictionary name even if the same dictionary name is configured in multiple AAA groups or multiple application configurations. That is, even if the same dictionary name is configured in several applications or several AAA groups, all these applications and AAA groups will refer to the same dynamic dictionary instance.

Examples

The following command configures a Diameter dictionary named dyn1 and loads this dictionary to /flash/diameter_custom1.sndd path:

```
diameter dynamic-dictionary dyn1 /flash/diameter_custom1.sndd
```
**diameter-host-template**

Specifies the name of a Diameter host template and enters the Diameter Host Select mode. A Diameter host template is a table of peer servers that can be shared by multiple services.

### Product

<table>
<thead>
<tr>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>GGSN</td>
</tr>
<tr>
<td>HA</td>
</tr>
<tr>
<td>HSGW</td>
</tr>
<tr>
<td>IPSG</td>
</tr>
<tr>
<td>PDSN</td>
</tr>
<tr>
<td>P-GW</td>
</tr>
<tr>
<td>SAEGW</td>
</tr>
<tr>
<td>S-GW</td>
</tr>
</tbody>
</table>

### Privilege

Security Administrator, Administrator

### Command Modes

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

### Syntax Description

- `diameter-host-template name [-noconfirm ]`
- `no diameter-host-template name`

- **no**
  - Removes the specified Diameter host template from the Global Configuration.

- **name**
  - Specifies the name of the template as an alphanumeric string of 1 through 63 characters.

- `[-noconfirm ]`
  - Executes the command without prompting for further input from the user.
Usage Guidelines

Specifies the name of a new or existing Diameter host template and opens the Diameter Host Select mode. You can configure up to 256 templates on the system.

To use the template, Diameter applications must be associated with the template. When an association is made to the template, the system selects the Diameter peer to be contacted based on rows configured in the table and the algorithm configured for selecting rows in the table.

Important

Currently, only Gx service can be associated with the template.

If more than one service is using the same set of peer-select commands, then it is better to define all the peer selection CLIs in the template and associate the services to the template.

Entering this command results in the following prompt:

```
[context_name] hostname(config-host-template)#
```

Diameter host select configuration commands are defined in the Diameter Host Select Configuration Mode Commands chapter.

Examples

The following command specifies a Diameter host template named diamtemplate:

```
diameter-host-template diamtemplate
```
diameter-proxy ram-disk

This command configures the amount of extra RAM disk space in MB to be allocated to Diamproxy task when local storage (hard disk) is enabled.

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

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration
  - configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

**Syntax Description**
- `diameter-proxy ram-disk mb space_mb`
- `default diameter-proxy ram-disk mb`

**Syntax Description**
- `default`
  - Configures the default setting.
  - Default: 32 MB

  - `mb space_mb`
  - Specifies the storage space in MB.
  - `space_mb` must be an integer from 10 through 256.

**Usage Guidelines**
- Specifies the additional storage space to be allocated to Diamproxy for file write, in MB. The specified memory in MB is added to the existing memory allocated to Diamproxy only if HDD storage is enabled. By default, 32 MB is additionally allocated.

**Examples**
- The following command specifies that 100 MB of additional storage space be allocated to the Diamproxy task:
  - `diameter-proxy ram-disk mb 100`
ecmp-lag hash

This command provides the configuration to select source Boxer Internal Address (SBIA) as the input to the hashing function for ECMP-LAG distribution.

Product

HNBGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

[no] ecmp-lag hash use-sbia-only

no

Disables the hashing function selection and sets the system to use IP Source Address, IP Destination Address, IP Protocol and Source BIA as inputs to the hashing algorithm for ECMP-LAG distribution.

Usage Guidelines

Use this command to allow the operator to change the way hashing works in deciding which link to use for ECMP and Link Aggregation. In the default hashing algorithm the IP Source Address, IP Destination Address, IP Protocol and Source BIA are used in the hashing function. When "use-sbia-only" option is selected, only the Source BIA is used in the hashing function.

Caution

When using ECMP-LAG on a HNB-GW, this configuration is mandatory for standalone HNB-GW deployment and highly recommended in other deployment scenarios where HNB-GW is used in combination with other services.

Examples

The following command enables the SBIA as input to hash function for ECMP-LAG on the HNB-GW:

ecmp-lag hash use-sbia-only

The following commands sets the hashing function to use standard inputs for ECMP-LAG on HNB-GW:

no ecmp-lag hash use-sbia-only
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.
**enforce imsi-min equivalence**

Enables the PDSN/HA to treat IMSI and MIN as the same for identifying the PDSN/HA session.

**Product**

PDSN

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no | default | enforce imsi-min equivalence
```

**default**

Returns the command to its default setting of disabled.

**no**

Disables the PDSN/HA from treating IMSI and MIN as the same for identifying the PDSN/HA session.

**Usage Guidelines**

Generally on an HA, the IMSI and MIN are treated as different and hence the RRQs with 1x and DO PDSNs are processed as different sessions. You can use this feature to treat the IMSI and MIN with the matching lower 10-digit as the same for identifying a session. The 10-digit MIN and the 15-digit IMSI are treated as equivalent for the purpose of matching sessions if the lower 10 digits are the same. Any handoff from 1x to DO or vice-versa is treated as the same session if the NAI and HoA also match. If the NAI and/or HoA do not match, then the duplicate IMSI session detect and terminate feature is applicable.

Generally on a PDSN, the IMSI and MIN are treated as different and hence RP messages from 1x and DO PDSNs are processed as different sessions. You can use this feature to treat the IMSI and MIN with the matching lower 10-digit as the same for identifying a session. The 10-digit MIN and the 15-digit IMSI are treated as equivalent for the purpose of matching PDSN sessions if the lower 10 digits are the same. Any handoff from 1x to DO or vice-versa is treated as the same session.

**Examples**

To monitor or clear subscriber session information filtered by on IMSI/MIN refer to the `show subscribers msid` command.
This command must be executed at startup only and will not take effect when reconfigured without rebooting.

Examples

The following command enables the treatment of the IMSI and MIN as the same for identifying the session:

```
enforce imsi-min equivalence
```

Either of the following commands disables the treatment of the IMSI and MIN as the same for identifying sessions:

```
no enforce imsi-min equivalence
default enforce imsi-min equivalence
```
**exit**

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

`exit`

**Usage Guidelines**

Use this command to return to the parent configuration mode.
fa-spi-list

Replaces a duplicate Foreign Agent- Security Parameter Index (FA-SPI) remote address list applied to multiple FA services with a list name.

**Product**
- PDSN
- FA

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration
- configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no ] fa-spi-list fa_spi_list
```

- **no**
  - Disables this feature.

- **fa_spi_list**
  - Remote address list name expressed as an alphanumeric string of 1 through 64 characters.

**Usage Guidelines**

Use this command to Replace duplicate FA-SPI remote address list applied to multiple FA or HA services with a list name.

**Examples**

The following command configures the list FA SPI list to `fa-list2`:

```
fa-spi-list fa-list2
```
**fabric egress drop-threshold**

Enables or disables the generation of a syslog event message when the number of egress Fabric Access Processor (FAP) packet drops exceeds a set threshold within a window of time on an ASR 5500.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
fabric egress drop-threshold enable count number interval-secs seconds
fabric egress drop-threshold disable

disable
Enables the specified egress dropped-packet threshold settings. Settings are disabled by default.

enable
Enables the specified egress dropped-packet threshold settings. Settings are disabled by default.

count number
Specifies the maximum number of egress traffic packets that can be dropped before a syslog event message is generated. The count is specified as an integer from 10 through 5000.

interval-secs seconds
Specifies the time interval (window) within which the maximum egress packet drop count can be exceeded. The interval is specified in seconds as an integer from 30 through 600.
```

**Usage Guidelines**

Use this command to enable or disable the generation of a syslog event message when the number of egress FAP packet drops exceeds a set threshold within a window of time on an ASR 5500.

When the threshold is exceed, the syslog event message is generated once, until the condition clears. Only then will it be generated again.
By default this feature is disabled.

**Examples**

The following command sets the egress FAP dropped-packet threshold at 2000 packets within a 60-second window:

```
fabric egress drop-threshold enable count 2000 interval-secs 60
```
fabric fsc-auto-recovery

Enables or disables Fabric Storage Card (FSC) fabric recovery via automatic resets on the ASR 5500.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

```configure

```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`fabric fsc-auto-recovery { disable | enable } [ max-attempts | number_attempts | unlimited ] ]`

- `{ disable | enable }`
  - **Disable** turns off the automatic FSC recovery feature.
  - **Enable** turns on the automatic FSC recovery feature. When enabled the FSC will initiate auto recovery/reset upon detecting an excessive number of discarded fabric egress (EGQ) packets.

- `[ max-attempts | number_attempts | unlimited ] ]`
  - Specifies how many times StarOS will attempt to reset each FSC as an integer from 1 to 99 or unlimited (will not stop until FSC is reset). Default is 1.

**Usage Guidelines**

Use this command to enable or disable automatic FSC auto recovery/reset in the ASR 5500 upon detecting an excessive number of discarded egress packets. You can optionally specify the maximum number of reset attempts; the default is 1.

**Important**

To enable this feature, you must first configure the Fabric Egress Drop Threshold via the Global Configuration mode `fabric egress drop-threshold` command.

**Examples**

The following command enables FSC automatic recovery with a maximum of 50 attempts.

`fabric fsc-auto-recovery enable max-attempts 50`
failure-handling-template

This command allows the user to create/modify/delete a Diameter failure handling template at the global configuration level. This command specifies the name of failure handling template and enters the Failure Handling Template mode. The users can define the failure handling configurations within this template.

**Important**
A maximum of 64 templates can be configured on the system.

**Product**
- GGSN
- HA
- HSGW
- IPSG
- PDSN
- P-GW
- SAEGW
- S-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration
  - configure
  Entering the above command sequence results in the following prompt:
  [local]\host_name\(config)\# 

**Syntax Description**
- failure-handling-template name [ -noconfirm ]
- no failure-handling-template name

  - no
  Removes the specified failure handling template from the Global Configuration.

  - name
  Specifies the name of the failure handling template as an alphanumeric string of 1 through 63 characters.
Executes the command without prompting for further input from the user.

**Usage Guidelines**

Specifies the name of a new or existing failure handling template and opens the Failure Handling Template mode. Depending on which application is using the failure handling template, some of the syntactically possible configurations within the template are not applicable.

To use the template, Diameter applications must be associated with the template. When an association is made to the template, in the event of a failure, the system takes the action as defined in the failure handling template. Both IMS Authorization (Gx) and Diameter Credit Control Application (DCCA) (Gy) services can be associated with the template.

Entering this command results in the following prompt:

```
[context_name] hostname (config-fh-template) #
```

Failure handling template configuration commands are defined in the *Diameter Failure Handling Template Configuration Mode Commands* chapter.

**Examples**

The following command specifies a failure handling template named *FHtemplate*:

```
failure-handling-template FHtemplate
```
global-title-translation address-map

Creates an instance of a Global Title Translation (GTT) address-map, a database, for global titles (ISDN-type address) used for SCCP routing. Upon creating the instance, the system enters global title translation address-map configuration mode. For the commands to configure the database, go to the Global Title Translation Address-Map Configuration Mode Commands chapter.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#!
```

**Syntax Description**

```
[ no ] global-title-translation address-map instance instance
```

**no**

Removes the specified GTT address-map database from the SCCP portion of the configuration.

**instance**

This value uniquely identifies a specific instance of a GTT address-map.

*instance* must be an integer from 1 through 4096.

**Usage Guidelines**
Create a GTT address map with a unique identifier and enter the GTT address-map configuration mode.

**Examples**
The following command creates a GTT address map identified as 324:

```
global-title-translation address-map instance 324
```
global-title-translation association

Creates an instance of a Global Title Translation (GTT) association which defines the rules for handling global title translation. Upon creating the instance, the system enters global title translation association configuration mode. For the commands to configure the rules, go to the Global Title Translation Association Configuration Mode Commands chapter.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

global-title-translation association instance instance
no global-title-translation association instance instance

no

Removes the specified instance of a GTT association from the SCCP portion of the configuration.

instance

This value uniquely identifies a specific instance of a GTT association.

instance must be an integer from 1 through 16.

Usage Guidelines

Create a GTT association with a unique identifier and enter the GTT association configuration mode.

Examples

The following command creates a GTT association identified as 2:

global-title-translation association instance 2
gtpc-load-control-profile

Creates a GTP-C Load Control Profile and enters GTP-C Load Control Configuration Mode.

**Product**
P-GW
SAEGW
S-GW

**Privilege**
Administrator, Security Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

| no | gtpc-load-control-profile  profile_name |

**no**
Removes specified GTP-C Load Control Profile.

**gtpc-load-control-profile**
Creates a GTP-C Load Control Profile and enters GTP-C Load Control Profile Configuration Mode.

**profile_name**
Must be an alphanumeric string from 1 to 64 characters in length.

**Usage Guidelines**
Use this command to create a GTP-C Load Control Profile and enter GTP-C Load Control Profile Configuration Mode

**Examples**
The following example creates a GTP-C Load Control Profile named LOADCTRL.
```
gtpc-load-control-profile LOADCTRL
```
gtpc-overload-control-profile

Creates a GTP-C Overload Control Profile and enters GTP-C Overload Control Profile Configuration Mode.

**Product**

P-GW
SAEGW
S-GW

**Privilege**

Administrator, Security Administrator

**Command Modes**

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no ] gtpc-overload-control-profile profile_name
```

- **no**
  
  Removes specified GTP-C Overload Control Profile.

- **gtpc-overload-control-profile**
  
  Creates a GTP-C Overload Control Profile with the specified profile name.

- **profile_name**
  
  Must be an alphanumeric string from 1 to 64 characters in length.

**Usage Guidelines**

Use this command to create a GTP-C Overload Control Profile and enter GTP-C Overload Control Profile Configuration Mode.

**Examples**

This example creates a GTP-C Overload Control Profile named OVERLOADCTRL
```
gtpc-overload-control-profile OVERLOADCTRL
```
**gtpp compression-process**

This command configures the maximum number of child compression processes that AAA proxy can have.

**Product**
- GGSN
- SAEGW
- SGSN

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration
  - configure
  
  Entering the above command sequence results in the following prompt:

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

**Syntax Description**

- `gtpp compression-process max_number`
- `default gtpp compression-process`

  `default`
  
  Restores the system to the default settings for the number of child compression processes allowed.

  `max_number`
  
  Specifies the maximum number of child processes. The default is 1

  `max_number`: must be an integer from 1 through 4.

**Usage Guidelines**

This command configures the maximum number of child compression processes that AAA proxy can have only if hard disk storage is enabled.

**Examples**

- `gtpp compression-process 3`
gtpp push-to-active

This command enables/disables Push-To-Active feature to automatically transfer CDR files from new standby chassis to new active chassis when the ICSR switchover occurs.

Important
This CLI command is applicable only to GTPP groups having streaming mode.

Product
  GGSN
  P-GW
  SAEGW
  SGSN
  S-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
  configure
Entering the above command sequence results in the following prompt:
  [local]host_name(config)#

Syntax Description
  gtp pp push-to-active [ encrypted ] url via-context context_name
  no gtp pp push-to-active

  no
  Disables Push-To-Active feature to automatically transfer CDR files from new standby chassis to new active chassis.

  [ encrypted ] url
  Specifies the peer chassis URL where the CDR files are to be transferred when the chassis becomes standby.
  This keyword denotes the peer chassis URL in this format:
  sftp://user:password@host:[port]/hd-raid/records/cdr/. It accepts a string of size 1 through 1024.
  [ encrypted ] - Indicates that the URL is encrypted for security reasons.
via-context context_name

Specifies the name of the context through which the active chassis is reachable. context name must be an alphanumeric string of 1 through 79 characters.

Usage Guidelines

During an ICSR switchover, the GTPP charging interface between the active chassis and CGF server goes down and all pending CDRs are written to internal hard disk. Once the chassis becomes standby, the CDRs will remain on HDD until the chassis becomes active.

This feature provides a way to move the stranded CDRs from the new standby chassis to the new active chassis and stream them to the OCG. This CLI command enables/disables the Push-To-Active feature to automatically transfer CDR files from new standby chassis to new active chassis.

Releases prior to 16.0, CDRs from current standby chassis were manually transferred to current active chassis using the CLI command "gtpp storage-server streaming start". Once the transfer is complete, a CLI command in the Exec mode is configured to stream the CDRs to CGF.

In 16.0 and later releases, the stranded CDRs in the standby ICSR node (moved from active to standby) are automatically transferred to the newly active ICSR node. This automation process is achieved through the use of "gtpp push-to-active" CLI command in the global configuration mode.

This feature could lead to duplicate CDRs. When streaming is in progress and ICSR switchover happens, the current file being streamed, will not complete the streaming as interface with CGF went down. This file will be transferred to new active chassis and streamed from beginning from new chassis.

In case AAAProxy restarts during file transfer, the file transfer statistics will not be accurate. The accounting contexts should be in same order in both the chassis. The directory names are created using vpn-id. If the accounting contexts are in different order, vpn-id will be different and the sub-directories in HDD will be different in both the chassis for same GTPP group.

Examples

The following command enables the Push-To-Active feature to automatically transfer CDR files from new standby chassis to new active chassis.:

```bash
gtpp push-to-active url sftp://user:password@host:5000 via-context aaa
```
gtpp ram-disk-limit

This command configures additional storage space to be allocated for writing files.

**Product**
- GGSN
- SAEGW
- SGSN

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- `Exec > Global Configuration`
- `configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
- `gtpp ram-disk-limit mb mega_bytes`
- `default gtpp ram-disk-limit`
  - `default`
    - Restores the system to the default settings of 32 MB of storage.
  - `mb mega_bytes`
    - Specifies the number of megabytes of storage allocated for files.
    - `mega_bytes`: must be an integer from 10 through 256. The default is 32 MB.

**Usage Guidelines**
The memory specified with this command would be added to the existing memory allocated to the AAA proxy only if hard disk storage is enabled.

**Examples**
- `gtpp ram-disk-limit mb 256`
**gtpp single-source**

Configures the system to reserve a CPU for performing a proxy function for accounting.

**Product**
ePDG  
GGSN  
SGSN  
P-GW  
SAEGW

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration  
`configure`

Entering the above command sequence results in the following prompt:  
`[local] host_name(config)#`

**Syntax Description**

gtpp single-source | centralized-lrsn-creation | private-extensions |  
no gtpp single-source

**centralized-lrsn-creation**  
Defines Log Record Sequence Number (LRSN) generation at proxy. The AAA proxy will generate the LRSN for all CDR types generated by either the GGSN or the SGSN.  
Default: disabled

**private-extensions**  
This optional keyword enables the proprietary use of customer-specific GTPP extensions.  
If `private-extensions` is not configured, all customer specific private extensions related to GTPP message transfer with CGF and recovery through GSS are disabled.

**Important**  
In order for the customer-specific extensions to work properly, the `gtpp max-pdu-size` command in the Context Configuration Mode should be set to 65400 and the `gtpp server` command's `max` value should be set to "1".
**no**

Disables GTPP single-sourcing. This is the default setting.

---

⚠️ **Caution**

Entering this command while PDP contexts are in process could cause the loss of pending CDRs. The configuration must be saved and the chassis reloaded for this option to take effect.

---

**Usage Guidelines**

When GTPP single-sourcing is enabled, the system's AAA proxy function generates requests to the accounting server using a single UDP source port number, instead of having each AAA Manager generate independent requests with unique UDP source port numbers. This is accomplished by the AAA Managers forwarding their GTPP PDUs to the AAA Proxy function that runs on a reserved packet processing card CPU. Since a packet processing card CPU is being reserved, fewer Session Managers and AAA Managers will be started on that card.

⚠️ **Caution**

This command must be entered prior to the configuration of other services. Specifying it later may return an error due to a lack of CPU availability.

---

**Examples**

The following command enables GTPP single-sourcing with the use of private GTPP extensions:

```
  gtppp single-source private-extensions
```

The following command disables GTPP single-sourcing:

```
  no gtppp single-source
```
ha-spi-list

Replaces a duplicate Home Agent-Security Parameters Index (HA-SPI) remote address list applied to multiple HA services with a list name.

**Product**
- PDSN
- HA

**Privilege**
- Security Administrator
- Administrator

**Command Modes**
- Exec > Global Configuration
- configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
ha-spi-list  ha_spi_list
```

- `ha_spi_list`
  Remote address list name expressed as an alphanumeric string of 1 through 64 characters.

**Usage Guidelines**

Use this command to Replace duplicate HA-SPI remote address list applied to multiple HA services with a list name.

**Examples**

The following command configures the list HA SPI list to `ha-list2`:
```
ha-spi-list ha-list2
```
hd raid

Performs RAID management operations on the platform's hard disk drives.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

For the ASR 5000:

```
hd raid { default { overwrite { invalid disk | unknown disk | valid disk } | quarantine | select } | overwrite
{ invalid disk | unknown disk | valid disk } | quarantine { directory pathname | limit number_files | mtime minutes } | select { newer disk | none disk } } [-noconfirm]
```

For the ASR 5500:

```
hd raid { default { overwrite { invalid disk | unknown disk | valid disk } | quarantine } | overwrite
{ invalid disk | unknown disk | valid disk } | quarantine { directory pathname | limit number_files | mtime minutes } } [-noconfirm]
```

For VPC:

```
hd raid { default { overwrite { invalid disk | unknown disk | valid disk } | quarantine | select } | overwrite
{ invalid disk | unknown disk | valid disk } | quarantine { directory pathname | limit number_files | mtime minutes } | select { local1 | local2 } } [-noconfirm]
```

default { overwrite { invalid disk | unknown disk | valid disk } | quarantine | select }

**overwrite** For the ASR 5000, this keyword sets the default overwrite option as:

- **invalid disk** – the disk with an invalid partition or RAID image (Default = On)
- **unknown disk** – the disk with an unknown RAID image (Default = Off)
- **valid disk** – the disk with a valid RAID image (Default = Off)

**overwrite** For the ASR 5500, this keyword sets the default overwrite option as:

- **invalid disk** – the disk with an invalid partition or RAID image (Default = On)
- **unknown disk** – the disk with an unknown RAID image (Default = On)
• **valid disk** – the disk with a valid RAID image (Default = On)

**quarantine** This keyword is not supported on the ASR 5000. On the ASR 5500 it is disabled by default. When enabled without any options, it restores default quarantine parameters (directory = lost+found; limit = 3000 files; ntime = 5 minutes). The default parameters can be configured through other CLI keywords.

**select** sets the default disk preference when both disks contain valid RAID (ASR 5000 Default = newer disk). This keyword is not supported for the ASR 5500.

**overwrite** {invalid disk | unknown disk | valid disk }

When enabled this keyword Overwrites the specified disk and adds it to the current running RAID array.

• **invalid disk** specifies the disk with an invalid partition (empty, incorrectly partitioned or partially constructed) or RAID image.

• **unknown disk** specifies the disk with an unknown RAID image that has a valid RAID superblock but is not configured in the standard way.

• **valid disk** specifies the disk with a valid RAID image that is a clean RAID component but is not part of the current or selected RAID.

**select** { newer disk | none disk }

On the ASR 5000, selects the specified disk to assemble a RAID when two unrelated RAID disks are present in the system. The resulting RAID runs in degraded mode.

• **newer disk** specifies the newest disk by timestamp and event counter in superblocks. if all are the same, the array will start with both disks. A different array will need administrator intervention.

• **none disk** indicates wait for administrator intervention.

This keyword is not supported on the ASR 5500.

**select** { local1 | local2 }

On VPC, selects the specified vHD to assemble a RAID when two or more unrelated RAID disks are present in the system. The resulting RAID runs in degraded mode.

**-noconfirm**

Executes the command without displaying "are you sure" prompts.

**Usage Guidelines**

All commands need confirmation unless the **-noconfirm** is included in the command. If the result will bring down a running RAID, you have to force the command using **-force**.

RAID commands are needed to intervene in the following situations:

• The hard disk controller task cannot determine the correct operation.

• Administrative action is required by policy.

• The administrator wants to wipe an unused disk.
In an automated system, the policies created with this CLI address the possibility of a manually partitioned disk, a disk resulting from a different version of software, a partially constructed disk, or the case of two unrelated disks in the system.

To reduce administrator intervention, a set of policies can be configured to set the default action using the commands in the HD RAID configuration mode. These commands are described in the *HD Storage Policy Configuration Mode Commands* chapter of this guide.

---

**Caution**

Use of the `hd raid` commands and keywords has the potential for deleting the contents of hard disk drives without the possibility of recovery. You should only use these commands under guidance from the Cisco Technical Assistance Center (TAC).

---

**Examples**

The following instructs StarOS to overwrite an invalid hard drive.

```
hd raid overwrite invalid disk -force
```
**hd storage-policy**

Provides access to the local hard drive configuration mode in order to manage parameters supporting local storage of records.

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

**Privilege**
Administrator

**Command Modes**
- Exec > Global Configuration

**configure**
Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
| no | hd storage-policy name
```

- **no**
  Removes a configured HD storage policy from the system.

- **storage-policy name**
  Specifies a name for an HD storage policy and then enters the HD Storage Policy Configuration Mode. `name` must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Creates a new policy or specifies an existing policy and enters the HD Storage Policy Configuration Mode. Entering this command results in the following prompt:

```
[context_name]hostname(config-hd-storage-policy)#
```

HD Storage Policy Configuration Mode commands are defined in the HD Storage Policy Configuration Mode Commands chapter.
The following command creates an HD storage policy named *policy3* and enters the HD Storage Policy Configuration Mode:

```
hd storage-policy policy3
```
**high-availability**

Configures the speed for detection of packet processing card task failures before switchover occurs.

**Product**
- PDSN
- GGSN
- ASN-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
*configure*

Entering the above command sequence results in the following prompt:

```
[local]\host_name(config)#
```

**Syntax Description**

```
high-availability fault-detection speed {aggressive | normal}
default high-availability fault-detection speed
```

- **default**
  Resets fault detection speed to normal.

- **aggressive**
  Specifies packet processing card failover should occur without performing additional checks.

- **normal**
  Specifies that packet processing card failover will only occur after additional checks have been performed. This is the default setting.

**Usage Guidelines**

Use this command to increase the fault detection speed for faster switchovers after a packet processing card task failure.

Setting fault detection speed to aggressive will trigger packet processing card failover as soon as possible if a potential failure is detected. Aggressive mode will reduce the duration of subscriber outages caused by a failed packet processing card if session recovery is enabled.

Aggressive mode also bypasses most information gathering steps and logs that can be used to determine the root cause of the failure.
In normal mode, additional checks are performed before triggering a packet processing card failover to ensure that the card has actually failed. In aggressive mode these checks are bypassed so that session recovery can start as soon as possible. These additional checks reduce the likelihood of a false positive failure.

**Examples**

The following command sets the fault detection speed for packet processing card tasks to **aggressive**:
```
high-availability fault-detection speed aggressive
```
**hybrid-mode**

Enables an ASR 5000 chassis to run a mix of Packet Services Cards (PSCs) and PSC Type A (PSCAs). When enabled, PSCAs will boot and be compatible with the PSCs as long as encryption services are disabled. The default is to run the chassis in non-hybrid mode; PSCAs will not boot when inserted in the chassis.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no | hybrid-mode [ force ] ]
```

no

Returns the chassis to non-hybrid mode. PSCAs will not boot.

force

Always updates the configuration, even if the encryption services could not be disabled. However, the PSC and PSCA cards will continue to be incompatible until encryption services are manually disabled.

**Usage Guidelines**

To allow a chassis to run in PSC/PSCA hybrid-mode with encryption services disabled you must configure `hybrid-mode force` once.

To go from hybrid mode to non-hybrid mode, you must enter the `no hybrid-mode force` command. Non-hybrid chassis mode allows encryption services to be started through the appropriate CLI commands. However, all PSCAs in the chassis will be disabled.

For additional information, see the *ASR 5000 Installation Guide*.

**Examples**

The following command enables the chassis to run a mix of PSCs and PSCAs without encryption services:

```
hybrid-mode force
```
imei-profile

Creates an instance of an International Mobile Equipment Identity (IMEI) profile.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

**Syntax Description**

```
[ no ] imei-profile imei_profile_name
```

- **no**
  - Deletes the IMEI profile instance from the configuration.

- **imei_profile_name**
  - Specifies the name of the IMEI profile as an alphanumeric string of 1 through 64 characters.

**Usage Guidelines**

Use this command to create an instance of an IMEI profile and to enter the IMEI Profile Configuration mode. An IMEI profile is a template which groups a set of device instructions, such as blacklisting, that may be applicable to one or more calling devices. See the IMEI Profile Configuration Mode Commands chapter for information regarding the definition of the rules contained within the profile and the use of the profile.

**Important**
An IMEI profile is a key element of the Operator Policy feature and is only valid when associated with at least one operator policy.

To see what IMEI profiles have already been created, return to the Exec mode and enter the `show imei-profile all` command.

**Examples**

The following command creates a configuration instance of an IMEI profile:

```
imei-profile imeiprof1
```
Global Configuration Mode Commands (L-S)

The Global Configuration Mode is used to configure basic system-wide parameters.

This section includes the commands license through system.

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

---

**Important**

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

- license, page 249
- line, page 251
- link-aggregation, page 252
- local-policy-service, page 254
- local-user allow-aaa-authentication, page 256
- local-user lockout-time, page 257
- local-user max-failed-logins, page 258
- local-user password, page 260
- local-user username, page 263
- logging console, page 267
- logging disable, page 268
- logging display, page 269
- logging filter, page 271
• logging include-uid, page 281
• logging monitor, page 284
• logging runtime, page 286
• lte-policy, page 287
• mediation-device, page 288
• network-overload-protection mme-new-connections-per-second, page 289
• network-overload-protection mme-tx-msg-rate-control, page 293
• network-overload-protection sgsn-new-connections-per-second, page 295
• network-service-entity, page 297
• ntp, page 298
• ntsr pool-id, page 299
• operator-policy, page 300
• orbem, page 302
• pac-standby-priority, page 303
• pdu-session-recovery, page 304
• peer-profile, page 306
• plugin, page 308
• port atm, page 309
• port bits, page 310
• port channelized, page 311
• port ethernet, page 312
• port mac-address virtual-base-address, page 313
• port rs232, page 315
• profile-id-qci-mapping, page 316
• ps-network, page 318
• qci, page 320
• qci-qos-mapping, page 323
• qos ip-dscp-iphb-mapping, page 325
• qos l2-mapping-table, page 327
• qos npu inter-subscriber traffic bandwidth, page 329
• qos npu inter-subscriber traffic bandwidth-sharing, page 331
• qos npu inter-subscriber traffic priority, page 333
• quality-of-service-profile, page 335
• ran-peer-map, page 337
• require active-charging, page 338
• require demux, page 340
• require detailed-rohc-stats, page 342
• require diameter-proxy, page 343
• require ecs credit-control, page 346
• require graceful-cleanup-during-audit-failure, page 348
• require ipsec-large, page 350
• require session recovery, page 351
• reveal disabled commands, page 353
• rlf-template, page 354
• rohc-profile, page 356
• sccp-network, page 358
• sctp-param-template, page 360
• session disconnect-reasons bucket-interval, page 362
• session trace, page 363
• sgsn-global, page 366
• sgsn-operator-policy, page 367
• snmp authentication-failure-trap, page 369
• snmp community, page 370
• snmp discard-snmpv3-pdu, page 372
• snmp engine-id, page 373
• snmp heartbeat, page 374
• snmp history heartbeat, page 375
• snmp mib, page 376
• snmp notif-threshold, page 377
• snmp runtime-debug, page 379
• snmp server, page 381
• snmp target, page 382
• snmp trap, page 385
• snmp trap-pdu-v1tov2, page 387
• snmp trap-timestamps, page 388
• snmp user, page 389
• ss7-routing-domain, page 391
• ssh key-size, page 393
• statistics-backup, page 394
• statistics-backup-interval, page 396
• support collection, page 397
• support record, page 399
• suspend local-user, page 401
• system, page 402
license

Configures the session license key.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description

| no | license key key_value | -force | session-limit |

no

Removes the license key(s) installed.

key key_value

Installs the license key specified by key_value. key_value is enclosed with double quotation marks (" "). The license is provided by the Cisco operations staff.

session-limit

Use this keyword to suppress fail-over calls from being rejected if the licensed threshold is crossed.

Important

This is a customer-specific command that is available for HA, PDSN, EHA, and PDIF. Please contact your local Cisco sales representative for more information.

-force

Sets the license key even if resources are not available. The system supports the dynamic resizing of demultiplexor software tasks based on the licensed session capacity and feature type. When installing a license, the system automatically attempts to resize currently functioning tasks. Warning messages are displayed if there is an issue. Though its use is not recommended, the -force keyword can be used to suppress these warning messages.
Using the **-force** keyword to install an invalid license key automatically places the license in a 30-day grace period.

**Caution**

Use of this option is not recommended.

**Usage Guidelines**

Install or update system session keys when necessary due to expiration and/or capacity needs.

**Examples**

The following command installs the license key that appears within double quotation marks:

```
license key "\VER=1\C1M=StarentSimCF\C1S=10000020\DOI=1339011659\DOE=1354866669\ISS=3
|NUM=52612\CMT=BxB_HSGW\LEC=1000\FIS=Y\FR4=Y\FTC=Y\FSR=Y\FIs=Y\FLI=Y
|FCA=Y\FTM=Y\FTP=Y\FDC=Y\FGR=Y\FAA=Y\FDQ=Y\BEP=Y\FAI=Y\FLS=Y\LGW=1000\FVN=Y
|FRE=Y\FUR=Y\FAL=Y\FST=Y\FLP=Y\FSE=Y\FIT=Y\LSE=2000\Fuz=Y\Sig=MC0CFAZdtHcnRL/
SN4hXY3CJFQy/e/JXAhUA3JWMbauC7RMF7hVJxzS0fCSXCMQ"
```
**line**

Enters the terminal display Line Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

**Syntax Description**

`line`

**Usage Guidelines**

Change the terminal display configuration based upon the users own terminal characteristics.

**Examples**

The following command enters the Line Configuration mode.

```
line
```
link-aggregation

Configures system MAC address and priority 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

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

link-aggregation { system-mac { mac_address | auto } | system-priority priority } [-noconfirm] { default | no } link-aggregation { system-mac | system-priority } [-noconfirm]

default

Resets the configuration to the default.

system-mac { mac_address | auto }

Sets the system MAC address used along with the system priority to form the system ID.

mac_address is manually entered as six groups of two hexadecimal digits separated by hyphens (for example, 01-23-45-67-89-ab).

Auto is the default and is the MAC address of the LAG master port.

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).

-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 QGLC or XGLC 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
**local-policy-service**

This command enables creating, configuring, or deleting a local QoS policy.

**Product**

P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration  
```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
local-policy-service name [ -noconfirm ]  
no local-policy-service name
```

- **no**
  
  Deletes the specified local QoS policy service from the system.

- **name**
  
  Specifies name of the local QoS policy service as an alphanumeric string of 1 through 63 characters.

  **Important**

  The `name` must be unique across all contexts.

  If the named local QoS policy service does not exist, it is created, and the CLI mode changes to the Local Policy Service Configuration Mode wherein the local QoS policy service can be configured.

  If the named local QoS policy service already exists, the CLI mode changes to the Local Policy Service Configuration Mode for that local QoS policy service.

- **-noconfirm**
  
  Specifies that the command must execute without prompting for confirmation.

**Usage Guidelines**

Use this command to specify a local QoS policy service name to allow configuration of a local QoS policy service.
**Important**  This feature is license dependent. Please contact your local sales representative for more information.

A local QoS policy service can be used to control different aspects of a session, such as QoS, data usage, subscription profiles, or server usage, by means of locally defined policies.

Local QoS policies are triggered when certain events occur and the associated conditions are satisfied. For example, when a new call is initiated, the QoS to be applied for the call could be decided based on the IMSI, MSISDN, and APN.

**Important**  A maximum of 16 local QoS policy services are supported.

Entering this command results in the following prompt:

```
[context_name] hostname(config-local-policy-service)#
```

Local Policy Service Configuration Mode commands are defined in the *Local Policy Service Configuration Mode Commands* chapter.

**Examples**

The following command creates a local QoS policy service named *lctest* and enters the Local Policy Service Configuration Mode:

```
local-policy-service lctest
```
**local-user allow-aaa-authentication**

Enables or disables the use of administrative accounts other than local-user administrative accounts.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] *host_name* (config) #

**Syntax Description**

| default | no | local-user allow-aaa-authentication |

**default**

Returns this parameter to its default setting of enabled.

**no**

Disables administrative user accounts other than local-user accounts.

**Usage Guidelines**

Local-user administrative accounts are separate from other administrative user accounts configured at the context level (Security Administrator, Administrator, Operator, and Inspector).

Context-level administrative users rely on the system's AAA subsystems for validating user names and passwords during login. This is true for both administrative user accounts configured locally through a configuration file or on an external RADIUS server.

Since the T1.276-2003 password security mechanisms are supported only for local-user administrative accounts and not for the AAA-based administrative accounts, this command provides a mechanism for disabling AAA-based administrative accounts.

By default, AAA-based administrative accounts are allowed.

**Examples**

The following command forces the system to authenticate local-user accounts based only on the information in the security account file on its CompactFlash:

no local-user allow-aaa-authentication
**local-user lockout-time**

Configures the lockout period for local-user administrative accounts.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

**Syntax Description**

local-user lockout-time time
default local-user lockout-time
default

Restores the parameter to its default setting.

time

Default: 60

Specifies the amount of time (in minutes) that must elapse before a previously locked-out local-user account can attempt to login again. *time* is an integer from 1 through 10080.

**Usage Guidelines**

Local-user administrative accounts can become locked for reasons such as exceeding the configured maximum number of login failures.

Once an account is locked, this parameter specifies the lockout duration. Once the amount of time configured by this parameter has elapsed, the local-user can once again attempt to login.

**Examples**

The following command configures a lockout time of 120 minutes (2 hours):

`local-user lockout-time 120`
local-user max-failed-logins

Configures the maximum number of failed login attempts a local-user can have before their account is locked out.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

local-user max-failed-logins number
| default | no | local-user max-failed-logins

no
Disables this functionality.

default
Restores this parameter to its default setting of 5.

number
Specifies the maximum number of times a local-user could experience a login failure before their account is locked out. number is an integer from 2 through 100. Default: 5

Usage Guidelines

This command configures the maximum number of failed login attempts a local-user can have before their account is locked out. For example if, this parameter is configured to "3" then after the third failed login attempt, the account would be locked.

Important

Local-user accounts can be configured to either enforce or reject a lockout due to the maximum number of failed login being reached. Refer to the local-user username command for more information.

Refer to the local-user lockout-time command for more information.
Examples

The following command configures a maximum of three login attempts:

```
local-user max-failed-logins 3
```
**local-user password**

Configures local-user administrative account password properties.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

*configure*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

local-user password {
[ complexity {ansi-t1.276-2003 | none } ] |
[ history length number | duration days ] |
[ max-age days ] |
[ min-change-char number ] |
[ min-change-interval days ] |
[ min-length number ] }

no local-user password {
[ history ] |
[ max-age ] |
[ min-change-interval ] }

default local-user password {
[ complexity ] |
[ history ] |
[ max-age ] |
[ min-change-char ] |
[ min-change-interval ] |
[ min-length ] }

*no*

Disables the specified parameter.

*default*

Restores the specified parameter to its default setting.

**| complexity {ansi-t1.276-2003 | none }**

Default: ansi-t1.276-2003

Specifies the password strength as one of the following:

- **ansi-t1.276-2003**: If this option is selected, the following rules are enforced:
  - Passwords may not contain the username or the reverse of the username
  - Passwords may contain no more than three of the same characters used consecutively
  - Passwords must contain at least three of the following:
    - uppercase alpha character (A, B, C, D ... Z)
    - lowercase alpha character (a, b, c, d ... z)
• numeric character (0, 1, 2, 3 …)
• special character (see the Alphanumeric Strings section of the Command Line Interface Overview chapter)

• none: Only the password length is checked. No additional password checks are performed.

[ history length number [ duration days ] ]
Default: length is 5
Specifies the number of previous password entries kept in the history list maintained by the system. A password cannot be reused if it is one of the entries kept in the history list unless the time it was last used was more than the number of days specified by the duration keyword.
If the duration keyword is not used, the only check performed by the system is that it is not in the history list. number is the number of entries for each account stored in the history list entered as an integer from 1 through 100. days is the number of days during which a password can not be reused entered an integer from 1 through 365.

[ max-age days ]
Specifies the maximum age for a password. Users logging in with a password older than the specified limit are locked out. Once the lockout period expires, at their next login attempt, they are prompted to change their password before accessing the CLI. Default: 90

days is the number of days that passwords remain valid entered as an integer from 1 through 365.

[ min-change-char number ]
Specifies the minimum number of characters that must be changed (in comparison to the current password) when a user changes their password. Default: 2

number is the number of characters entered as an integer from 0 through 16.

[ min-change-interval days ]
Specifies the frequency that passwords can be changed (other than first login).
days is the minimum number of days that must pass before a user can change their password. It is an integer from 1 through 365. Default: 1
If the **no local-user password min-change-interval** command is used, users may change their password as often as desired which could allow them to circumvent the password history function.

```
[ min-length number ]
```

Specifies the minimum length allowed for user-defined password.

*number* is the minimum number of alphanumeric characters that the password must contain, entered as an integer from 3 through 32. Default: 8

**Usage Guidelines**

This command is used to set the property requirements for user-defined passwords and system behavior in relation to those passwords.

Information pertaining to user passwords, login failures, and password history are stored on the packet processing cards and in the software's Shared Configuration Task (SCT).

The system uses the information in the SCT for runtime operations such as determining password ages and determining if new passwords meet the criteria specified by this command.

**Examples**

The following command configures a minimum password length requirement of 6 characters:

```
local-user password min-length 6
```

The following command configures the system to store the 4 most recently used passwords per user-account in the history list:

```
local-user password history length 4
```
**local-user username**

Adds or removes local-user administrative accounts.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] *host_name* (config) #

**Syntax Description**

```
local-user username name | authorization-level { administrator | inspector | operator | security-admin } ] | [ ecs | noecs | [ ftp | sftp-server | sftp-name | [ noftp | [ timeout-min-absolute time ] | [ no-lockout-login-failure | [ no-lockout-password-aging | [ password password | nopassword ] | [ timeout-min-idle time ]
```

no

Removes a previously configured user.

**name**

Specifies the name of the user as an alphanumeric string of 3 through 16 characters that is case sensitive.

```
[ authorization-level { administrator | inspector | operator | security-admin } ]
```

Default: Operator

Configures the authorization level for the user as one of the following:

- **administrator**: Administrator users have read-write privileges and can execute any command throughout the CLI except for a few security functions allowed only in the administrator mode. Administrators can configure or modify the system and are able to execute all system commands, including those available to the operator and inspector user. This level corresponds to the both the System Administrator and Application Administrator levels in the T1.276-2003.

- **inspector**: Inspector users are limited to a small number of read-only Exec Mode commands. The bulk of these are "show" commands giving the inspector the ability to view a variety of statistics and conditions.
The Inspector cannot execute show configuration commands and do not have the privilege to enter the Config Mode.

- **operator**: Operator users have read-only privileges to a larger subset of the Exec Mode commands as depicted in the following figure. Operator users can execute all commands that are part of the inspector mode, plus some system monitoring, statistical, and fault management functions. Operators do not have the ability to enter the Config Mode.

- **security-admin**: Security Administrator users have read-write privileges and can execute any command throughout the CLI. Security Administrators can execute all system commands, including those available to the administrator, operator, and inspector users. This level corresponds to both the System Security Administrator and Application Security Administrator levels in T1.276-2003.

[ **ecs | noecs** ]

Specifies whether or not the user has access to Active Charging Service configuration parameters.

- **ecs**: The user has access.
- **noecs**: The user does not have access.

Default: **ecs**

[ **ftp | noftp** ]

Default: **ftp**

Specifies whether or not the user is allowed to access the system via the File Transfer Protocol (FTP) and/or the Secure File Transfer Protocol (SFTP).

- **ftp**: The user has access.
- **noftp**: The user does not have access.

[ **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.

[ **no-lockout-login-failure** ]

Default: Disabled

Specifies that this user will never be locked out due to login attempt failures.

[ **no-lockout-password-aging** ]

Default: Disabled

Specifies that this user will never be locked out due to the age of their password.

[ **password password | nopassword** ]

Specifies the initial password for this user. **password** must an alphanumeric string of 6 through 32 characters that is case sensitive.
The user is requested to change their password upon their first login.

```
[ timeout-min-absolute time ]
Default: 0
Specifies the maximum session time (in minutes) for this user. time is an integer from 0 through 525600. A value of "0" indicates no limit.
```

```
Important
This limit applies only to the user's CLI sessions.
```

```
[ timeout-min-idle time ]
Default: 0
Specifies the maximum idle time (in minutes) for this user. time is an integer from 0 through 525600. A value of "0" indicates no limit.
```

```
Important
This limit applies only to the user's CLI sessions.
```

**Usage Guidelines**

The ability to configure administrative local-users is provided in support of the login security mechanisms specified in ANSI T1.276-2003.

Like administrative users configured at the context level, local-users can be assigned one of 4 security levels:

<table>
<thead>
<tr>
<th>Local-User Level User</th>
<th>Context Level User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Administrator</td>
<td>Administrator</td>
</tr>
<tr>
<td>Administrator</td>
<td>Config-Administrator</td>
</tr>
<tr>
<td>Operator</td>
<td>Operator</td>
</tr>
<tr>
<td>Inspector</td>
<td>Inspector</td>
</tr>
</tbody>
</table>

Local-user configuration support is handled differently from that provided for administrative users configured at the context level.

Context-level administrative users rely on the system's AAA subsystems for validating user names and passwords during login. This is true for both administrative user accounts configured locally through a configuration file or on an external RADIUS server. Passwords for these user types are assigned once and are accessible in the configuration file.

Local-user account information (passwords, password history, lockout states, etc.) is maintained in non-volatile memory and in the software's Shared Configuration Task (SCT). This information is maintained in a separate
file – not in configuration files used by the system. As such, the configured local-user accounts are not visible with the rest of the system configuration.

Local-user and context-level administrative accounts can be used in parallel.

**Examples**

The following command configures a security-administrator level local-user administrative account for a user named *User672* that has FTP privileges, a temporary password of *abc123*, and that does not lockout due to either login attempt failures or password aging:

```plaintext
local-user username User672 authorization-level security-admin ftp no-lockout-login-failure no-lockout-password-aging password abc123
```

The following command deletes a previously configured local-user administrative account called admin32:

```plaintext
no local-user username admin32
```
logging console

Enables the output of logged events to be displayed on the console terminal.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure
Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no ] logging console
```

- **no**
  Disables the output of events to the console port.

**Usage Guidelines**
Log console output to allow for offline review during system monitoring and/or trouble shooting.
logging disable

Enables/disables the logging of the specified event ID or range of IDs.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local]host_name(config)#

Syntax Description

| no | logging disable eventid | id | to | to_id |

no
Indicates the event IDs specified are to be enabled for logging.

eventid id
Specifies the event for which no logging is to occur.
In 14.1 and earlier releases, id is an integer from 1 through 202699.
In 15.0, id is an integer from 1 through 204999.
In 17.0 and later releases, id is an integer from 1 through 215999.

to to_id
Specifies the end ID of the events when a range of event ID is to be disabled from being logged. to_id must be an integer from 1 through 204999. The to_id must be equal to or larger than the id specified.

Usage Guidelines

Disable common events which may occur with a normal frequency are not of interest in monitoring the system for troubles.

Examples

The following command disables the logging the range of events from 4500 through 4599, respectively.
logging disable eventid 4500 to 4599
logging display

Configures the level of detail for information to be logged.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config) #

Syntax Description

logging display (event-verbosity (min | concise | full) | pdu-data {none | hex | hex-ascii} | pdu-verbosity pdu_level )

event-verbosity (min | concise | full)
Specifies the level of verbosity to use in logging of events as one of:

- **min**: displays minimal detail.
- **concise**: displays summary detail.
- **full**: displays all details.

pdu-data {none | hex | hex-ascii}
Specifies output format for packet data units when logged as one of:

- **none**: output in raw format.
- **hex**: displays output in hexadecimal format.
- **hex-ascii**: displays output in hexadecimal and ASCII similar to a main-frame dump.

pdu-verbosity pdu_level
Specifies the level of verbosity to use in logging of packet data units as an integer from 1 through 5, where 5 is the most detailed.
Usage Guidelines

Tune the level of information to be logged so as to avoid flooding a log file with information which is not useful or critical.

Examples

The following sets event logging to display the maximum amount of detail.

logging display event-verbosity full
logging filter

Configures the logging of events to be performed in real time for the specified facility.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`logging filter runtime facility facility level report_level [critical-info | no-critical-info | ]`

- `facility facility`
  - Specifies the facility to modify the filtering of logged information. The following list displays the valid facilities for this command:
    - `a10`: A10 interface facility
    - `a11`: A11 interface facility
    - `a11mgr`: A11 Manager facility
    - `aaa-client`: Authentication, Authorization and Accounting (AAA) client facility
    - `aaamgr`: AAA manager logging facility
    - `aaaproxy`: AAA Proxy facility
    - `aal2`: ATM Adaptation Layer 2 (AAL2) protocol logging facility
    - `acl-log`: Access Control List (ACL) logging facility
    - `acsctrl`: Active Charging Service (ACS) Controller facility
    - `acsmgr`: ACS Manager facility
    - `afctrl`: Fabric Controller facility [ASR 5500 only]
    - `afmgr`: Fabric Manager logging facility [ASR 5500 only]
    - `alarmctrl`: Alarm Controller facility
• **alcap**: Access Link Control Application Part (ALCAP) protocol logging facility
• **alcapmgr**: ALCAP manager logging facility
• **all**: All facilities
• **asngwmgr**: Access Service Network (ASN) Gateway Manager facility
• **asnpemgr**: ASN Paging Controller Manager facility
• **bfd**: Bidirectional Forwarding Detection (BFD) protocol logging facility
• **bgp**: Border Gateway Protocol (BGP) facility
• **bindmux**: IPCF BindMux-Demux Manager logging facility
• **bngmgr**: Broadband Network Gateway (BNG) Demux Manager logging facility
• **bssap+**: Base Station Sub-system Application Part+ protocol facility for the login interface between the SGSN and the MSC/VLR (2.5G and 3G)
• **bssgp**: Base Station Sub-system GPRS Protocol logging facility handles exchange information between the SGSN and the BSS (2.5G only)
• **callhome**: Call Home application logging facility
• **cap**: CAMEL Application Part (CAP) logging facility for protocol used in prepaid applications (2.5G and 3G)
• **cbsmgr**: Cell Broadcasting Service (CBS) logging facility [HNBGW]
• **cdf**: Charging Data Function (CDF) logging facility
• **cgw**: Converged Access Gateway (CGW) logging facility
• **cli**: Command Line Interface (CLI) logging facility
• **cmp**: Certificate Management Protocol (IPSec) logging facility
• **connectedapps**: SecGW ASR 9000 oneP communication protocol
• **connproxy**: Controller Proxy logging facility
• **credit-control**: Credit Control (CC) facility
• **csp**: Card/Slot/Port controller facility
• **css**: Content Service Selection (CSS) facility
• **css-sig**: CSS RADIUS Signaling facility
• **cx-diameter**: Cx Diameter Messages facility [CSCF <---> HSS]
• **data-mgr**: Data Manager Framework logging facility
• **dcardctrl**: IPSec Daughter Card Controller logging facility
• **dcardmgr**: IPSec Daughter Card Manager logging facility
• **demuxmgr**: Demux Manager API facility
• **dgmbmgr**: Diameter Gmb Application Manager logging facility
• **dhcp**: Dynamic Host Configuration Protocol (DHCP) logging facility
• dhcpv6: DHCPv6
• dhost: Distributed Host logging facility
• diabase: Diabase messages facility
• diactrl: Diameter Controller proclet logging facility
• diameter: Diameter endpoint logging facility
• diameter-acct: Diameter Accounting
• diameter-auth: Diameter Authentication
• diameter-dns: Diameter DNS subsystem
• diameter-ecs: ACS Diameter signaling facility
• diameter-engine: Diameter version2 engine logging facility
• diameter-hdd: Diameter Horizontal Directional Drilling (HDD) Interface facility
• diameter-svc: Diameter Service
• diamproxy: DiamProxy logging facility
• dpath: IPSec Data Path facility
• drvctrl: Driver Controller facility
• dpath: IPSec Data Path logging facility
• drvctrl: Driver Controller logging facility
• doulosuemgr: Doulos (IMS-IPSec-Tool) user equipment manager
• eap-diameter: Extensible Authentication Protocol (EAP) IP Sec urity facility
• eap-ipsec: Extensible Authentication Protocol (EAP) IPSec facility
• eap-sta-s6a-s13-s6b-diameter: EAP/STA/S6A/S13/S6B Diameter messages facility
• ecs-css: ACSMGR <-> Session Manager Signalling Interface facility
• egtpc: eGTP-C logging facility
• egtpmgr: enhanced GPRS Tunneling Protocol (eGTP) manager logging facility
• egtpu: eGTP-U logging facility
• embms: evolved Multimedia Broadcast Multicast Service Gateway facility
• embms: eMBMS Gateway Demux facility
• epdg: evolved Packet Data (ePDG) gateway logging facility
• event-notif: Event Notification Interface logging facility
• evlog: Event log facility
• famgr: Foreign Agent manager logging facility
• firewall: Firewall logging facility
• fng: Femto Network Gateway (FNG) logging facility
• **gbmgr**: SGSN Gb Interface Manager facility
• **gmm**:  
  - For 2.5G: Logs the GPRS Mobility Management (GMM) layer (above LLC layer)  
  - For 3G: Logs the access application layer (above the RANAP layer)
• **gprs-app**: GPRS Application logging facility
• **gprs-ns**: GPRS Network Service Protocol (layer between SGSN and the BSS) logging facility
• **gq-rx-tx-diameter**: Gq/Rx/Tx Diameter messages facility
• **gss-gcdr**: GTPP Storage Server GCDR facility
• **gtp**: GTP-C protocol logging facility
• **gtpc**: GTP-C protocol manager logging facility
• **gtpp**: GTP-prime protocol logging facility
• **gtpu**: GTP-U protocol logging facility
• **gtpumgr**: GTP-U Demux manager
• **gx-ty-diameter**: Gx/Ty Diameter messages facility
• **gy-diameter**: Gy Diameter messages facility
• **h248prt**: H.248 port manager facility
• **hamgr**: Home Agent manager logging facility
• **hat**: High Availability Task (HAT) process facility
• **hdctr**: HD Controller logging facility
• **henbapp**: Home Evolved NodeB (HENB) App facility
• **henbgw**: HENB-GW facility
• **henbgw-pws**: HENB-GW Public Warning System logging facility
• **henbgw-sctp-acs**: HENB-GW access Stream Control Transmission Protocol (SCTP) facility
• **henbgw-sctp-nw**: HENBGW network SCTP facility
• **henbgwdemux**: HENB-GW Demux facility
• **henbgwmgm**: HENB-GW Manager facility
• **hnb-gw**: HNB-GW (3G Femto GW) logging facility
• **hnbmgm**: HNB-GW Demux Manager logging facility
• **hss-peer-service**: Home Subscriber Server (HSS) Peer Service facility
• **igmp**: Internet Group Management Protocol (IGMP)
• **ikev2**: Internet Key Exchange version 2 (IKEv2)
• **ims-authorizatn**: IP Multimedia Subsystem (IMS) Authorization Service facility
• **ims-sh**: HSS Diameter Sh Interface Service facility
- **imsimgr**: SGSN IMSI Manager facility
- **imsue**: IMS User Equipment (IMSUE) facility
- **ip-arp**: IP Address Resolution Protocol facility
- **ip-interface**: IP interface facility
- **ip-route**: IP route facility
- **ipms**: Intelligent Packet Monitoring System (IPMS) logging facility
- **ipne**: IP Network Enabler (IPNE) facility
- **ipsec**: IP Security logging facility
- **ipsecdemux**: IPSec demux logging facility
- **ips**: IP Service Gateway interface logging facility
- **ipsgmgr**: IP Services Gateway facility
- **ipsp**: IP Pool Sharing Protocol logging facility
- **kvstore**: Key/Value Store (KVSTORE) Store facility
- **l2tp-control**: Layer 2 Tunneling Protocol (L2TP) control logging facility
- **l2tp-data**: L2TP data logging facility
- **l2tpdemux**: L2TP Demux Manager logging facility
- **l2tpmgr**: L2TP Manager logging facility
- **lagmgr**: Link Aggregation Group (LAG) manager logging facility
- **lc**: Location Services (LCS) logging facility
- **ldap**: Lightweight Directory Access Protocol (LDAP) messages logging facility
- **li**: Refer to the *Lawful Intercept Configuration Guide* for a description of this command.
- **linkmgr**: SGSN/BSS SS7 Link Manager logging facility (2.5G only)
- **llc**: Logical Link Control (LLC) Protocol logging facility; for SGSN: logs the LLC layer between the GMM and the BSSGP layers for logical links between the MS and the SGSN
- **local-policy**: Local Policy Service facility
- **location-service**: Location Services facility
- **m3ap**: M3 Application Protocol facility
- **m3ua**: M3UA Protocol logging facility
- **magmgr**: Mobile Access Gateway manager logging facility
- **map**: Mobile Application Part (MAP) protocol logging facility
- **megadiammgr**: MegaDiameter Manager (SLF Service) logging facility
- **mme-app**: Mobility Management Entity (MME) Application logging facility
- **mme-embms**: MME evolved Multimedia Broadcast Multicast Service facility
- **mme-misc**: MME miscellaneous logging facility
- **mmedemux**: MME Demux Manager logging facility
- **mmemgr**: MME Manager facility
- **mmgr**: Master Manager logging facility
- **mobile-ip**: Mobile IP processes
- **mobile-ip-data**: Mobile IP data facility
- **mobile-ipv6**: Mobile IPv6 logging facility
- **mpls**: Multiprotocol Label Switching (MPLS) protocol logging facility
- **mrme**: Multi Radio Mobility Entity (MRME) logging facility
- **mseg-app**: Mobile Services Edge Gateway (MSEG) application logging facility (This option is not supported in this release.)
- **mseg-gtpc**: MSEG GTP-C application logging facility (This option is not supported in this release.)
- **mseg-gtpu**: MSEG GTP-U application logging facility (This option is not supported in this release.)
- **msegmgr**: MSEG Demux Manager logging facility (This option is not supported in this release.)
- **mtp2**: Message Transfer Part 2 (MTP2) Service logging facility
- **mtp3**: Message Transfer Part 3 (MTP3) Protocol logging facility
- **multicast-proxy**: Multicast Proxy logging facility
- **nas**: Non-Access Stratum (NAS) protocol logging facility [MME 4G]
- **netwstrg**: Network Storage facility
- **npuctrl**: Network Processor Unit Control facility
- **npudrv**: Network Processor Unit Driver facility [ASR 5500 only]
- **npumgr**: Network Processor Unit Manager facility
- **npumgr-accl**: NPUMGR ACL logging facility
- **npumgr-drvc**: NPUMGR DRV logging facility
- **npumgr-flow**: NPUMGR FLOW logging facility
- **npumgr-fwd**: NPUMGR FWD logging facility
- **npumgr-init**: NPUMGR INIT logging facility
- **npumgr-lc**: NPUMGR LC logging facility
- **npumgr-port**: NPUMGR PORT logging facility
- **npumgr-recovery**: NPUMGR RECOVERY logging facility
- **npumgr-rril**: NPUMGR RRI (Reverse Route Injection) logging facility
- **npumgr-vpn**: NPUMGR VPN logging facility
- **npusim**: NPUSIM logging facility [ASR 5500 only]
- **ntfy-intf**: Notification Interface logging facility [Release 12.0 and earlier versions only]
- **ocsp**: Online Certificate Status Protocol logging facility.
• orbs: Object Request Broker System logging facility
• ospf: OSPF protocol logging facility
• ospfv3: OSPFv3 protocol logging facility
• p2p: Peer-to-Peer Detection logging facility
• pagingmgr: PAGINGMGR logging facility
• pccmgr: Intelligent Policy Control Function (IPCF) Policy Charging and Control (PCC) Manager library
• pdg: Packet Data Gateway (PDG) logging facility
• pdgdmgr: PDG Demux Manager logging facility
• pdif: Packet Data Interworking Function (PDIF) logging facility
• pgw: Packet Data Network Gateway (PGW) logging facility
• pmm-app: Packet Mobility Management (PMM) application logging facility
• ppp: Point-To-Point Protocol (PPP) link and packet facilities
• pppoe: PPP over Ethernet logging facility
• proclet-map-frwk: Proclet mapping framework logging facility
• push: VPNMGR CDR push logging facility
• radius-acct: RADIUS accounting logging facility
• radius-auth: RADIUS authentication logging facility
• radius-koa: RADIUS change of authorization and radius disconnect
• ranap: Radio Access Network Application Part (RANAP) Protocol facility logging info flow between SGSN and RNS (3G)
• rct: Recovery Control Task logging facility
• rdt: Redirect Task logging facility
• resmgr: Resource Manager logging facility
• rf-diameter: Diameter Rf interface messages facility
• rip: Routing Information Protocol (RIP) logging facility [RIP is not supported at this time.]
• rlf: Rate Limiting Function (RLF) logging facility
• rohc: Robust Header Compression (RoHC) facility
• rsvp: Reservation Protocol logging facility
• rua: RANAP User Adaptation (RUA) [3G Femto GW - RUA messages] logging facility
• s102: S102 protocol logging facility
• s102mgr: S102Mgr logging facility
• s1ap: S1 Application Protocol (S1AP) Protocol logging facility
• sabp: Service Area Broadcast Protocol (SABP) logging facility
• saegw: System Architecture Evolution (SAE) Gateway facility
- **sbc**: SBc protocol logging facility
- **secp**: Signalling Connection Control Part (SCCP) Protocol logging (connection-oriented messages between RANAP and TCAP layers).
- **sct**: Shared Configuration Task logging facility
- **sctp**: Stream Control Transmission Protocol (SCTP) Protocol logging facility
- **sef_ecs**: Severely Errored Frames (SEF) APIs printing facility
- **sess-gr**: SM GR facility
- **sessctrl**: Session Controller logging facility
- **sessmgr**: Session Manager logging facility
- **sesstrc**: session trace logging facility
- **sft**: Switch Fabric Task logging facility
- **sgs**: SGs interface protocol logging facility
- **sgsn-app**: SGSN-APP logging various SGSN "glue" interfaces (for example, between PMM, MAP, GPRS-FSM, SMS).
- **sgsn-failures**: SGSN call failures (attach/activate rejects) logging facility (2.5G)
- **sgsn-gtpc**: SGSN GTP-C Protocol logging control messages between the SGSN and the GGSN
- **sgsn-gtpu**: SGSN GTP-U Protocol logging user data messages between the SGSN and GGSN
- **sgsn-mbms-bearer**: SGSN Multimedia Broadcast/Multicast Service (MBMS) Bearer app (SMGR) logging facility
- **sgsn-misc**: Used by stack manager to log binding and removing between layers
- **sgsn-system**: SGSN System Components logging facility (used infrequently)
- **sgsn-test**: SGSN Tests logging facility; used infrequently
- **sgtpcmgr**: SGSN GTP-C Manager logging information exchange through SGTPC and the GGSN
- **sgw**: Serving Gateway facility
- **sh-diameter**: Sh Diameter messages facility
- **sitmain**: System Initialization Task main logging facility
- **sls**: Service Level Specification (SLS) protocol logging facility
- **sm-app**: SM Protocol logging facility
- **sms**: Short Message Service (SMS) logging messages between the MS and the SMSC
- **sndcp**: Sub Network Dependent Convergence Protocol (SNDCP) logging facility
- **snmp**: SNMP logging facility
- **sprmgr**: IPCF Subscriber Policy Register (SPR) manager logging facility
- **srdb**: Static Rating Database
- **srp**: Service Redundancy Protocol (SRP) logging facility
• **sscnii**: Service-Specific Coordination Function for Signaling at the Network Node Interface (SSCF-NNI) logging facility
• **sscop**: Service-Specific Connection-Oriented Protocol (SSCOP) logging facility
• **ssh-ipsec**: Secure Shell (SSH) IP Security logging facility
• **ssl**: Secure Socket Layer (SSL) message logging facility
• **stat**: Statistics logging facility
• **supserv**: Supplementary Services logging facility [H.323]
• **system**: System logging facility
• **tacacsplus**: TACACS+ Protocol logging facility
• **tcap**: TCAP Protocol logging facility
• **testctrl**: Test Controller logging facility
• **testmgr**: Test Manager logging facility
• **threshold**: threshold logging facility
• **ttg**: Tunnel Termination Gateway (TTG) logging facility
• **tuccl**: TCP/UDP Convergence Layer (TUCL) logging facility
• **udr**: User Data Record (UDR) facility (used with the Charging Service)
• **user-data**: User data logging facility
• **user-l3tunnel**: User Layer 3 tunnel logging facility
• **usertcp-stack**: User TCP Stack
• **vim**: Voice Instant Messaging (VIM) logging facility
• **vinfo**: VINFO logging facility
• **vmgctrl**: Virtual Media Gateway (VMG) controller facility
• **vmgctrl**: VMG Content Manager facility
• **vpn**: Virtual Private Network logging facility
• **wimax-data**: WiMAX DATA
• **wimax-r6**: WiMAX R6
• **wsg**: Wireless Security Gateway (ASR 9000 Security Gateway)
• **x2gw-app**: X2GW (X2 proxy Gateway, eNodeB) application logging facility
• **x2gw-demux**: X2GW demux task logging facility

**level report_level | critical-info | no-critical-info |**

**level report_level**: specifies the level of information to be logged, *report_level*, as one of:

• **critical**
• **debug**
- error
- info
- trace
- unusual
- warning

critical-info | no-critical-info: indicates if critical information is to be displayed or not. The keyword critical-info specifies that events with a category attribute of critical information are to be displayed. Examples of these types of events can be seen at bootup when system processes and tasks are being initiated. The no-critical-info keyword specifies that events with a category attribute of critical information are not to be displayed.

Usage Guidelines
This command is useful when it is necessary to get real time output of events. Event output may be cached otherwise which may make it difficult to troubleshoot problems which do not allow the last cache of events to be output prior to system problems.

Caution
Issuing this command could negatively impact system performance depending on system loading, the log level, and/or the type of facility(ies) being logged.

Examples
Set real time output for the point-to-point protocol facility and all facilities, respectively, to avoid logging of excessive information.

logging filter runtime facility ppp
logging filter runtime facility all level warning
logging include-ueid

Enables the sending of the International Mobile Station Identifier (IMSI) and International Mobile Equipment Identifier (IMEI) in logging details of event log types error and critical.

**Product**
P-GW
SAEGW

**Privilege**
Administrator, Security Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no ] logging include-ueid
```

*no*
Disables the sending of the IMSI/IMEI in logging details of event log types error and critical.

*include-ueid*
Enables the sending of the IMSI/IMEI in logging details of event log types error and critical. When enables, the following event logs of type error and critical will contain the IMSI/IMEI in the logging details.

**Table 4: System Event Logs of Type Error and Critical with IMSI/IMEI in System Event Log Details**

<table>
<thead>
<tr>
<th>Event Log #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12225</td>
<td>Represents misc_error3 in format &quot;[IMSI &lt;IMSI&gt;] Misc Error3: %s, error code %d&quot;</td>
</tr>
<tr>
<td>12226</td>
<td>Represents recover_call_from_crr_failed1 error in format &quot;[IMSI &lt;IMSI&gt;]Sessmgr-%d Recover call from CRR failed for callid:0x%x reason=%s&quot;</td>
</tr>
<tr>
<td>12227</td>
<td>Represents aaa_create_session_failed_no_more_sessions1 error in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Ran out of session handles&quot;</td>
</tr>
<tr>
<td>140075</td>
<td>Represents error_log1 in format &quot;[IMSI &lt;IMSI&gt;]%s&quot;</td>
</tr>
<tr>
<td>Event Log #</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>139001</td>
<td>To print miscellaneous PGW error log.</td>
</tr>
<tr>
<td>191006</td>
<td>To print miscellaneous SAEGW error log.</td>
</tr>
<tr>
<td>10034</td>
<td>Represents FSM error in format &quot;[IMSI &lt;IMSI&gt;] default call fsm error: ostate=%s(%d) state=%s(%d) event=%s(%d)&quot;</td>
</tr>
<tr>
<td>10035</td>
<td>Represents FSM INVALID event in format &quot;[IMSI &lt;IMSI&gt;] default call fsm invalid event: state=%s(%d) event=%s(%d)&quot;</td>
</tr>
</tbody>
</table>
| 12382      | Represents SN_LE_SESSMGR_PGW_REJECT_BEARER_OP in format "[IMSI <IMSI>] Sessmgr-%d: Request to %s bearer rejected. Reason: %s". For example 
"[IMSI] 112233445566778 Sessmgr-1: Request to Create bearer rejected. Reason: Create Bearer Request denied as session recovery is in progress" |
<p>| 12668      | Represents fsm_event_error in format &quot;[IMSI &lt;IMSI&gt;] Misc Error: Bad event in sessmgr fsm, event code %d&quot; |
| 12774      | Represents pgw_purge_invalid_crr in format &quot;[IMSI &lt;IMSI&gt;] Local %s TEID [%lu] Collision: Clp Connect Time: %lu, Old Clp Callid: %d, Old Clp Connect Time: %lu %s&quot; |
| 12855      | Represents ncqos_nrspca_trig_err in format &quot;[IMSI &lt;IMSI&gt;] NCQOS NRSPCA trig rcvd in invalid bcm mode.&quot; |
| 12857      | Represents ncqos_nrupc_tft_err in format &quot;[IMSI &lt;IMSI&gt;] NCQOS NRUPC Trig : TFT validation failed for nsapi &lt;%u&gt;.&quot; |
| 12858      | Represents ncqos_nrxx_trig_already in format &quot;[IMSI &lt;IMSI&gt;] NCQOS NRSPCA/NRUPC is already triggered on sess with nsapi &lt;%u&gt;.&quot; |
| 12859      | Represents ncqos_nrxx_tft_check_fail in format &quot;[IMSI &lt;IMSI&gt;] NCQOS TFT check failed as TFT has invalid opcode for nsapi &lt;%u&gt;: pf_id_bitmap 0x%x and tft_opcode: %d&quot; |
| 12860      | Represents ncqos_sec_rej in format &quot;[IMSI &lt;IMSI&gt;] NCQOS Secondary ctxt with nsapi &lt;%u&gt; rejected, due to &lt;%s&gt;.&quot; |
| 12861      | Represents ncqos_upc_rej in format &quot;[IMSI &lt;IMSI&gt;] UPC Rejected for ctxt with nsapi &lt;%u&gt;, due to &lt;%s&gt;.&quot; |
| 12862      | Represents ggsn_subsession_invalid_state in format &quot;[IMSI &lt;IMSI&gt;] GGSN subsession invalid state state:&lt;%s&gt;,[event:&lt;%s&gt;]&quot; |
| 11830      | Represents gngp_handoff_rejected_for_pdn_ipv4v6 in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Handoff from PGW-to-GGSN rejected, as GGSN doesn't support Deferred allocation for IPv4v6, dropping the call.&quot; |</p>
<table>
<thead>
<tr>
<th>Event Log #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>11832</td>
<td>Represents <code>gnpgp_handoffRejected_no_non_gbr_bearer_for_def_bearer_selection</code> in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Handoff from PGW-to-GGSN rejected, as GGSN Callline has no non-GBR bearer to be selected as Default bearer.&quot;</td>
</tr>
<tr>
<td>11834</td>
<td>Represents <code>gnpgp_handoff_from_ggsn_rejected_no_ggsn_call</code> in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d Handoff from GGSN-to-PGW rejected, as GGSN call with TEID C &lt;0x%x&gt; not found.&quot;</td>
</tr>
<tr>
<td>12960</td>
<td>Represents <code>gtp_pdp_type_mismatch</code> in format &quot;[IMSI &lt;IMSI&gt;] Mismatch between PDP type of APN %s and in create req. Rejecting call&quot;</td>
</tr>
<tr>
<td>11282</td>
<td>Represents <code>pcc_intf_error_info</code> in format &quot;[IMSI &lt;IMSI&gt;] %s&quot;</td>
</tr>
<tr>
<td>11293</td>
<td>Represents <code>collision_error</code> in format &quot;[IMSI &lt;IMSI&gt;] Collision Error: Temp Failure Handling Delayed Pending Active Transaction: , error code %d&quot;</td>
</tr>
<tr>
<td>11917</td>
<td>Represents <code>rcvd_invalid_bearer_binding_req_from_acs</code> in format &quot;[IMSI &lt;IMSI&gt;] Sessmgr-%d: Received invalid bearer binding request from ACS.&quot;</td>
</tr>
<tr>
<td>11978</td>
<td>Represents <code>saegw_uid_error</code> in format &quot;[IMSI &lt;IMSI&gt;] %s&quot;</td>
</tr>
<tr>
<td>11994</td>
<td>Represents <code>unwanted_pcc_intf_setup_req</code> error in format &quot;[IMSI &lt;IMSI&gt;] GGSN_INITIATE_SESS_SETUP_REQ is already fwd to PCC interface &quot;</td>
</tr>
<tr>
<td>140005</td>
<td>Represents <code>ue_fsm_illegal_event</code> in format &quot;[IMSI &lt;IMSI&gt;] Invalid/unhandled UE event &lt;%s&gt; in state &lt;%s&gt;&quot;</td>
</tr>
<tr>
<td>140006</td>
<td>Represents <code>pdsn_fsm_illegal_event</code> in format &quot;[IMSI &lt;IMSI&gt;] Invalid/unhandled PDN event &lt;%s&gt; in state &lt;%s&gt;&quot;</td>
</tr>
<tr>
<td>140007</td>
<td>Represents <code>e EPSB_fsm_illegal_event</code> in format &quot;[IMSI &lt;IMSI&gt;] Invalid/unhandled EPSB event &lt;%s&gt; in state &lt;%s&gt;&quot;</td>
</tr>
<tr>
<td>10726</td>
<td>Represents <code>saegwdrv_generic_error</code> &quot;[IMSI &lt;IMSI&gt;] %s&quot;</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to enable the logging of the UE's IMSI/IMEI in event log types of error and critical. This is useful in identifying the specific UE affected by events that can potentially affect service.

**Examples**

The following command enables the sending of the IMSI/IMEI in the logging details of event logs of type error and critical.

`logging include-ueid`
logging monitor

Enables or disables the monitoring of a specified user.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
| no | logging monitor { ipaddr ip_address | ipv6addr ipv6_address | msid ms_id | username user_name }
```

```
no
```

Disables the monitoring of the user specified by the options given.

```
ipaddr ip_address
```

Specifies the IP address of the user for which the monitoring filter is to be set. `ip_address` must entered using IPv4 dotted-decimal notation.

```
ipv6addr ipv6_address
```

Specifies the IPv6 address of the user for which the monitoring filter is to be set. `ipv6_address` must be followed by IPv6 address in a `xx:yy:zz` format.

```
msid ms_id
```

**msid ms_id**: specifies the mobile subscriber ID for which the monitoring filter is to be set. `ms_id` must be from 7 to 16 digits.

This keyword/option can be used to specify the Mobile Subscriber ISDN (MSISDN) for GGSN calls which enables logging based on MSISDN.

```
username user_name
```

**username user_name**: specifies a user for which the monitoring filter is to be set. `user_name` must refer to a previously configured user.
Usage Guidelines

Monitor subscribers which have complaints of service availability or to monitor a test user for system verification.

Caution

Issuing this command could negatively impact system performance depending on the number of subscribers for which monitoring is performed and/or the amount of data they're passing.

Examples

The following command enables the monitoring of user user1 and mobile subscriber ID 4441235555, respectively.

```
logging monitor username user1
logging monitor msid 44441235555
```

The following disables the monitoring of user user1.

```
no logging monitor username user1
```
logging runtime

Enables events to be filtered and logged in real time.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local]\(host\_name\)(config)#

Syntax Description
logging runtime buffer store \{ all-events | filtered-events-only \}

**all-events**
Logging daemon runtime buffer stores all logs that come to it.

**filtered-events-only**
Logging daemon runtime buffer stores only logs that pass the runtime filter.

Usage Guidelines
Sets the filtering of logged information to log in real time.

Examples
The following command enables storage of logs that pass the runtime filter:
logging runtime buffer store filtered-events-only
**Ite-policy**

This command enters the LTE Policy Configuration Mode where LTE policy parameters can be configured.

**Product**
- MME
- SAEGW
- S-GW
- SGSN

**Privilege**
Administrator

**Command Modes**
- Exec > Global Configuration
- configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
- **Ite-policy**

**Usage Guidelines**

Enters the LTE Policy Configuration Mode.

Entering this command results in the following prompt:

```
[context_name]hostname(Ite-policy)#
```

LTE Policy Configuration Mode commands are defined in the *LTE Policy Configuration Mode Commands* chapter.
mediation-device

This command is obsolete. Even though the CLI accepts the command no function is performed.
network-overload-protection
mme-new-connections-per-second

This command configures an attach rate throttle mechanism to control the number of new connections allowed on a per second basis.

**Product**  
MME

**Privilege**  
Administrator

**Command Modes**  
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```

default
Disables the MME attach rate throttle feature.

mme-new-connections-per-second #_new_connections
Define the number of new connections to be accepted per second.

#_new_connections: Must be an integer from 50 to 5000.

action
Specifies the action to be taken by the MME when the new connection queue is full. Specific actions can be defined for each of the following connection types:

- UE-initiated attaches (see attach keyword).
- UE-initiated inter-CN node TAU requests (see tau keyword).
- Peer SGSN/MME intiated forward relocation requests (see fwd-reloc keyword).
attach { drop | reject-with-emm-cause { congestion | network-failure | no-suitable-cell-in-tracking-area } }

Specifies the action to be taken for all types of UE-initiated initial attaches (IMSI, local GUTI, foreign GUTI, mapped GUTI, etc.). Select one of the following actions:

- **drop**: Drop the new connection request.
- **reject-with-cause**: Reject the new connection request. Include one of the following as the cause in the reject message:
  - congestion
  - network-failure
  - no-suitable-cell-in-tracking-area

\[
\text{tau} \{ \text{drop} | \text{reject-with-emm-cause} \{ \text{congestion} | \text{network-failure} | \text{no-sec-ctxt-in-nw} | \text{no-suitable-cell-in-tracking-area} \} \}
\]

Specifies the action to be taken for UE-initiated inter-CNTAU requests requiring context transfer from old MME/SGSN, including TAU requests with foreign GUTI or mapped GUTI. Select one of the following actions:

- **drop**: Drop the new connection request.
- **reject-with-cause**: Reject the new connection request. Include one of the following as the cause in the reject message:
  - congestion
  - network-failure
  - no-sec-ctxt-in-nw
  - no-suitable-cell-in-tracking-area

\[
\text{fwd-reloc} \{ \text{drop} | \text{reject} \}
\]

Specifies the action to be taken for peer SGSN/MME initiated forward relocation requests via Gn/S10/S3. Select one of the following actions:

- **drop**: Drop the new connection request.
- **reject**: Reject the new connection request. If the inbound forward-relocation requests are rejected, the following cause codes shall be used:
  - GTPv1 - No resources available (199)
  - GTPv2 - No resources available (73)

\[
\text{ddn} \{ \text{drop} | \text{reject-with-cause} \{ \text{unable-to-page-ue} | \text{context-not-found} \} \}
\]

In the event of an MME failure, the surviving MME in the pool may receive a very large number of IMSI requests, which may overwhelm the IMSI Manager. To avoid congestion, the MME can be configured using
this keyword to throttle the IMSI-based DDN requests it receives if the configured \#_new_connections rate is exceeded. Select one of the following actions:

- **drop**: Drop new IMSI-based DDN requests.
- **reject**: Reject the IMSI-based DDN request. Include one of the following as the cause in the reject message:
  - `unable-to-page-ue`
  - `context-not-found`

---

**Important**

Beginning with Release 19.4, the **dnn** keyword behavior changes from mandatory to optional. If the **dnn** option is not configured, then the default action is to drop the Downlink Data Notification.

---

**queue-size queue_size**

Defines the maximum size of the pacing queue used for buffering the packets. If configured, the queue-size should be greater than or equal to the \#_new_connections value and less than or equal to the optimal value (the wait_time * \#_new_connections). This validation is done in the CLI.

`queue_size` Must be an integer from 250 to 25000.

Default: unconfigured. The default value is the \#_new_connections * wait-time. This will be the optimal value.

**wait-time wait_time**

Defines the maximum life-time (number of seconds) of the packets in the queue beyond which the packets are considered to be "stale" and are dropped.

`wait_time` Must be an integer from 1 to 15

Default: 5

---

**Usage Guidelines**

Use this command to configure attach rate throttling on the MME.

When enabled, new connections (except emergency requests) are buffered and paced through the queue. Messages in the queue are processed (FIFO) until they age-out when the queued message's lifetime crosses the configured wait-time. The wait-time and the attach rate decide the optimal size of the queue. If the queue is full, packets are rejected or dropped based on the configured action.

This feature functions at a system (chassis) level for all MME services. All MME services on the system are controlled by a single pacing queue. For a combo MME-SGSN node, each type of service shall be controlled by its own queue and its own configuration.

Emergency attaches are not be throttled when this feature is enabled.

---

**Important**

This command is available only if a valid license (MME Resiliency) is installed. Contact your Cisco account representative for more information.
Examples

Configure the new connections per second rate at 2500, reject all (non-emergency) attaches and TAU requests, and drop forward relocation requests if the new connection rate is exceeded. Rejects will return emm cause code "Congestion".

```
network-overload-protection mme-new-connections-per-second 2500 action attach reject-with-emm-cause congestion tau reject-with-emm-cause congestion fwd-reloc drop ddn drop wait-time 5
```

Set the attach rate to 500 per second, the same actions as the previous example, but set the wait time to 5 seconds, and the queue size to be calculated (as follows: wait_time * #_new_connections - i.e., 2500)

```
network-overload-protection mme-new-connections-per-second 500 action attach reject-with-emm-cause congestion tau reject-with-emm-cause congestion fwd-reloc drop ddn drop wait-time 5
```

Command Line Interface Reference, Modes G - H, StarOS Release 19
network-overload-protection mme-tx-msg-rate-control

Enables and configures the S1 Paging Rate Limit feature as well as UE Deactivation Rates upon EGTPC path failure feature.

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

Command Modes
Exec > Global Configuration
   configure

Entering the above command sequence results in the following prompt:
   [local]host_name(config)#

Syntax Description
network-overload-protection mme-tx-msg-rate-control { egtp-pathfail ecm-idle rate ecm-connected rate } | enb s1-paging rate } | default | network-overload-protection mme-tx-msg-rate-control

default
Applies the default MME message rate control configuration; S1 paging rate limit is disabled and a path failure processing rate of 1000 per second per session manager without distinguishing between ECM idle/connected sessions.

egtp-pathfail ecm-idle rate ecm-connected rate
Configures the UE deactivation pacing rate for MME S11/S10/S3 interfaces (any EGTPC service with interface type "interface-mme").
ecm-idle rate: This keyword defines the deactivation rate for UEs in ECM Idle mode.
ecm-connected rate: This keyword defines the deactivation rate for UEs in ECM Connected mode.
rerate specifies a rate threshold in sessions per second per session manager (SessMgr) as an integer from 1 through 5000.
Note: Configuring a high deactivation rate can have a negative effect on performance. Appropriate dimensioning exercises should be performed to arrive at the optimum rate.
enb s1-paging rate

Configures an S1 paging rate limit applicable to all eNodeBs connected all MME services. S1 Paging requests to an eNodeB will be rate limited at this threshold value. S1 Paging requests to an eNodeB exceeding this threshold will be dropped.

*rate* specifies the rate threshold in messages per second per eNodeB as an integer from 1 through 65535.

**Usage Guidelines**

Use this command to enable and configure the S1 Paging Rate Limit feature as well as UE Deactivation Rates upon EGTPC path failure feature.

**Examples**

The following command configures S1 Paging rate limit of 150 messages per second per eNodeB.

```
network-overload-protection mme-tx-msg-rate-control enb s1-paging 150
```

The following command configures EGTP path failure processing rate limit for UE sessions in ECM-Idle mode to 10 sessions per second per session manager and for UE sessions in ECM-Connected mode to 20 sessions per second per session manager.

```
network-overload-protection mme-tx-msg-rate-control egtp-pathfail ecm-idle 10 ecm-connected 20
```
network-overload-protection
sgsn-new-connections-per-second

This command configures an attach rate throttle mechanism to control the number of new connections (attaches or inter-SGSN RAUs), through the SGSN, on a per second basis.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
network-overload-protection sgsn-new-connections-per-second 

#_new_connections action { drop | reject with cause { congestion | network failure } } [ queue-size queue_size ] [ wait-time wait_time ]

default network-overload-protection sgsn-new-connections-per-second

default

Using `default` in the command, disables this attach rate throttle feature that provides network overload protection.

sgsn-new-connections-per-second #_new_connections

Define the number of new connections to be accepted per second.

#_new_connections: Must be an integer from 50 to 5000.

**action**

Specifies the action to be taken by the SGSN when the attach rate exceeds the configured limit on the number of attaches. Select one of the following actions:

- **drop**: Drop the new connection request.
- **reject-with-cause**: Reject the new connection request. Include one of the following as the cause in the reject message:
  - **congestion**
network failure

queue-size queue_size
Defines the maximum size of the pacing queue used for buffering the packets. If configured, the queue-size should be greater than or equal to the \#_new_connections value and less than or equal to the optimal value (the wait_time * \#_new_connections). This validation is done in the CLI.

queue_size Must be an integer from 250 to 25000.
Default: unconfigured. The default value is the \#_new_connections * wait-time. This will be the optimal value.

wait-time wait_time
Defines the maximum life-time (number of seconds) of the packets in the queue beyond which the packets are considered to be "stale".
wait_time Must be an integer from 1 to 15
Default: 5

Usage Guidelines
Use this command to configure the rate at which the SGSN must process new connection requests. The rate is the number of new connections to be accepted per second.

With basic network overload protection, the incoming new connection rate is higher than this configured rate. When this occurs, all of the new connection requests cannot be processed. This command can also be used to configure the action to be taken when the rate limit is exceeded. The new connection requests, which cannot be processed, can be either dropped or rejected with a specific reject cause.

The SGSN's optimized network overload protection performs attach-rate throttling to avoid overloading Gr, Gn and Gf interfaces. This is enabled with queue-size and wait-time keywords so that the IMSIMgr throttles the attach rate to values configured with these keywords.

If the SGSN receives more than the configured number of attaches in a second, then the attaches are buffered in the pacing queue and requests are only dropped when the buffer overflows due to high incoming attach rate. Messages in the queue are processed (FIFO) until they age-out when the queued message's lifetime crosses the configured wait-time. The wait-time and the attach rate decide the optimal size of the queue.

Counters for this feature are available in the show gmm-sm statistics command display in the Network Overload Protection portion of the table.

Examples
Configure the throttle rate or limit to 2500 attaches per second and to drop all requests if the limit is exceeded.

network-overload-protection sgsn-new-connections-per-second 2500 action drop
Disables the network-overload protection feature and set the default queue size to 1000 and the wait time to 5 seconds:

default network-overload-protection
sgsn-new-connections-per-second

Set the attach rate to 500 per second, the action to drop, the wait time to 5 seconds, and the queue size to be calculated (as follows: wait_time * \#_new_connections - i.e., 2500)

network-overload-protection
sgsn-new-connections-per-second
500 action drop wait-time 5
network-service-entity

This command creates a new instance of an SGSN network service entity (NSE) for either the IP environment or the Frame Relay environment.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

| no | network-service-entity ( ip-local | peer-nsei peer_nsei_number frame-relay )

no

Deletes the network service entity definition from the system configuration.

ip-local

Configures the local endpoint for NS/IP and enters the NSE-IP configuration mode. The prompt will change to:

[local]<hostname>(nse-ip-local)#

peer-nsei peer_nsei_number frame-relay

Configures a peer NSE with frame relay connectivity. This set of keywords also provides access to the NSE-FR Configuration mode. The prompt will change to:

[local]<hostname>(nse-fr-peer-nsei-<peer_nsei_number>)#

**Usage Guidelines**

Use this command to access the configuration modes for either the IP or Frame Relay network service entities.

**Examples**

Enter the NSE for a Frame Relay configuration instance identified as 4554:

network-service-entity peer-nsei 4554 frame-relay
Overview
(ntp)
Enters the Network Time Protocol (NTP) configuration mode or disables the use of NTP on the system.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

| no | ntp |

- **no**

Disables the use of NTP for clock synchronization. When omitted, NTP client support is enabled on the chassis. By default NTP synchronization to external servers is disabled.

**Important**
If the use of NTP is disabled the system clock may drift over a period of time. This may require manual updates to the system clock to synchronize the clock with other network elements.

**Usage Guidelines**
Used when it is necessary to enable or configure NTP settings. For additional information refer to the NTP Configuration Mode Commands chapter and the System Administration Guide.

**Examples**
The following command enters the NTP configuration mode:

```
ntp
```

The following disables the use of the network timing protocol for system clock synchronization:

```
no ntp
```
**ntsr pool-id**

Configures a pool ID and pool type (either MME or S4-SGSN) for Network Triggered Service Restoration (NTSR). Once executed, the user is placed in NTSR Pool Configuration Mode.

**Product**

S-GW

**Privilege**

Administrator, Security Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
ntsr pool-id  number  pool-type [mme | s4-sgsn ]
no ntsr pool-id
```

```
ntsr pool-id  number
```

Specifies an ID number for this NTSR pool. Valid entries are from 1 to 65535.

```
pool-type
```

Specifies the type of pool for the pool-id. Options are MME or S4-SGSN.

**Usage Guidelines**

This command is used to configure a pool ID and pool type (either MME or S4-SGSN) for NTSR. Once executed, the operator must configure a peer IP address in NTSR Pool Configuration mode using the **peer-ip-address** command.

**Examples**

This example configures an NTSR pool ID of 1 and a pool type of mme.

```
ntsr pool-id  1  pool-type mme
```
operator-policy

This command creates an operator policy and enters the operator policy configuration mode. Commands for configuration of the policies are available in the Operator Policy Configuration Mode Commands chapter.

**Product**

- MME
- SGSN
- SAEGW
- S-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

- operator-policy ( default | name policy_name ) [ -noconfirm ]
- no operator-policy ( default | name policy_name )

- **-noconfirm**
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

- **no**
  Removes the specified operator policy from the system configuration.

- **default**
  
  **Important**
  You should configure this default operator policy to be it available to handle IMSIs that are not matched with other defined policies.

  "default", in this case, is the name of a specific operator policy. This default policy is used when no other defined operator policy matches the incoming IMSI.
name policy_name

Specifies the unique name of an operator policy. policy_name is entered as an alphanumeric string of 1 through 64 characters.

Usage Guidelines

Use this command to create an operator policy and to enter the operator policy configuration mode to define or modify policies.

An operator policy associates APNs, APN profiles, IMEI ranges, IMEI profiles, an APN remap table and a call-control profile to ranges of IMSIs. These profiles and tables are created and defined within their own configuration modes to generate sets of rules and instructions that can be reused and assigned to multiple policies. In this manner, an operator policy manages the application of rules governing the services, facilities and privileges available to subscribers. These policies can override standard behaviors and provide mechanisms for an operator to get around the limitations of other infrastructure elements such as DNS servers and HLRs.

The system supports up to 1,000 operator policies, including the default operator policy.

Important

An operator policy is the key element of the Operator Policy feature. After defining an instance of an operator policy, you must go to the SGSN Global Configuration Mode (from the Global Configuration mode) to define the IMSI range(s). This requirement does not hold if you are using a default operator policy.

To see what operator policies have already been created, return to the Exec mode and enter the show operator-policy all command.

Examples

The following command accesses the default operator policy and enters the operator policy configuration mode to view or modify the specified policy:

operator-policy default
orbem

Enters the Object Request Broker Element Manager (ORBEM) Configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
orbem

**Usage Guidelines**
Set the configuration mode to allow modification of the ORBEM configuration data.

**Examples**
The following command enters the Object Request Broker Element Manager (ORBEM) Configuration mode:

```
orbem
```
pac-standby-priority

This command has been renamed to card-standby-priority. Please refer to that command for details. Note that for backwards compatibility, the system accepts this command as valid.
pdu-session-recovery

Enables or disables support for early PDU recovery of VoLTE calls during Transaction Protocol Data Unit (TPDU) based session recovery. When this CLI is enabled, data is allowed for VoLTE-only calls when Session Manager is recovering.

Product

- GGSN
- P-GW
- S-GW
- SAE-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

pdu-session-recovery call-type ims-media services { ggsn [pgw] | sgw | pgw [ggsn] | sgw | sgw [ggsn] | pgw }

no pdu-session-recovery call-type ims-media

no

Disables early PDU recovery of VoLTE calls during session recovery.

{ ggsn [pgw] | sgw | pgw [ggsn] | sgw | sgw [ggsn] | pgw }

Specifies one or more services for which this feature can be enabled.

Usage Guidelines

usage

Use this command to enable or disable support for early PDU recovery of VoLTE calls during TPDU based session recovery. When this CLI is enabled, data is allowed for VoLTE-only calls when Session Manager is recovering.

Even with GnGp association, the pgw option needs to be explicitly configured for PGW calls.
Examples

The following command enables early PDU recovery for P-GW services:

```
pdu-session-recovery call-type ims-media services pgw
```
peer-profile

This command creates a peer profile based on service type and interface and enters the Peer-Profile Configuration mode. Commands for configuration of the policies are available in the Peer Profile Configuration Mode Commands chapter.

Product

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

Privilege

Security Administrator, Administrator

Command Modes

- Exec
- Global Configuration
- configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description

`peer-profile service-type { ggsn-access | pgw-access | sgw-access | sgw-network } { default | name peer_profile_name } [-noconfirm ]`

`no peer-profile service-type { ggsn-access | pgw-access | sgw-access | sgw-network } name peer_profile_name [-noconfirm ]`

Indicates that the command is to execute without any additional prompt and confirmation from the user.

`no`

Removes the specified peer profile for specific service type from the system configuration.

`service-type`

Specifies service type for which peer profile is being configured.

- `ggsn-access` configure profile for peer nodes of GGSN.
- `pgw-access` configures profile for peer nodes of P-GW.
- `sgw-access` configures profile for peer nodes of S-GW toward S4/S11 interfaces.
- `sgw-network` configures profile for peer nodes of S-GW toward S5/S8 interfaces.
**name peer_profile_name**

Specifies the unique name of a peer profile for specific service type.

peer_profile_name is entered as an alphanumeric string of 1 through 64 characters.

**default**

default, in this case, is the name of a specific peer profile. This default profile is used when no other defined peer profile matches.

---

**Usage Guidelines**

Use this command to create a peer profile for specific service type and to enter the service specific Peer Profile configuration mode to define or modify the peer profile parameters.

The peer profile feature allows flexible profile-based configuration to accommodate growing requirements of customizable parameters with default values and actions for peer nodes of GGSN/P-GW/S-GW. With this feature, configuration of GTP-C echo parameters and disabling/enabling of Lawful intercept per MCC/MNC or IP address based on rules can be managed.

Before StarOS Release 15.0, the GGSN service allowed operator to configure list of SGSNs. Using this configuration, operator can also control some parameters associated with the configured SGSN, such as RAT type. This would be taken from configuration if CPC request does not have RAT type.

---

**Important**

The system supports up to 64 peer profiles configured for each of the peer profile types; there can be up to 1024 peer map rules configured, including all the peer maps.

---

**Examples**

The following command accesses the default peer profile for GGSN service and enters the GGSN Peer Profile configuration mode to view or modify the specified profile:

```
peer-profile service-type ggsn-access default
```
plugin

Specifies a previously installed software plugin module and enters the Plugin Configuration Mode. This function is associated with the patch process for dynamic software upgrades. A plugin module is a loadable dynamic link library (DLL) of shared objects.

Product

ADC

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

plugin module_name

module_name

Specifies the name of an existing plugin module that you want to downgrade as an alphanumeric string of 1 through 16 characters. If the named module is not known to the system, an error message is displayed.

Usage Guidelines

Specify a previously loaded software plugin module that you wish to configure. The specified module must have been previously copied onto the system and unpacked/verified via the patch plugin and install patch plugin commands.

For additional information, refer to the Plugin Configuration Mode Commands chapter.

Examples

To specify the plugin module named p2p_odyssey enter the following command:

plugin p2p_odyssey
port atm

Identifies a physical port on a line card that supports ATM signaling and then enters the configuration mode for the specific interface-type. For the commands to configure the port interface, see the CLI chapter ATM Port Configuration Mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
port atm slot/port

- **atm**
  Indicates the port identified is an ATM interface port.

- **slot/port**
  To determine valid ATM slot and port numbers, use the Exec mode's command `show port table`
  
  - **slot**: Identifies the chassis slot holding the line card that supplies ATM ports. The slot ID number can be an integer from 17 through 48.
  - **port**: Identifies the physical port that is to be configured to support ATM signaling. The ID number can be an integer from 1 through 4.

**Usage Guidelines**
Change the current configuration mode to Ethernet Port Configuration mode.

---

**Important**

This command is not supported on all platforms.

**Examples**
The following enters the ATM port configuration mode for ATM port 1 on the card in slot 19:

`port atm 19/1`
port bits

Enters the Building Integrated Timing Supply (BITS) port configuration mode by identifying the BITS port on the active or standby SPIO.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

port bits slot/port

bits
Identifies the BITS port.

slot/port

slot: Identifies the chassis slot holding the SPIO. The slot ID can be either 24 (active SPIO) or 25 (standby SPIO).

port: Identifies the BITS port on the SPIO. The port ID number must be 4.

Usage Guidelines

Change the current configuration mode to BITS port configuration mode.

Important

This command is not supported on all platforms.

Examples

The following enters the BITS port configuration mode for the active SPIO:

port bits 24/4
port channelized

Identifies a physical port on a Channelized Line Card (CLC) that supports Frame Relay signaling and creates a Frame Relay interface. This command enters the configuration mode for the commands that configure the Frame Relay interface and the channelized port interface. For additional information, see the *Channelized Port Configuration Mode Commands* chapter.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`port channelized slot/port`

`channelized`

Selects the channelized frame relay interface for the selected line card and port.

`slot/port`

To determine valid slots and port numbers, use the Exec mode's command `show port table` to find the channelized line card.

`slot`: Identifies the chassis slot holding the Channelized Line Card that sources Frame Relay ports. The slot ID number can be an integer from 17 through 48.

`port`: Identifies the physical port that is to be configured to support Frame Relay signaling. The ID number can only be 1.

**Usage Guidelines**

Change the current configuration mode to Channelized Port configuration mode.

**Examples**

The following enters the Channelized port configuration mode for port 1 on the card in slot 20:

```
port channelized 20/1
```
**port ethernet**

Enters the Ethernet Port Configuration mode for the identified port.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

`port ethernet slot/port`

- `ethernet`
  Indicates the port identified is an Ethernet interface port.

- `slot/port`
  Specifies the slot and port for which Ethernet Port Configuration mode is being entered. The slot and port must refer to an installed card and port.

**Important**

The range of slot and port numbers varies by platform type – ASR 5x00 versus VPC.

**Usage Guidelines**

Change the current configuration mode to Ethernet Port Configuration mode.

**Examples**

The following command enters the Ethernet Port Configuration mode for ethernet port 1 in slot 17 (ASR 5000):

`port ethernet 17/1`

The following command enters the Ethernet Port Configuration mode for ethernet port 11 in slot 5 (ASR 5500):

`port ethernet 5/11`
port mac-address virtual-base-address

This command defines a block of 256 consecutive media access control (MAC) addresses and enables virtual MAC addressing for Ethernet line card ports. Not available for the XT2 platform.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

- `port mac-address virtual-base-address mac_address`
- `no port mac-address virtual-base-address`

- **no**
  
  Disables virtual MAC addressing for Ethernet line card ports. The block of virtual MAC addresses is not saved.

- **mac_address**
  
  Specifies the beginning address of a block of 256 MAC addresses that are used for virtual MAC addressing.

**Usage Guidelines**

Use this command to disregard the MAC addresses assigned and stored in card firmware and assign MAC addresses for all Ethernet ports from the specified block of virtual MAC addresses. This command does not affect the MAC addresses on SPIO cards.

There are 65536 MAC addresses (00:05:47:FF:00:00 - 00:05:47:FF:FF:FF) reserved for use by customers. This range allows for the creation of 256 address blocks each containing 256 MAC addresses (for example, 00:05:47:FF:00:00, 00:05:47:FF:01:00, 00:05:47:FF:02:00, 00:05:47:FF:03:00, 00:05:47:FF:04:00, etc.).

**Caution**

This configuration requires the configuration of a valid block of unique MAC addresses that are not used anywhere else. Use of non-unique MAC addresses can degrade and impair the operation of your network.
This command is not supported on all platforms.

**Examples**

To enable virtual MAC addressing for Ethernet ports on all Ethernet line cards in the system using a block of MAC addresses starting at 00:05:47:FF:00:00, enter the following command:

```
port mac-address virtual-base-address 00:05:47:FF:00:00
```
port rs232

Enters the RS-232 Port Configuration mode for the RS-232 console port on the specified SPIO card. Not available on the XT2 platform.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`port rs232 slot 3`

- **rs232**
  
  Indicates the port identified is an RS-232 port on a SPIO card.

- **slot 3**
  
  Specifies the slot of the SPIO for which RS-232 Port Configuration mode is being entered. The slot must refer to an installed SPIO card. The specified port must always be 3 for an RS-232 port.

  The value for `slot` must be either 24 or 25.

**Usage Guidelines**

Change the current configuration mode to RS-232 Port Configuration mode.

**Examples**

The following command enters the RS-232 Port Configuration mode for the SPIO in slot 24;

```
port rs232 24 3
```
profile-id-qci-mapping

Creates a Qos Class-Identifier-Radio Access Network (QCI-RAN) ID mapping table or specifies an existing table and enters the QCI Mapping Configuration mode for the system.

**Product**
HSGW

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no | profile-id-qci-mapping name [ -noconfirm ] ]
```

- **no**
  Removes the specified mapping table from the system

- **name**
  Creates a new or enters an existing mapping table configuration. *name* must be an alphanumeric string of 1 through 63 alphanumeric.

- **-noconfirm**
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage Guidelines**

Enters the QCI-RAN ID mapping configuration mode for an existing table or for a newly defined table. This command is also used to remove an existing table.

Entering this command results in the following prompt:

```
[context_name] hostname (config-hsgw-association-table) #
```

QCI Mapping Configuration Mode commands are defined in the *QCI Mapping Configuration Mode Commands* chapter.

Use this command when configuring the HSGW eHRPD component.
Important

This command creates a mapping table available to any HSGW context configured on the system.

Examples

The following command enters the existing QCI mapping configuration mode (or creates it if it doesn't already exist) for a mapping table named qci_table1:

```
profile-id-qci-mapping qci_table1
```

The following command will remove qci_table1 from the system:

```
no profile-id-qci-mapping qci_table1
```
ps-network

This command creates/removes an HNB-PS network configuration instance for Femto UMTS access over Iu-PS/Iu-Flex interface between Home NodeB Gateway (HNB-GW) service and PS networks elements; i.e. SGSN. This command also configures an existing HNB-CS network instance and enters the HNB-CS Network Configuration mode on a system.

Product

HNBGW

Privilege

Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name(config) #

Syntax Description

[ no ] ps-network ps_instance [ -noconfirm ]

no ps-network ps_instance

no

Removes the specified HNB-PS network instance from the system.

Caution

Removing the HNB-PS network instance is a disruptive operation and it will affect all UEs accessing SGSN(s) in specific PS core network through the HNB-GW service.

Caution

If any HNB-PS Network instance is removed from the system, all parameters configured in that mode will be deleted and Iu-PS/Iu-Flex interface will be disabled.

ps_instance

Specifies the name of the Packet Switched Core Networks instance which needs to be associated with HNB Radio Network PLMN in HNB RN-PLMN configuration mode. If ps_instance does not refer to an existing HNB-PS instance, the new HNB-PS network instance is created.

ps_instance must be an alphanumeric string of 1 through 63 characters.
-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to enter the HNB-PS Network Configuration mode for an existing PS network instance or for a newly defined HNB-PS network instance. This command is also used to remove an existing HNB-PS network instance.

This configuration enables the Iu-PS/Iu-Flex interface on HNB-GW service with CS core network elements; i.e. MSC/VLR.

A maximum of 1 HNB-PS networks instance which is further limited to a maximum of 256 services (regardless of type) can be configured per system.

Caution

This is a critical configuration. The HNBs can not access SGSNs in PS core network without this configuration. Any change to this configuration would lead to disruption in HNB access to PS core network.

Entering this command results in the following prompt:

```
[context_name] hostname(config-ps-network)#
```

The various parameters available for configuration of an HNB-PS network instance are defined in the HNB-PS Network Configuration Mode Commands chapter.

Examples

The following command enters the existing HNB-PS Network configuration mode (or creates it if it doesn't already exist) for the instance named hnb-ps1:

```
ps-network hnb-ps1
```

The following command will remove HNB-PS network instance hnb-ps1 from the system without any prompt to user:

```
no ps-network hnb-ps1
```
**qci**

Defines QCI value.

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

**Privilege**
Administrator

**Command Modes**
- Exec > Global Configuration > qci-qos-mapping
- configure > qci-qos-mapping mapping_name

Entering the above command sequence results in the following prompt:

```
[context_name] host_name (config-gtpu-service)#
```

**Syntax Description**
```
qci num | delay-class delay-class-value | precedence-class precedence-class-value | reliability-class
reliability-class-value | | | downlink | 802.1p-value value | | encaps-header {copy-inner |
dscp-marking dscp-marking-value | copy-outer} | | gbr | | max-packet-delay max-packet-delay-value
max-error-rate max-error-rate | | non-gbr | | traffic-policing interval value | | uplink | 802.1p-value
value | | encaps-header {copy-inner | dscp-marking dscp-marking-value | copy-outer} | |
mpls-exp-value value | | user-datagram dscp-marking dscp-marking-value | |
no | default qci num
```

**no**
Removes the specified QCI value.

**default**
Sets the default QCI value.

**qci num**

`num` must be an integer from 1 through 256.

**delay-class delay-class-value**
Defines Pre Release 8 value for configuring packet delay.
**delay-class delay-class-value**: Defines Pre Release 8 value for configuring packet delay as an integer from 1 through 9.

**precedence-class precedence-class-value**
Defines Pre Release 8 value for configuring packet precedence.

**precedence-class precedence-class-value**: Defines Pre Release 8 value for configuring packet precedence as an integer from 1 through 32.

**reliability-class reliability-class-value**
Defines Pre Release 8 value for configuring packet reliability.

**reliability-class reliability-class-value**: Defines Pre Release 8 value for configuring packet reliability as an integer from 1 through 32.

**downlink**
Configures for downlink traffic.

**802.1p-value value**

**802.1p-value value**: Configures for downlink traffic 802.1p-value as an integer from 1 through 7.

**encaps-header { copy-inner | dscp-marking dscp-marking-value | copy-outer}**

**encaps-header**: Defines the DSCP value to be applied to encaps header.

**copy-inner**: Copy inner DSCP to outer.

**dscp-marking dscp-marking-value**: Defines the DSCP value to be applied to packets with this QCI.

**dscp-marking-value**: A Hexadecimal number between 0x0 and 0x3F.

**copy-outer**: Copies the DSCP value coming in an encapsulation header from the S1u interface to the encapsulation header sent on the S5 interface and vice-versa.

**gbr**
Sets the type of the QCI to GBR.

**max-packet-delay max-packet-delay-value**
Defines the maximum packet delay in ms for the data with the QCI as an integer from 10 through 1000.

**max-error-rate max-error-rate**
Defines the maximum error rate that the data stream can handle in power of 10 as an integer from 1 through 6.

**non-gbr**
Sets the type of the QCI to non GBR.

**traffic-policing interval value**
Sets the parameters for traffic policing interval in seconds as an integer from 1 through 100.
uplink
Configures for uplink traffic.

mpls-exp-value value
Configures for uplink traffic mpls-exp-value as an integer from 1 through 7.

user-datagram
Defines DSCP value to be applied to user data gram.

Usage Guidelines
Use this command to define QCI value in qci-qos-mapping.

Examples
The following command defines QCI value as 56:
qci 56
**qci-qos-mapping**

Global QCI-QoS mapping tables are used to map QoS Class Identifier (QCI) values to appropriate Quality of Service (QoS) parameters.

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

| Privilege | Administrator |

**Command Modes**

- Exec > Global Configuration
- `configure`

Entering the above command sequence results in the following prompt:

```
[local]\host\name\(config)\#
```

**Syntax Description**

`qci-qos-mapping name [-noconfirm]`

- `no`

Removes the specified mapping configuration from the system.

- `name`

Creates a new or enters an existing mapping configuration. `name` must be an alphanumeric string of 1 through 63 characters.

- `-noconfirm`

Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage Guidelines**

Enter the QCI-QoS mapping configuration mode for an existing table or for a newly defined table. This command is also used to remove an existing table.
Entering this command results in the following prompt:

```
(context_name)hostname(config-qci-qos-mapping)#
```

QCI - QoS Mapping Configuration Mode commands are defined in the *QCI - QoS Mapping Configuration Mode Commands* chapter.

Use this command when configuring the following eHRPD component: HSGW, P-GW, SAEGW, S-GW.

```
Important
This command creates a mapping configuration available to any GGSN, HSGW, P-GW, SAEGW, S-GW context configured on the system.
```

**Examples**

The following command enters the existing QCI - QoS mapping configuration mode (or creates it if it doesn't already exist) for a mapping configuration named `qci-qos3`:

```
qci-qos-mapping qci-qos3
```
**qos ip-dscp-iphb-mapping**

Manages internal QoS (Internal-Per-Hop-Behavior/IPHB).

<table>
<thead>
<tr>
<th>Product</th>
<th>ePDG</th>
</tr>
</thead>
<tbody>
<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>S-GW</td>
</tr>
</tbody>
</table>

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

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
qos ip-dscp-iphb-mapping dscp dscp_value internal-priority cos class_of_service_value default qos ip-dscp-iphb-mapping dscp dscp_value
```

**default**

Map any IP Differentiated Services Code Point (DSCP) to an IPHB value of 0.

**dscp dscp_value**

Map IP DSCP values into internal QoS.

- `dscp_value` must be a Hexadecimal number between 0x0 and 0x3F.

**internal-priority cos class_of_service_value**

Maps to the internal QoS priority/class of service.

- `class_of_service_value` must be a Hexadecimal number between 0x0 and 0x7.

**Usage Guidelines**

Use this command to manage internal QoS.
Examples

The following command maps DSCP values in a packet to internal-QoS COS marking values:

```
qos ip-dscp-iphb-mapping dscp 0x3 internal-priority cos 0x5
```
qos l2-mapping-table

Creates or modifies a Level 2 mapping table and enters the QoS L2 Mapping Configuration Mode to map internal QoS priority.

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

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
qos l2-mapping-table { name map_table_name | system-default }
no qos l2-mapping-table name map_table_name
```

- **no**
  Deletes the specified L2 mapping table.

---

**Important**

| Important | The system-default table cannot be deleted. Only named tables that were previously created using this CLI command can be deleted.

- **name map_table_name**
  Specifies the name of an internal table from which to map QoS to L2 values.
  *map_table_name* must be an alphanumeric string of 0 through 80 characters.

- **system-default**
  Configure the system default mapping.
Usage Guidelines

Use this command to create or modify an L2 mapping table and enter the QoS L2 Mapping Configuration Mode, which is used to map internal QoS values to L2 values.

Entering this command results in the following prompt:

\[(context\_name)host(config-qos-l2-mapping)\#

QoS L2 Mapping Configuration Mode commands are defined in the QoS L2 Mapping Configuration Mode Commands chapter.

Examples

The following command creates an L2 mapping table and enters the QoS L2 Mapping Configuration Mode:

`qos l2-mapping-table name qostable1`
qos npu inter-subscriber traffic bandwidth

Configures NPU QoS bandwidth allocations for the system.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
qos npu inter-subscriber traffic bandwidth gold percent silver percent bronze percent best-effort percent
no qos npu inter-subscriber traffic bandwidth
```

- **no**
  Removes a previous bandwidth allocation.

- **gold percent**
  Default: 10%
  Specifies the maximum percentage of bandwidth to be allocated to the gold queue priority. 
  percent can be configured to an integer from 0 through 100.

- **silver percent**
  Default: 20%
  Specifies the maximum percentage of bandwidth to be allocated to the silver queue priority. 
  percent can be configured to an integer from 0 through 100.

- **bronze percent**
  Default: 30%
  Specifies the maximum percentage of bandwidth to be allocated to the bronze queue priority. 
  percent can be configured to an integer from 0 through 100.
**best-effort percent**

Default: 40%

Specifies the maximum percentage of bandwidth to be allocated to the best-effort queue priority. *percent* can be configured to an integer from 0 through 100.

**Usage Guidelines**

The bandwidth of a subscriber queue is maintained by rate limiting functions which implement packet-rate limiting at the first level and bit-rate limiting at the next level.

The packet-rate limit of a queue is defined by the number of packets-per-second (PPS) permitted for queuing. Before queuing a packet on a subscriber queue, the NPU ensures that the packet falls within the limit. If the packet to be queued exceeds the packet rate limit, it is dropped.

Each subscriber queue is configured with a bit rate limit, measured in megabits-per-second (Mbps), referred to as CP-BPS (bit-per-second to CP). The CP-BPS is available as the total bandwidth for the subscriber traffic that a CP can sustain. Each subscriber queue receives an allocation of a certain percentage of the CP-BPS. The following maximum CP-BPS values are supported:

- Lead CP (CP0) = 128 Mbps
- Remaining CPs (CP1, CP2, CP3) = 256 Mbps

For additional information on the NPU QoS functionality, refer to the System Administration and Configuration Guide.

**Examples**

The following command configures bandwidth allocations of 20, 30, 40, and 50% for the gold, silver, bronze, and best-effort queues respectively:

```
qos npu inter-subscriber traffic bandwidth gold 20 silver 30 bronze 40 best-effort 50
```

Upon executing this command, the priority queues will have the following packet processing card CP bandwidth allocations based on the maximum CP bandwidth specifications:

<table>
<thead>
<tr>
<th>Priority</th>
<th>Lead CP (CP 0) Bandwidth (Mbps)</th>
<th>CP 1 through CP 3 Bandwidth (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gold</td>
<td>25.6</td>
<td>51.2</td>
</tr>
<tr>
<td>Silver</td>
<td>38.4</td>
<td>76.8</td>
</tr>
<tr>
<td>Bronze</td>
<td>51.2</td>
<td>102.4</td>
</tr>
<tr>
<td>Best-effort</td>
<td>64</td>
<td>128</td>
</tr>
</tbody>
</table>
qos npu inter-subscriber traffic bandwidth-sharing

Configures NPU QoS bandwidth sharing properties for the system.

**Product**
GGSN

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration
    configure
Entering the above command sequence results in the following prompt:
    [local] host_name(config)#

**Syntax Description**
qos npu inter-subscriber traffic bandwidth-sharing { { enable | disable } { all | slot slot_num cpu cpu_num } }

- **enable**
  Enables bandwidth sharing for the specified criteria.

- **disable**
  Disables bandwidth sharing for the specified criteria.

- **all**
  Specifies that the bandwidth action is to be applied to all packet processing cards and every CPU on each packet processing card.

- **slot slot_num**
  Specifies that the bandwidth action is to be applied to a packet processing card in a specific chassis slot number. slot_num is the slot in which a packet processing card is installed. These cards can be installed in slots 1 through 8 and 10 through 16 on the ASR 5000, or 1 through 4 and 7 through 10 on the ASR 5500.

- **cpu cpu_num**
  Specifies a specific control processor (CP) on a packet processing card for which to perform the bandwidth action.
  cpu_num is an integer value from 0 to 3. 0 represents the lead CP.
Usage Guidelines

The available bandwidth of a subscriber queue can be shared equally among the other subscriber queues. Any unutilized bandwidth of a queue can be shared with the other queues equally. For example, if only one DSCP is configured and it is mapped to best-effort, that DSCP would get the bandwidth allocated to the best-effort in addition to the rest of the bandwidth allocated to the gold, silver, and bronze.

By default, the system enables sharing for all packet processing cards and their CPs.

For additional information on the NPU QoS functionality, refer to the System Administration Guide.

Examples

The following command disables bandwidth sharing for the fourth CP (CP 3) on a packet processing card installed in chassis slot 3:

```
qos npu inter-subscriber traffic bandwidth-sharing disable slot 4 cpu 3
```
**qos npu inter-subscriber traffic priority**

Configures the DSCP-to-Priority assignments for the system.

**Product**
- PDSN
- GGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
qos npu inter-subscriber traffic priority { best-effort | bronze | gold | silver } assigned-to dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef | dscp_num } 
no qos npu inter-subscriber traffic priority [ assigned-to dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef } ]
```

**best-effort**

Specifies the best-effort queue priority.

**bronze**

Specifies the bronze queue priority.

**gold**

Specifies the gold queue priority.

**silver**

Specifies the silver queue priority.

**afXX**

Assigns the Assured Forwarding XX PHB (per-hop behavior) DSCP.

Each Assured Forwarding PHB has a corresponding DSCP value as follows:

- af11 through af13: DSCP values 5 through 7 respectively
- af21 through af23: DSCP values 9 through 11 respectively
- af31 through af33: DSCP values 13 through 15 respectively
- af41 through af43: DSCP values 17 through 19 respectively

**be**
Assigns the Best Effort forwarding PHB which has a corresponding DSCP value of 0.

**ef**
Assigns the Expedited Forwarding PHB which has a corresponding DSCP value of 23.

**dscp_num**
Specifies a specific DSCP value as an integer from 0 through 31.

**Usage Guidelines**
The differentiated services (DS) field of a packet contains six bits (0-5) that represent the differentiated service code point (DSCP) value.

Five of the bits (1-5) represent the DSCP. Therefore, up to 32 (2^5) DSCPs can be assigned to the various priorities. By default, they're all assigned to the lowest priority (best-effort).

For additional information on the NPU QoS functionality, refer to the *System Administration Guide*.

---

**Important**
This functionality is not supported for use with the PDSN at this time.

**Examples**
The following command maps the ef DSCP to the gold priority queue:

```
qos npu inter-subscriber traffic priority gold assigned-to dscp ef
```
quality-of-service-profile

This command creates an instance of a quality of service QoS profile and causes the system to enter the QoS Profile Configuration Mode for commands to configure the QoS parameters.

Product

MME
SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]\host_name(config)#

Syntax Description

[ no ] quality-of-service-profile qos_profile_name [ -noconfirm ]

no

Including the no command filter causes the system to delete the QoS profile instance from the system configuration.

noconfirm

Do not prompt for additional verification when executing this command.

qos_profile_name

Enter 1 to 64 alphanumeric characters to uniquely name a quality of service (QoS) profile.

Usage Guidelines

This command creates a quality of service profile and provides access to the QoS profile configuration mode to use the commands to configure the QoS parameters, refer to the QoS Profile section of the Command Line Interface Reference for command information. The parameters configured in the QoS profile will override the QoS parameters configured using the APN profile configuration commands if configured for the APN profile.
The MME's QoS profile does not become valid until it is associated with an APN profile with access type "eps". For more information, refer to the APN Profile Configuration Mode section in the Command Line Interface Reference.

Examples

Create a QoS profile named *QoStest*:

```bash
quality-of-service-profile QoStest
```
**ran-peer-map**

Creates a Radio Access Network (RAN) Peer Map and enters the RAN Peer Map Configuration Mode.

**Product**
- ASN-GW
- PHSGW

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
```plaintext
[ no ] ran-peer-map name [ -noconfirm ]
```

- `no`
  Removes the RAN Peer Map from the system.

- `name`
  Specifies the name of the RAN Peer Map. `name` must be an alphanumeric string of 1 through 31 characters.

**Usage Guidelines**
Use this command to create a new RAN Peer Map or edit an existing one. RAN peer maps reconcile base station MAC addresses received in R6 protocol messages to the base station's IP address.

Entering this command results in the following prompt:

```
[context_name]hostname(config-ran-peer-map) #
```

See the *RAN Peer Map Configuration Mode* chapter for descriptions of the commands supported in this mode.

**Examples**
The following command creates a RAN peer map named `ran12`:

```
ran-peer-map ran12
```
require active-charging

This command enables/disables Active Charging Service (ACS) with or without the Category-based Content Filtering application.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
  configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
```
require active-charging [isolated-mode] [content-filtering category [static-and-dynamic] [optimized-mode]]
no require active-charging

no
Disables ACS on the system.

isolated-mode
Enables ACS and separates ACS-related resources from other sub-system resource sharing.

*Important*
In 8.1 and later releases, this keyword is not supported.

optimized-mode
Enables ACS in Optimized mode, wherein ACS functionality is managed by SessMgrs.

*Important*
In 8.0 and earlier releases and in 9.0 and later releases, this keyword is not supported.

*Important*
In Release 8.1, ACS must be configured in the Optimized mode.
In Release 8.1, if the active-charging mode is changed from the default (non-optimized) mode to the Optimized mode, or vice-versa, the system must be rebooted for the change to take effect.

Important
In Release 8.3, this keyword is obsolete. With or without this keyword ACS is always enabled in the Optimized mode.

Use the **require active-charging** command to enable ACS in the non-optimized mode. Wherein, ACS Managers will spawn to support ACS.

Use the **require active-charging optimized-mode** command to enable ACS in the Optimized mode. Wherein, ACS is enabled as part of Session Managers.

**content-filtering category [static-and-dynamic]**
Enables the Category-based Content Filtering application with ACS support and creates the necessary Static Rating Database (SRDB) tasks to utilize the internal database of static/dynamic URLs.

For Dynamic Content Filtering support, the **static-and-dynamic** keyword must be configured to specify that the Dynamic Rater Package (model and feature files) must be distributed to rating modules on startup, recovery, etc. If not configured, by default, the static-only mode is enabled.

**Usage Guidelines**
Use this command to enable/disable ACS with or without Category-based Content Filtering application on the chassis.

Important
This command triggers the resource subsystem to switch to ACS-enabled mode and start ACS-related tasks. This CLI command must be configured before any services are configured, so that the resource subsystem can appropriately reserve adequate memory for the ACS-related tasks. After configuring this command, the configuration must be saved and the system rebooted in order to allocate the resources for ACS upon system startup.

In 8.0 and 8.1 releases, this command must be configured before configuring any services. This is to ensure that the resource subsystem can appropriately reserve adequate memory for ACS Manager tasks. If this command is configured after all the Session Manager tasks are already active, the ACS Manager tasks will not be started even if additional cards are added to the chassis—instead, the chassis must be rebooted.

**Examples**
In Release 8.0, the following command enables resource subsystem to configure ACS in isolated mode:

```
require active-charging isolated-mode
```

In Release 8.1, the following command enables ACS in Optimized mode:

```
require active-charging optimized-mode
```

In Release 8.3, the following command enables ACS in Optimized mode:

```
require active-charging
```
require demux

Enables or disables demux capabilities on an ASR 5x00 system. On an ASR 5500 when demux tasks are enabled on a management card, the Active and Standby MIOs will host and migrate all demux tasks.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description
| default | no | require demux { card | management-card | processing-card }

| default |
Demux functions will be run on a processing card.

| no |
Disables the demux capabilities except when session recovery is enabled.

Important
On a system with session recovery licensed and enabled, a processing or management card must be designated to run demux functions.

card
Prior to Release 15.0, this is an accepted keyword (defaults to processing-card).

management-card
Release 15.0+, enables demux functionality on a management (ASR 5500 MIO) card

processing-card
Enables demux functionality on a processing card (default). This is the only option on an ASR 5000.
Usage Guidelines

Use this command to configure the system to direct demux task placement.

The following restrictions apply when enabling an MIO/UMIO as a demux card:

- The **require demux management-card** command must be configured before any service or contexts have been created on the system. The command will not execute after a mode of operation has been selected for the chassis.

- Only the following services currently support the designation of an MIO/UMIO card for demux functions: GGSN, SGW, PGW, HA and SAE-GW.

- Ex-GW, L2TP, MME, NEMO and SGSN are not supported.

- After the ASR 5500 has booted with demux functions running on an MIO/UMIO, you cannot configure non-supported services. A maximum of eight Demux Managers are supported. Any attempt to add more than eight Demux Managers will be blocked.

- Service/products requiring a large number of VPN Managers, VRFs and/or Demux Managers must not enable demux functions on an MIO.

- With demux functions running on an MIO, the ASR 5500 supports a maximum of 10 contexts, 64 interfaces per context and 250 VRFs per system.

Implementation of this feature assumes that CEPS (Call Events Per Second) and the number of subscribers will remain constant, and only the data rate will increase. This ensures that the CPU demand will not increase on the MIO/UMIO.

---

**Caution**

Enabling the Demux on MIO/UMIO feature changes resource allocations within the system. This directly impacts an upgrade or downgrade between StarOS versions in ICSR configurations. Contact Cisco TAC for procedural assistance prior to upgrading or downgrading your ICSR deployment.

---

**Important**

Contact Cisco TAC for additional assistance when assessing the impact to system configurations when enabling the Demux on MIO/UMIO feature.

---

**Examples**

*For releases prior to 15.0,* to configure a DPC/UDPC as a demux card enter the following CLI commands:

```
require demux card
```

*For release 15.0+,* to configure a DPC/UDPC as a demux card enter the following CLI commands:

```
require demux processing-card
```

To configure an MIO/UMIO as a demux card enter the following CLI commands:

```
require demux management-card
```
require detailed-rohc-stats

Enables or disables context-specific Robust Header Compression (RoHC) statistics.

**Product**
- HSGW
- PDSN

**Privilege**
- Administrator

**Command Modes**
- Exec > Global Configuration
  - configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

| no | require detailed-rohc-stats |

- **no**
  - Disables statistics for RoHC calls. This is the default condition.

**Usage Guidelines**
- Enables context-specific statistics for RoHC calls.

**Examples**
- Enter the following command to enable context specific statistics for RoHC calls:
  ```
  require detailed-rohc-stats
  ```
**require diameter-proxy**

This command enables or disables Diameter Proxy mode.

**Product**

IPCF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name{(config)#

**Syntax Description**

```
require diameter-proxy { master-slave | multiple | single } | diamproxy-per-card 2 | | algorithm { facility | round-robin } |
no require diameter-proxy
```

**no**

Disables Diameter Proxy mode. This is the default configuration.

**master-slave**

Sets the Diameter-Proxy to Master-Slave mode.

In Master-Slave mode, multiple Diameter proxies are running, one on each packet processing card. One proxy serves as the Master and the other proxies are Slaves. The Master proxy relays the traffic across multiple Slave Diameter proxies.

**multiple { diamproxy-per-card 2 | | algorithm { facility | round-robin } }**

Configures one Diameter proxy for each active packet processing card.

**Important**

The [diamproxy-per-card 2 | | algorithm { facility | round-robin } ] options are primarily applicable for ASR 5500 DPC2 hardware. Multiple Diamproxies per card is the default behavior for the DPC2. This functionality can be extended to the DPC with a maximum of 2 instances of Diamproxies.

- **diamproxy-per-card**: Configure the number of Diameter proxies per card. By default, two Diamproxies are spawned for each DPC2. This allows the DPC2 to handle more transactions per proxy.
• **algorithm**: Configures the algorithm to be used to distribute the load to Diamproxies. The algorithm determines how the endpoints are distributed. Whenever an endpoint is associated with a service, the session controller sends an Allocate-Request message specifying the endpoint name with the facility type. The framework allocates a CPU based on the algorithm that has been configured.

  * **facility**: This algorithm specifies that the Diameter proxy (endpoint) will be selected based on the facility type. This is the default option. In this algorithm, all AAA endpoints will be present in CPU 0 and all session manager endpoints will be present in CPU 1.

  * **round-robin**: This algorithm specifies that the Diameter proxy selection will be in Round Robin fashion. For example, if the number of proclets running per card is 2, the first endpoint configured is associated with CPU 0 (proxy running in CPU 0 of the same card) and the next endpoint configured will be associated with CPU 1, the third one with CPU 0 and fourth one with CPU1.

```
single [diamproxy-per-card 2] [algorithm { facility | round-robin }]
```

Configures one Diameter proxy for the entire chassis.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>The [diamproxy-per-card 2] [algorithm { facility</td>
</tr>
</tbody>
</table>

• **diamproxy-per-card**: Configures the number of Diameter proxies per card. By default, two Diamproxies are spawned for each DPC2. This allows the DPC2 to handle more transactions per proxy.

• **algorithm**: Configures the algorithm to be used to distribute the load to Diamproxies. The algorithm determines how the endpoints are distributed. Whenever an endpoint is associated with a service, the session controller sends an Allocate-Request message specifying the endpoint name with the facility type. The framework allocates a CPU based on the algorithm that has been configured.

  * **facility**: This algorithm specifies that the Diameter proxy (endpoint) will be selected based on the facility type. This is the default option. In this algorithm, all AAA endpoints will be present in CPU 0 and all session manager endpoints will be present in CPU 1.

  * **round-robin**: This algorithm specifies that the Diameter proxy selection will be in Round Robin fashion. For example, if the number of proclets running per card is 2, the first endpoint configured is associated with CPU 0 (proxy running in CPU 0 of the same card) and the next endpoint configured will be associated with CPU 1, the third one with CPU 0 and fourth one with CPU1.

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>When the Diameter Proxy mode is enabled, each proxy process is a Diameter host, instead of requiring every Diameter application user (such as, every ACSMgr and/or every SessMgr, depending on the application) to be a host.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is always recommended that the chassis be rebooted when moving from non-proxy mode to proxy mode i.e. when configuring the require diameter-proxy CLI command at global configuration mode.</td>
</tr>
</tbody>
</table>
In Master-Slave mode, multiple Diameter proxies are running, one on each packet processing card. One proxy serves as the Master and the other proxies are Slaves. The Master relays the traffic from an incoming connection to a specific Slave Diameter proxy.

In releases prior to 18, when the chassis is in standby state, all the Diameter proxies are stopped. In 18 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 configures a Diameter proxy for each active packet processing card:

```bash
require diameter-proxy multiple
```

The following command configures a single Diameter proxy for the entire chassis:

```bash
require diameter-proxy single
```
require ecs credit-control

This command configures the Diameter Credit-Control Application (DCCA) to work in per subscriber-PDN level Gy mode.

**Product**
- GGSN
- HA
- IPSG
- PDSN
- P-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**

* Exec > Global Configuration
  * configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

In 14.0 and earlier releases:

```
| no | require ecs credit-control subscriber-mode
```

In 14.1 and later releases:

```
| no | require ecs credit-control session-mode per-subscriber
```

**Usage Guidelines**

In 14.0 and earlier releases:

This command is applicable to all products using the Gy interface. Use this command to configure DCCA/Gy to work in per subscriber-PDN level Gy mode, wherein one Diameter session is created per subscriber PDN rather than per bearer, and only one DCCA/Gy session is created for multi-bearer PDNs.

If this command is not configured, or the **no require ecs credit-control subscriber-mode** command is configured, DCCA/Gy sessions are created per bearer/PDP-context, and as a result when there are multiple PDP contexts or multiple bearers in a PDN as many DCCA/Gy sessions are created.
This command will take effect only when the system is booted/rebooted. When configured after the system comes up, the command will be accepted but will not be applied until after the system is rebooted with the saved configuration.

Important: This command is independent of the `require active-charging` command. The `ecs` keyword in this command is license dependent.

In 14.1 and later releases:

This CLI command is made configurable on the fly, that means, the credit control mode can be seamlessly changed from subscriber (PDN) to sub-session and vice-versa without requiring a system reboot.

This change is done to align with the new CLI commands "credit-control-client override session-mode {per-sub-session|per-subscriber}" introduced in APN and Subscriber Group configuration modes.

This will be the default mode for all subscribers unless overwritten by APN/Subscriber configuration mode CLI commands.

Releases prior to 14.1, subscriber mode Gy and bearer mode Gy were implemented based on the configuration of CLI command `require ecs credit-control subscriber-mode`. This CLI is used as a chassis level configuration which mandates that all subscribers anchored to this chassis should always be running in only one of these two modes. Enabling and disabling the CLI requires system reboot. ICSR switchover between two chassis running in two different modes will not work.

Release 14.1 and later, the Subscriber/Bearer mode Gy is selected based on APN/Subscriber mode instead of chassis wide configuration. This will provide the following:

- Flexibility to configure different modes for different subscriber.
- Flexibility to switch between modes without system reboot.
- Flexibility to switchover between two chassis working in different modes.
require graceful-cleanup-during-audit-failure

Enables or disables graceful cleanup of dropped calls during ICSR audit failures.

**Product**
- ICSR
- P-GW
- SAEGW
- S-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
```
require graceful-cleanup-during-audit-failure [ del-cause non-ims-apn { none | system-failure } ] [ default | no ] graceful-cleanup-during-audit-failure
```

- **default**
  By default, the Cause IE will be omitted from the Delete Bearer Request for Non-IMS/Custom1 APNs.

- **no**
  The Cause IE will be omitted from the Delete Bearer Request for Non-IMS/Custom1 APNs.

- **del-cause**
  For P-GW, specifies the Cause Code to be sent in the Delete Bearer Request resulting from the graceful cleanup for Audit Failure.

- **non-ims-apn { none | system-failure }**
  For Non IMS/Custom1 APNs, specifies the Cause Code to be sent in Delete Bearer Request from the P-GW resulting from the graceful cleanup for Audit Failure. By default the Cause IE will be omitted from the Delete Bearer Request for Non-IMS/Custom1 APNs.
  - **none**: Omits the GTP Cause IE from the Delete Bearer Request resulting from the graceful cleanup for Audit Failure.
• **system-failure**: Sends the GTP Cause Code SYSTEM FAILURE.

**Usage Guidelines**

Use this command to enable or disable graceful cleanup of dropped calls during ICSR audit failures.

During an audit on the gateways (P-GW/S-GW/GGSN/SAEGW) after Session Recovery or an ICSR event, if any critical information, internally or externally related to a subscriber session seems inconsistent, ICSR will locally purge the associated session information.

Since external gateways (peer nodes) are unaware of the purging of this session, the UE session may be maintained at other nodes. This leads to unnecessary hogging of resources external to the gateway and an unreachable UE for VoLTE calls.

When this feature is enabled, graceful cleanup for an ICSR audit of failed calls occurs. External signaling notifies peers of session termination before purging the session. The gateway will attempt to notify external peers of the removal of the session. External nodes to the local gateway include: S-GW, P-GW, SGSN, MME, AAA, PCRF, and IMSA.

Audit failure can occur because of missing or incomplete session information. Therefore, only the peers for which the information is available will be notified.

**Examples**

The following command sequence enables graceful cleanup and sends a Cause IE for non-IMS/Custom1 APNs of SYSTEM FAILURE.

```
require graceful-cleanup-during-audit-failure del-caus non-ims-apn system-failure
```
require ipsec-large

Enables or disables a boost in IPSec crypto processing performance.

**Product**
- ePDG
- PDIF

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration
  - configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[no] require ipsec-large
```

- **no**
  - Disables this feature.

**Usage Guidelines**

Enabling this command allows the resource manager (RM) task to assign additional IPSec managers to packet processing cards with sufficient processing capacity.

**Examples**

The following command assigns additional IPSec managers to packet processing:

```
require ipsec-large
```
**require session recovery**

Enables session recovery when hardware or software fault occurs within system.

**Product**
- ePDG
- GGSN
- ASN-GW
- HA
- HSGW
- MME
- PDG/TTG
- PDIF
- PDSN
- P-GW
- SAEGW
- SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

**Syntax Description**

| default | no | require session recovery |

**default**
Disables session recovery if enabled; requires a system restart via the `reload` command.

**no**
Disables session recovery feature after the configuration file is saved and the system is restarted via a `reload` command.
Usage Guidelines

When this feature is enabled, the system attempts to recover any home agent-based Mobile IP sessions that would normally be lost due to a hardware or software fault within the system.

This functionality is available for the following call types:

- ASN-GW services supporting simple IP, Mobile IP, and Proxy Mobile IP
- PDSN services supporting simple IP, Mobile IP, and Proxy Mobile IP
- Closed RP PDSN services supporting simple IP, Mobile IP, and Proxy Mobile IP
- HA services supporting Mobile IP and/or Proxy Mobile IP session types with or without per-user Layer 3 tunnels
- GGSN services for IPv4 and PPP PDP contexts
- SGSN services for all attached and/or activated subscribers
- LNS session types
- PDIF services supporting Simple-IP, Mobile-IP and Proxy Mobile-P
- MME services

The default setting for this command is disabled.

The no option of this command disables this feature.

This command only works when the Session Recovery feature is enabled through a valid Session and Feature Use License Key.

Important

After entering this command, you must restart the system for the command takes effect. Remember to save the configuration file before issuing the reload command.

Examples

The following command enables session recovery:

require session recovery
reveal disabled commands

Enables the input of commands for features that do not have license keys installed. The output of the command show cli indicates when this is enabled. This command effects all future CLI sessions. This is disabled by default.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

Syntax Description

[ no ] reveal disabled commands

no

Do not show disabled commands.

Usage Guidelines

When this is enabled and a disabled command is entered, a message is displayed that informs you that the required feature is not enabled and also lists the name of the feature that you need to support the command.

When this is disabled and a disabled command is entered, the CLI does not acknowledge the existence of the command and displays a message that the keyword is unrecognized.

Examples

Set the CLI to accept disabled commands and display the required feature for all future CLI sessions with the following command:

reveal disabled commands

Set the CLI to reject disabled commands and return an error message for all future CLI sessions:

no reveal disabled commands
This command enters the Rate Limiting Function (RLF) Template Configuration Mode. This mode is used to configure the RLF template to control the throttling parameters.

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
configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

Syntax Description

| no | rlf-template rlf_template_name |

no
Remove the specified RLF template from global configuration.

rlf_template_name
The name of the RLF template to create or remove. rlf_template_name must be an alphanumeric string of 1 through 127 characters.

Usage Guidelines
Use this command to enter the RLF Template Configuration mode. The users can define the rate limiting configurations within this template.

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.

This feature implements a generic framework that can be used by multiple interfaces and products for rate-limiting/throttling outgoing messages like Diameter messages on Gx, Gy interface towards PCRF.
When applications send messages to peers at a high rate, (e.g. when a large number of sessions goes down at the same time, accounting stop messages for all the sessions are generated at the same time) the peer may not be able to handle the messages at such high rates. To overcome this situation, the Rate Limiting Function (RLF) framework is developed so that the application sends messages at an optimal rate such that peer is capable of receiving all the messages and does not enter an overload condition.

When RLF feature is enabled, all the messages from the application are pushed to the RLF module for throttling and rate control, and depending on the message-rate configured the RLF module sends the messages to the peer. Once the rate or a threshold value is reached, the RLF module notifies the application to slow down or stop sending messages. RLF module also notifies the application when it is capable of accepting more messages to be sent to the peer. RLF module typically uses a Token Bucket Algorithm to achieve rate limiting.

Currently in the deployment of the Diameter applications (Gx, Gy, etc.), many operators make use of "max-outstanding <number>" as a means of achieving some rate-limiting on the outgoing control traffic. With RLF in place, this is no longer required since RLF takes care of rate-limiting in all cases. If RLF is used and max-outstanding is also used, there might be undesirable results.

**Important**

If RLF is being used with an "diameter endpoint", then set the max-outstanding value of the peer to be 255.

To use the template, Diameter or any other applications must be associated with the template. The 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.

Entering this command results in the following prompt:

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

RLF Template Configuration Mode commands are defined in the RLF Template Configuration Mode Commands chapter.

**Examples**

The following command creates an RLF template named rlf_1 and enters the RLF Template Configuration mode:

```
rlf-template rlf_1
```
**rohc-profile**

This command allows you to create an RoHC (Robust Header Compression) profile and enter the RoHC Profile Configuration Mode. This mode is used to configure RoHC Compressor and Decompressor parameters. RoHC profiles can then be assigned to specific subscriber sessions when RoHC header compression is configured.

**Product**

HSGW  
PDSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`rohc-profile profile-name name [-noconfirm] | common-options | compression-options | decompression-options | no rohc-profile profile-name name`

- **common-options**
  Configures common parameters for compressor and decompressor.

- **compression-options**
  Configures ROHC compression options.

- **decompression-options**
  Configures ROHC decompression options.

- **no**
  Remove the specified RoHC profile.

- **name**
  The name of the RoHC profile to create or remove. *name* must be an alphanumeric string of 1 through 63 characters.
**-noconfirm**

Do not prompt for additional verification when executing this command.

**Usage Guidelines**

Use this command to enter the RoHC Profile Configuration mode.

Entering this command results in the following prompt:

```
{context_name} host (config-rohcprofile-<profile_name>)#
```

RoHC Profile Configuration Mode commands are defined in the `RoHC Profile Configuration Mode Commands` chapter.

**Examples**

Enter the following command to create an RoHC profile named `HomeUsers` and enter the RoHC Configuration mode without prompting for verification:

```
rohc-profile profile-name HomeUsers
```

The following command removes the RoHC profile named `HomeUsers`:

```
no rohc-profile profile-name HomeUsers
```
sccp-network

This command creates or removes a Signaling Connection Control Part (SCCP) network instance which is used to define the SS7 end-to-end routing in a UMTS network. As well, this command enters the SCCP network configuration mode. The SGSN supports up to 12 SCCP network instances at one time.

**Product**
SGSN
HNBGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
sccp-network sccp_net_id [-noconfirm ]
no sccp-network sccp_net_id
```

- **no**
  Remove the SCCP network configuration with the specified index number from the system configuration.

  **sccp_net_id**
  This number identifies a specific SCCP network configuration.
  **sccp_net_id**: must be an integer from 1 through 12.

- **-noconfirm**
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage Guidelines**

Use this command to create or modify an SCCP network and enter the SCCP network configuration mode. The SCCP network is not a standard SS7 or UMTS concept - this concept is specific to this platform.

For details about the commands and parameters needed to create and edit the SCCP Network configuration, check the *SCCP Network Configuration Mode* chapter.
Examples

The following command creates an SCCP network with the index number of 1:

```
sccp-network 1
```

The following command creates an SCCP network with the index number of 2 to associate with HNB-GW service for HNB access network users without any prompt:

```
sccp-network 2 -noconfirm
```
sctp-param-template

This command allows you to create an SCTP parameter template and enter the SCTP Parameter Template Configuration Mode. This mode is used to configure parameters for SCTP associations.

Product
MME

Privilege
Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

| no | sctp-param-template name

no
Removes the specified SCTP parameter template from the system.

name
Specifies the name of the SCTP parameter template being created or accessed. name must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines
Use this command to enter the SCTP Parameter Template Configuration mode.

Entering this command results in the following prompt:

{context_name}host(sctp-param-template)#

SCTP Parameter Template Configuration Mode commands are defined in the SCTP Parameter Template Configuration Mode Commands chapter.

Important
The SCTP parameters will be activated in a service only if the corresponding service restarts or if the SCTP parameter template is re-associated with its corresponding service. The SCTP parameters will not be active if the SCTP template is changed.
Examples

The following command creates a new SCTP parameter template or enters an existing template named `sctp-tmpl2`:

```
sctp-param-template sctp-tmpl2
```
**session disconnect-reasons bucket-interval**

Configures an interval in minutes for displaying disconnect reasons.

**Product**

All

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
session disconnect-reasons bucket-interval  interval_minutes
no session disconnect-reasons bucket-interval  interval_minutes
```

- **no**
  
  Removes the specified bucket-interval.

- **interval_minutes**
  
  Configures interval "x" in minutes to display disconnect reasons for additional historical time intervals. The interval is specified as an integer from 1 through 20.

**Usage Guidelines**

Use this command to configure an interval in minutes for displaying historical disconnect reasons.

**Examples**

The following command specifies a bucket-interval of 5 minutes.

```
session disconnect-reasons bucket-interval 5
```
session trace

This command configures the type of network elements, file transfer protocol, and Trace collection entity mode to be used for the transportation of trace files collected for the subscriber session tracing on the UMTS/EPC network element(s) along with network connection parameters and timers.

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

**Privilege**
- Administrator

**Command Modes**
- Exec > Global Configuration
- configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
session trace network-element { all | enb | mme | pgw | sgw | ggsn | saegw } [ collection-timer sec ] [ file-type { a-type | b-type } ] [ tce-mode { none | push transport sftp path string username name { encrypted password enc_pw | password password } } ]
```

```
no session trace network-element { all | enb | mme | pgw | sgw | ggsn saegw }
```

**Important**
To modify the session trace network-element configuration, you must first enter the **no session trace network-element** form of the command to remove the session trace configuration and then enter an entirely new configuration.

```
no
```

Removes the entire session trace configuration from the system or a specific network element trace configuration.

```
network-element { all | enb | mme | pgw | sgw | ggsn saegw }
```

Identifies the type of service to the session trace application in order to determine the applicable interfaces.
all: Specifies that all network elements and their associated interfaces are to be made available to the session trace application.

cnb: Specifies that the eNodeB and its associated interfaces is to be made available to the session trace application. With this option, the allocated Trace Recording Session Reference and the Trace Reference is sent to MME over S1AP, which looks up the IMSI/IMEI associated with the corresponding S1 session and forwards the two references and UE ID to the TCE.

ggsn: Specifies that the GGSN and its associated interfaces is to be made available to the session trace application.

mme: Specifies that the MME and its associated interfaces is to be made available to the session trace application.

pgw: Specifies that the P-GW and its associated interfaces is to be made available to the session trace application.

sgw: Specifies that the S-GW and its associated interfaces is to be made available to the session trace application.

saegw: Specifies that the SAEGW and its associated interfaces is to be made available to the session trace application.

collection-timer sec
Specifies the amount of time (in seconds) to wait from initial activation/data collection before data is reported to the Trace Collection Entity (TCE). sec must be an integer from 0 through 255.

file-type { a-type | b-type }
Specifies which type of XML file is generated by the session trace. Options include an A-type file and B-type file. When B-type XML files are used, multiple trace recording session elements will be encoded in a single XML file. It should be noted that different trace recording sessions may be associated with different TCEs, according to the TCE IP address specified during activation. As expected, each Type-B XML file will contain traceRecSession elements that pertain only to the same target TCE. There will be different XML Type-B files created for different TCEs and they will be placed in different tce_x directories for transmission to the target TCEs.

Default: a-type

Important
If using the file-type keyword, it must be entered in the command before entering either of the other optional keywords.

tce-mode none
Specifies that session trace files are to be stored locally and must be pulled by the TCE.

tce-mode push transport sftp path string username name { encrypted password enc_pw | password password }
Specifies that session trace files are to be pushed to the Trace Collection Entity (TCE).
sftp: Specifies that Secure FTP is used to push session trace files to the TCE.
path string: Specifies the directory path on the TCE where files will be placed.
username name: Specifies the username to be used when pushing files to the TCE.
encrypted password \textit{enc\_pw}: Specifies the encrypted password to be used when pushing files to the TCE.
password \textit{password}: Specifies the password to be used when pushing files to the TCE.

**Usage Guidelines**

Use this command to configure the file transfer methods and modes for subscriber session trace functionality and to how and where session trace files are sent after collection.

This configuration contains collection timer, UMTS/EPC network element, type of file transfer, and user credentials setting to send the collected trace files to the TCE.

**Examples**

The following command configures the collection time for session traces to 30 seconds, identifies the network element as all elements (GGSN, MME, S-GW, SAEGW, and P-GW), and pushes session trace files to a TCE via SFTP into a directory named /trace/agw using a username \textit{admin} and a password of \textit{pw123}:

```
session trace network-element all collection-timer 30 tce-mode push transport sftp path /trace/agw username admin password pw123
```

The following command configures the collection time for session traces to 30 seconds, identifies the network element as an MME, and pushes session trace files to a TCE via SFTP into a directory named /trace/sgw using a username \textit{admin} and a password of \textit{pw123}:

```
session trace network-element mme collection-timer 30 tce-mode push transport sftp path /trace/mme username admin password pw123
```

The following command configures the collection time for session traces to 30 seconds, identifies the network element as GGSN, and pushes session trace files to a TCE via SFTP into a directory named /trace/ggsn using a username \textit{admin} and a password of \textit{pw123}:

```
session trace network-element ggsn collection-timer 30 tce-mode push transport sftp path /trace/ggsn username admin password pw123
```
gsn-global

This command gives access to the SGSN Global configuration mode to set parameters relevant to the SGSN and HNB-GW as a whole.

**Product**
- SGSN
- HNBGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
- `gsn-global`

**Usage Guidelines**
Using this command moves into SGSN Global Configuration mode. In this mode, you can set system-wide parameters on SGSN and HNB-GW to perform the following tasks:

**On SGSN:**
- monitoring and managing TLLIs in the BSSGP layer.
- defining IMSI ranges used as filters in the operator policy selection process.

**On HNB-GW:**
- setting system-wide IPC message aggregation parameters

**Examples**
Enter the SGSN Global configuration mode with the following:

```
gsn-global
```
sgsn-operator-policy

This command creates an SGSN Operator Policy and enters the SGSN operator policy configuration mode. Commands for configuration of the policies are available in the SGSN Operator Policy Configuration Mode chapter elsewhere in this Command Line Interface Reference.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

`[local]host_name(config)#`

**Syntax Description**

- `sgsn-operator-policy (default | name name) [ -noconfirm ]`
- `no sgsn-operator-policy (default | name name)`

- `-noconfirm`
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

- `no`
  Removes the specified SGSN operator policy from the system configuration.

- `default`
  In this case, default is the name of a specific operator policy. This default policy is used when no other defined operator policy matches the incoming IMSI.

**Important**

You should configure this default operator policy so that it is available to handle IMSIs that are not matched with other defined policies.
Usage Guidelines

Use this command to create an SGSN operator policy and to enter the SGSN operator policy configuration mode to define or modify policies.

The SGSN Operator Policy specifies rules governing the services, facilities and privileges available to subscribers. These policies can override standard behaviors and provide mechanisms for an operator to get around the limitations of other infrastructure elements such as DNS servers and HLRs.

The system supports up to 1000 operator policies, including the default operator policy.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Once the instance of an operator policy is defined, to use the policy it is necessary to go into the SGSN Operator Policy Configuration Mode to define the IMSI range with the MCC command - this requirement does not hold if you are using a default operator policy.</td>
</tr>
</tbody>
</table>

Examples

The following command accesses the default SGSN operator policy and enters the SGSN operator policy configuration mode to view or modify the specified policy:

**sgsn-operator-policy default**
**snmp authentication-failure-trap**

Enables or disables the SNMP traps for authentication failures.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:
```
[local]host_name(config)#
```

**Syntax Description**

```
[ no ] snmp authentication-failure-trap
```

- **no**
  Disables SNMP traps for authentication failures. When omitted, SNMP traps for authentication failures will be generated.

**Usage Guidelines**

Disables authentication failure traps if they are not of interest. At this time the option may be changed to support trouble shooting.

By default SNMP authentication failure traps are disabled.

**Examples**

The following command enables SNMP authentication failure traps:
```
snmp authentication-failure-trap
```
**snmp community**

Configures the SNMP v1 and v2 community strings.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

- configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

In StarOS 12.3 and later releases:

```
snmp community [encrypted | name string [ context context_name | read-only | read-write | view view_name ]

no snmp community [encrypted | name string
```

In StarOS 12.2:

```
snmp community [encrypted | name string [ read-only | read-write ]

no snmp community [encrypted | name string
```

In StarOS 12.1 and earlier releases:

```
snmp community string [ read-only | read-write ]

no snmp community string
```

**no**

The specified community string is removed from the configuration.

**encrypted**

Specifies the use of an encrypted string when entering the community name. Without the encrypted option, the plain-text community name must be provided.

**name string**

Specifies a community string whose options are to be modified. An unencrypted string must be an alphanumeric string of 1 through 31 characters. An encrypted string is an alphanumeric string of 1 through 80 characters.
**context context_name**

Default: community string applies to all contexts.

Specifies the context to which the community string shall be applied. *context_name* must be an alphanumeric string of 1 through 31 characters.

**read-only | read-write**

Default: read-only

Specifies if access rights for the community string.

**read-only**: the configuration may only be viewed.

**read-write**: the configuration may be viewed and edited.

**view view_name**

Default: community string applies to all views.

Specifies the view to which the community string shall be applied. *view_name* must be an alphanumeric string of 1 through 31 characters.

**Usage Guidelines**

The community strings define the privileges of SNMP users. It may be desirable to give read-only access to front line operators.

**Examples**

The following command configures an SNMP community name of *BxB102*:

```
snmp community name BxB102
```
**snmp discard-snmpv3-pdu**

Configures the system to discard all SNMPv3 protocol data units (PDUs) received.

**Product**

All

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```plaintext
[local] host_name(config)#
```

**Syntax Description**

| no | snmp discard-snmpv3-pdu |

**no**

Returns the command to the default setting, where SNMPv3 messages are processed.

**discard-snmpv3-pdu**

Configures the system to discard all SNMPv3 PDUs received.

**Usage Guidelines**

Use this command to configure the system to discard all SNMPv3 messages received. By default, the system processes SNMPv3 PDUs.

**Examples**

The following command configures the system to discard all SNMPv3 messages received.

```plaintext
snmp discard-snmpv3-pdu
```
**snmp engine-id**

Configures the SNMP engine to use for SNMP requests when SNMPv3 agents are utilized.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`snmp engine-id local id`

*id*

Specifies the SNMPv3 engine to employ. *id* must be an alphanumeric string of 1 through 31 characters.

**Usage Guidelines**

When SNMPv3 is used for SNMP access to the chassis the engine ID can be used to quickly change which schema is used for SNMP access.

**Important**

The system can send either SNMPv1, SNMPv2c, or SNMPv3 traps to numerous target devices. However, the Web Element Manager can only process SNMP version 1 (SNMPv1) and SNMP version 2c (SNMPv2c) traps. If the SNMP target being configured is Web Element Manager application, then you must not configure this command to use.

**Examples**

The following command configures an SNMP engine ID of `secure23`.

`snmp engine-id local secure23`
snmp heartbeat

Enables the sending of periodic "heartbeat" notifications (traps).

Product
All

Privilege
Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

snmp heartbeat { interval minutes | second-interval seconds } |
| default | no | snmp heartbeat

default
Resets the SNMP heartbeat to 60 minutes.

no
Disables the feature.

interval minutes
Specifies the interval time in minutes between notifications as an integer from 1 through 1440. Default: 60

second-interval seconds
Default: 30
Specifies the interval time in seconds between notifications as an integer from 10 through 50.

Usage Guidelines
Use this command to enable the sending of a heartbeat notification periodically to confirm a system is up and communicating.

Examples
The following command sets the SNMP heartbeat notification interval to 2 hours, 15 minutes.
snmp heartbeat interval 135
snmp history heartbeat

Enables the recording of heartbeat notifications in SNMP history.

**Product**
All

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ default | no ] snmp history heartbeat
```

**default**

Returns the command to the default setting of enabled.

**no**

Disables the history recording feature.

**Usage Guidelines**
Use this command to enable the recording of SNMP heartbeat notifications in SNMP history files.

**Examples**

The following command enables the recording of heartbeat notifications in SNMP history:
```
snmp history heartbeat
```
snmp mib

Enables or disables a specified SNMP Management Information Base (MIB).

Product
All

Privilege
Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local] host_name (config) #

Syntax Description
| no | snmp mib  mib_name

no
Disables the specified MIB.

mib_name
Specifies a MIB by its name. You can find the currently supported MIBs by running the Exec mode show snmp server command. Enter the MIB name as a text string exactly as displayed under "SNMP Agent Mib Configuration",
By default the STARENT-MIB is enabled.

Usage Guidelines
Use this command to enable or disable system support for an SNMP MIB.

Examples
The following command enables the SNMP MIB entitled "CISCO-MOBILE-WIRELESS-SERVICE-MIB".
snmp mib CISCO-MOBILE-WIRELESS-SERVICE-MIB
**snmpnotif-threshold**

Configures the number of SNMP notification that need to be generated for a given event before it is propagated to the SNMP users.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
snmpnotif-threshold count [ low low_count ] [ period seconds ]
| default | no | snmpnotif-threshold
```

**default**

Resets the threshold to 100.

**no**

Removes all SNMP notification thresholds. All notifications will be broadcast to SNMP users.

**count**

The traps creation rate will be monitored periodically (as configured by the `period` field). If the number of traps created over one period cycle exceeds the count value configured, then the trap creation will be disabled. `count` must be an integer from 1 through 10000. Default: 100 for release 18.0 and earlier Default: 300 for release 19.0 and forward

**low low_count**

The traps creation rate will be monitored periodically (as configured by the `period` field). The trap creation will be enabled again only if the number of trap creation drops below the `low_count` value configured. Otherwise, trap creation remains disabled. `low_count` must be an integer from 1 through 10000. Default: 20
**period seconds**

Specifies the number of seconds of the monitoring window size before any subsequent notification may be broadcast to users. *seconds* must be an integer from 10 through 3600. Default: 300

**Usage Guidelines**

Set the notification threshold to avoid a flood of events which may be the result of a single failure or maintenance activity.

**Examples**

The following command sets the SNMP notification threshold to 100 traps:

```
snmp notif-threshold 100
```
**snmp runtime-debug**

Enables or disables runtime SNMP debugging. When enabled (the default), this feature consumes CPU time with event logging. Disabling runtime debugging controls CPU usage and mitigates potential security threats when external bogus packets keep hitting SNMP.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
snmp runtime-debug | debug-tokens token_id +
no snmp runtime-debug

no
Disables SNMP runtime debugging.

ddebug-tokens token_id +
```

Enables DEBUGMSG tokens from the list of supported tokens appearing below. + indicates that multiple token IDs can be specified separated by spaces.

- `agentx` – agentx(12) token
- `disman` – disman(11) token
- `dumph` – dumph(13) token
- `dumpv` – dumpv token
- `init_mib` – init_mib(14) token
- `mib_init` – mib_init(1) token
- `parse-file` – parse-file(2) token
- `parse-mibs` – parse-mibs(3) token
- `read_config` – read_config(4) token
• **snmp** – snmp(5) token
• **snmpd** – snmpd(6) token
• **snmptrapd** – snmptrapd(7) token
• **transport** – transport(9) token
• **trap** – trap(8) token
• **usm** – usm(10) token

The numbers appearing in parentheses above will appear in the output of the `show snmp server` command for "Runtime Debug Token."

**Usage Guidelines**  
Use this command to enable and disable SNMP runtime debugging. When enabled (the default), this feature consumes CPU time with event logging. Disabling runtime debugging controls CPU usage and mitigates potential security threats when external bogus packets keep hitting SNMP.

This command also supports optional DEBUGMSG MIB tokens that represent textual MIB files that are to be found and parsed. The list of supported tokens is limited to those that appear in the CLI.

**Examples**  
The following command disables SNMP runtime debugging:

```plaintext
no snmp runtime-debug
```
**snmp server**

Enables the SNMP server as well the configuration of the SNMP server port.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```bash
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```bash
snmp server [ port number ]
no snmp server

no
```

Restores the default SNMP port assignment of 161.

```bash
port number
```

Specifies the port number to use for SNMP communications. `number` must be an integer from 1 to 65535. Default: 161

**Usage Guidelines**
Set the SNMP port for communications when SNMP is enabled.

---

**Important**

This will result in restarting the SNMP agent when the `no` keyword is omitted. SNMP queries as well as notifications/traps will be blocked until the agent has restarted.

---

**Examples**
The following command sets the SNMP server to communicate on port 100:

```bash
snmp server port 100
```
**snmp target**

Configures remote receivers for SNMP notifications.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

```plaintext
[local] host_name (config) #
```

**Syntax Description**

```plaintext
snmp target name ip_address [ port number ] [ non-default ] [ security-name string ] [ version { 1 | 2c | 3 } ] [ view ] [ security-level { noauth | auth | priv-auth privacy [ encrypted ] des privpassword } authentication [ encrypted ] { md5 | sha } authpassword ] [ informs | traps ]
```

`no`

Removes the specified target as a receiver of unsolicited SNMP messages (traps).

`authentication { md5 | sha } authpassword`

Reads the authentication type and password if the security level of the SNMP messages is set to auth or priv-auth. Authentication types are:

- **md5**: Configures the hash-algorithm to implement MD5 per RFC 1321.
- **sha**: Specifies that the hash protocol is Secure Hash Algorithm.

`security-level { noauth | { auth | priv-auth privacy [ encrypted ] des privpassword } }
```

Sets the security level of the SNMPv3 messages, as follows:

- **noauth**: No authentication and encryption is used.
- **auth**: Only authentication will be used.
- **priv-auth**: Both authentication and encryption will be used.
- **privacy des privpassword**: Reads the privacy type and password.
**name**

Specifies a logical name to use to refer to the remote receiver. *name* must be an alphanumeric string of 1 through 31 characters.

**ip_address**

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

**non-default**

Specifies that this destination is only used for SNMP traps which have been specifically identified.

**port number**

Default: 162

Specifies the port which is to be used in communicating with the remote receivers. *number* must be an integer from 0 through 65535.

**security-name string**

Default: no community string included

Specifies the community string to use in the unsolicited messages. *string* must be an alphanumeric string of 1 through 31 characters.

**version { 1 | 2c | 3 } | view**

Default: 1

Specifies the SNMP version the target supports and consequently the version of the SNMP protocol to use for communications.

---

**Important**

The system can send either SNMPv1, SNMPv2c, or SNMPv3 traps to numerous target devices. However, the Web Element Manager can only process SNMP version 1 (SNMPv1) and SNMP version 2c (SNMPv2c) traps. If the SNMP target being configured is the Web Element Manager application, then you must configure this command to use version 1 or version 2c.

**informs | traps**

Default: traps

Specifies the type of SNMP event to use to send notifications to SNMP targets. *traps* are unacknowledged (fire and forget) whereas *informs* require a response from the SNMP target.

If the notification type is set to *informs*, the notification is resent if no response is received within 5 seconds. The notification is resent at most two times.

**Usage Guidelines**

The target manages the list of remote receivers to which unsolicited messages are sent. Use this command to add/remove a monitoring system to/from a network.
Examples

The following command configures a target named `rcvr021` at IP address 10.1.1.1 to accept version 2c traps:

```
snmp target rcvr021 10.1.1.1 version 2c traps
```
**snmp trap**

This command enables or disables generation of specific or all SNMP traps.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
snmp trap { enable | suppress } {trap_name + | all | target target_name }
```

- **enable**
  Enables or allows the generation of one or more SNMP traps by the system.

- **suppress**
  Disables the generation of one or more SNMP traps by the system.

- **trap_name +**
  The name of the specific SNMP trap to enable or disable. + indicates that multiple traps separated by a space can be listed for a single instance of this command.

**Important**

The system disregards character case (case insensitive) when entering trap names.

- **all**
  Specifies that all SNMP traps will be affected by the specified operation (enable or suppress). Default: Enable All

- **target target_name**
  Specifies that these SNMP traps should be sent to the specified target name. target_name is the name of an existing SNMP target specified as an alphanumeric string of 1 through 31 characters.
**Usage Guidelines**

SNMP traps are used by the system to indicate that certain events have occurred. A complete listing of the traps supported by the system and their descriptions can be found in the *SNMP MIB Reference*. Additionally, a trap listing can be viewed using the following command:

```
snmp trap { enable | suppress } ?
```

By default, the system enables the generation of all traps. However, individual traps can be disabled allowing only traps of a certain type or alarm level to be generated. This command can be used to disable un-desired traps and/or re-enable previously suppressed traps.

**Examples**

The following command suppresses the LogMessage trap:

```
snmp trap suppress logmessage
```
snmp trap-pdu-v1tov2

Converts responses received from a SNMPv1 entity acting in an agent role into responses sent to a SNMPv2 entity acting in a manager role. This command inserts an extra zero in the outgoing trap PDU as required by RFC 1908 section 3.1.2.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration
c

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

| no | snmp trap-pdu-v1tov2 |

- no
  - Disables the adding of the extra zero in the outgoing trap PDU.

**Usage Guidelines**

Use this command to enable SNMPv2 support as defined in RFC 1908, section 3.1.2. By default, StarOS does not add the extra zero because Cisco Prime Network does not support the extra zero.

**Examples**

The following command adds the extra zero to support of SNMPv2:

```
snmp trap-pdu-v1tov2
```
snmp trap-timestamps

Adds an additional system-time varbind to generated traps.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local] host_name (config) #

Syntax Description

| no | snmp trap-timestamps

no

Disables the adding of timestamps to generated traps.

Usage Guidelines

The timestamp added to the generated trap reflects the current system time. The timestamp is proprietary. This functionality is disabled by default.

Important

If the Web Element Manager application is used as your alarm server, the application relies on the timestamp provided by enabling this command to identify duplicate traps. As a result, it is recommended that this parameter be enabled for this case.

Examples

The following command enables the inclusion of a timestamp with each generated trap:

snmp trap-timestamps
**snmp user**

Configures an SNMPv3 user for secure SNMP access.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
snmp user user_name  [ encrypted ] password password [ engine id ] [ group grp_name ] [ security-model model auth [ [ encrypted ] password password ] ]
no snmp user user_name
```

**no**

Removes the specified user from the list of valid SNMPv3 users.

**user_name**

Specifies the user which is to use SNMPv3 interfaces to the system. `user_name` must be an alphanumeric string of 1 through 31 characters.

**engine id**

The SNMP engine ID. `id` must be an alphanumeric string of 1 through 31 characters.

**group grp_name**

Default: undefined (not a member of any group)

Specifies the user SNMPv3 group the into which user will be added. `grp_name` must be an alphanumeric string of 1 to 1023 characters.

**security-model model auth**

Default: USM

Specifies the security model used to authenticate the user. `model` must be configured to the following:
The following command configures SNMP user `user1`.

```
snmp user user1
```
**ss7-routing-domain**

This command creates an SS7 routing domain instance and enters the SS7 Routing Domain Configuration mode.

**Product**

SGSN

HNBGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
ss7-routing-domain rd_id variant v_type [ -noconfirm ]
no ss7-routing-domain rd_id
```

**no**

Removes the specified SS7 routing domain from the system configuration.

**rd_id**

Identifies a specific SS7 routing domain. Once it has been created, it can be accessed for further configuration and modification by entering the `rd_id` without entering the variant.

`rd_id` must be an integer from 1 through 12.

**variant v_type**

Identifies the national standard to be used for call setup, routing and control, signaling. Select one of the following:

- **ansi**: American National Standards Institute (U.S.A.)
- **bici**: Broadband Intercarrier Interface standard
- **china**: Chinese standard
- **itu**: International Telecommunication Union (ITU-T) Telecommunication Standardization Sector
- **ntt**: Japanese standard
- **ttc**: Japanese standard

- **-noconfirm**
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

### Usage Guidelines

Use this command to create an SS7 routing domain configuration instance or to enter the SS7 routing domain configuration mode to edit the configuration.

A routing domain groups configuration items to facilitate the management of the SS7 connection resources for an SGSN service. An Access Gateway supports up to 12 configured SS7 routing domains at one time.

After entering this command, the prompt appears as:

```
[context_name]<hostname>(config-ss7-routing-domain-routing_domain_id)#
```

For details about the commands and parameters used to define or edit an SS7 routing domain, refer **SS7 Routing Domain Configuration Mode** chapter.

### Examples

The following creates an SS7 routing domain with an index of 1 and the variant selection of Broadcast Intercarrier Interface (bici):

```
ss7-routing-domain 1 variant bici
```

The following command creates an SS7 routing domain instance with an index of 2 and the variant selection of Broadcast Intercarrier Interface (bici) to be associated with HNB RN-PLMN in an HNB access network:

```
ss7-routing-domain 1 variant bici
```
**ssh key-size**

Configures the key size in bits for SSH RSA key generation for all contexts.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

```plaintext
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`ssh key-size { 2048 | 3072 | 4096 | 5120 | 6144 | 7168 | 9216 }`

**Usage Guidelines**

Configures the SSH key size in bits used to generate RSA key pairs for all contexts.

**Examples**

The following command sets the SSH key size as 4096 bits:

```plaintext
ssh key-size 4096
```
statistics-backup

Enables the *Backup and Recovery of Key KPI Statistics* functionality.

**Product**

MME  
SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration  
configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

**Syntax Description**

| no | statistics-backup { mme | sgsn | }

*no*

Disables the backup/recovery of key KPI counters.

*mme*

Enables the backup and recovery of the MME's key KPI counters, which are identified in the MME-BK schema.

*sgsn*

Enables the backup and recovery of the SGSN's key KPI counters, which are identified in the IuPS-BK schema, the GPRS-BK schema, MAP-BK schema, and the SGTP-BK schema.

**backup-interval**

| Important |

This keyword has been deprecated in Release 17.1 and replaced by the `statistics-backup-interval` command, also in this Global Configuration mode.

**Usage Guidelines**

This command enables the backup and recovery of key KPI counters after a crash. The counter values that are backed up and recovered are a subset of the counters of the MME or SGSN and SGTP schemas. For
additional information about this functionality, we recommend that you check the schema listed above in the Statistics and Counters Reference or the Backup and Recovery of Key KPI Statistics feature chapters in the associated product Administration Guide.

**Examples**

Use a command similar to the following to enable backup of the SGSN or MME's key KPI statistics:

```
statistics-backup mme
```

Use a command similar to the following to disable backup of key KPI statistics for the MME or SGSN:

```
no statistics-backup sgsn
```
statistics-backup-interval

This command defines the time between backups of the service's key KPI statistics.

**Product**

MME
SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
statistics-backup-interval  minutes
no  statistics-backup-interval
```

**no**

Disables the interval configuration.

**minutes**

Enter an integer from 1 to 60 to define the number of minutes for the interval between each backup.

**Usage Guidelines**

This interval should only be defined after the `statistics-backup` command has been entered to configure the MME or SGSN to enable backup of statistics. For details on the feature, refer to the *Backup and Recovery of Key KPI Statistics* feature chapter in the associated product *Administration Guide*.

**Examples**

Set the interval between backups to 30 minutes with the following command:

```
statistics-backup-interval 30
```
support collection

Modifies and/or enables the Support Data Collector (SDC) process. If record collection has been previously disabled, this command enables the collection activity. If the record collection is currently enabled, this command may be used to modify the sleep-duration interval and/or the maximum number of Support Data Records (SDRs) that can be collected and stored.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)>
```

**Syntax Description**

```
support collection sleep-duration { hours | minutes } value max-records number_records
| default | no | support collection

default
Resets the sleep duration and maximum number of records to their default values.

no
Removes the settings for support collection and effectively disables the SDC.

support collection
Enables the SDC.

sleep-duration { hours | minutes } value
Specifies the hours and/or minutes between record collection activity. value must be an integer from 1 through 1000. The default setting is one hour (60 minutes).

Important
The period between SDRs is equal to the configured sleep-duration interval + the time taken to collect the previous record.
max-records number_records

Specifies the maximum number of records to maintain within the record collection. number_records must be an integer from 1 through 1000. When this value is exceeded, a new SDR overwrites the oldest SDR. Default is 168.

Usage Guidelines
Use this command to control the amount of support information that is collected by the Support Data Collector. Increasing the sleep interval for data collection and reducing the number of records to be collected frees system resources for processing calls and storing other data records.
For additional information, refer to the System Administration Guide.

Examples
The following command sets the collection sleep interval to 30 minutes with a maximum of 100 records being stored:
support collection sleep-duration minutes 30 max-records 100
support record

Specifies the show commands that will be collected and output by the Support Data Collector (SDC) process in the specified record section(s). The order in which the record section commands are specified defines the order in which the collected support data record sections are saved.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

```
support record section section_name command "command_string" [ section section_name command "command_string" ] +
no support record { all | section section_name }
default support record section { all | section section_name }
```

**no support record { all | section section_name**

Removes the specified record section or all sections from the output of the SDC. This effectively disables the support data collector mechanism.

**default support record section { all | section section_name**

Resets all support record sections or the specified section to the default command listing.

**section section_name**

Identifies the record section as an alphanumeric string of 1 through 64 characters.

**command "command_string"**

Identifies a CLI show command to be included in the record section as an alphanumeric string of 1 through 256 characters enclosed in double quotation marks.
Important Refer to the System Administration Guide for a comprehensive list of command strings that can be entered via this keyword.

+ indicates that you can add command strings to the record section by repeating the section section_name command "command_string" keywords.

Usage Guidelines Use this command to tune the output of the Support Data Collector to meet specific site requirements. Refer to the System Administration Guide for a complete description of the SDC feature.

Important If the support record section command is not explicitly configured by the user, a default set of record section commands are used. These default record section commands are displayed when you run the show configuration verbose command. If support record section commands are explicitly configured, they replace the default commands.

Examples The following command creates a record section named show_ip_vrf containing the CLI command show ip vrf:

support record section vrf command "show ip vrf"
suspend local-user

Suspends a local-user administrative account.

Product

All

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]\host_name\(config)\#

Syntax Description

| no | suspend local-user name

no

Removes the suspended status for the specified local-user account.

name

The name of the local-user account expressed as an alphanumeric string of 3 through 16 characters that is case sensitive.

Usage Guidelines

This command allows a security administrator to suspend local-user administrative accounts.

A "suspended" user cannot login to the system. The user's account information (passwords, password history, etc.), however, is preserved.

Examples

The following command suspends a local-user account called Inspector1:

suspend local-user Inspector1

The following command removes the suspension from a local-user account called Admin300:

no suspend local-user Admin300
**system**

Configures system information which is accessible via SNMP.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] *host_name* (config) #

**Syntax Description**

```
system | carrier-id mcc mcc_id mnc mnc_id | contact who | description string | hostname host_name
| location text | serial-number ser_number | sysdesc-sysoid-style | default | new |
```

default

Removes the configured system contact and system location form the system.

```
carrier-id mcc mcc_id mnc mnc_id
```

---

**Important**

This carrier ID is not used by the GGSN.

Specifies a carrier-id that is a unique identifier for the carrier that has installed the system. When the carrier ID values are set, the carrier-id and gmt_offset attributes are included in access-request and accounting packets when using the following RADIUS dictionaries:

- 3gpp2
- 3gpp2-835
- starent
- starent-835
- starent-vsa1
- starent-vsa1-835
- custom9
**mcc mcc_id:** The mobile country code. This must be specified as a 3-digit string from 001 through 999.

**mnc mnc_id:** The mobile network code. This must be specified as a 2- or 3-digit string from 01 through 999.

**contact who**
Default: No contact specified.

**contact who:** specifies the contact information for the chassis. *who* must be an alphanumeric string of 0 through 255 characters. The string must be embedded in double quotes (") if spaces and special punctuation is to be used.

**description string**
Allows a user to describe the system for identification purposes. The system description can be comprised of a mix of alphanumeric characters, as follows:

- `%version%` - software version.
- `%build%` - software build number
- `%chassis%` - chassis type (ST16, ASR 5000, or ASR 5500)
- `%staros%` - OS type
- `%hostname%` - system name
- `%release%` - release number
- `%kerver%` - kernel version
- `%machine%` - machine hardware name
- `string` - an alphanumeric string of 1 through 255 characters.

**hostname host_name**

**hostname host_name:** configures the chassis host name where *host_name* must be an alphanumeric string of 1 through 63 characters.

---

**Important**
Please note that changing the chassis host name results in the command prompt changing as well to reflect the new name. This may affect any previously scripted interfaces from an OSS or maintenance facility.

**location text**
Default: No location specified.

**location text:** specifies the system location expressed as an alphanumeric string of 0 through 255 characters. The text specified must be embedded in double quotes (") if spaces are to be used.

**serial-number ser_number**
Default: None.

Specifies a system identifier as an alphanumeric string of 1 through 11 characters.
sysdesc-sysoid-style [ default | new ]

Allows the user to select the SNMP return for the objects sysDesc and sysOid.

- **default** - SNMP returns old style system description and old style system OID string.
- **new** - SNMP returns Cisco style system description and Cisco style OID string.

**Usage Guidelines**

Specify system basic information which is useful back at a network operations center which uses the SNMP interfaces for management.

**Examples**

The following commands configure the contact information, system host name, and location text, or remove configured location and system respectively.

```
system contact user1@company.com
system hostname system16
system location "Clark Street Closet\nBasement Rack 4"
```

The following commands remove the configured contact and location from system respectively

```
default system contact
default system location
```
Global Configuration Mode Commands (T-threshold phspc)

The Global Configuration Mode is used to configure basic system-wide parameters.

This section includes the commands tacacs mode through threshold phs pc-sm-entry-denial.

---

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Important**

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

- tacacs mode, page 409
- task facility acs mgr, page 410
- task facility insimgr, page 411
- task facility ipsecmgr, page 414
- task facility linkmgr, page 416
- task facility mmedemux, page 418
- task facility mmemgr, page 420
- task facility mmemgr max, page 422
- task facility mmemgr per-sesscard-count, page 424
- task facility sessmgr, page 426
- task resource cpu-memory-low, page 427
- tech-support test-commands password, page 428
• template-session-trace, page 430
• terminal, page 431
• threshold 10sec-cpu-utilization, page 433
• threshold aaa-acct-archive-queue-size, page 435
• threshold aaa-acct-archive-size, page 437
• threshold aaa-acct-failure, page 439
• threshold aaa-acct-failure-rate, page 441
• threshold aaa-auth-failure, page 443
• threshold aaa-auth-failure-rate, page 445
• threshold aaa-retry-rate, page 447
• threshold aaamgr-request-queue, page 449
• threshold asngw-auth-failure, page 451
• threshold asngw-handoff-denial, page 453
• threshold asngw-max-eap-retry, page 455
• threshold asngw-network-entry-denial, page 457
• threshold asngw-r6-invalid-nai, page 459
• threshold asngw-session-setup-timeout, page 461
• threshold asngw-session-timeout, page 463
• threshold asnpd-idle-mode-timeout, page 465
• threshold asnpd-im-entry-denial, page 467
• threshold asnpd-lu-denial, page 469
• threshold asnpd-session-setup-timeout, page 471
• threshold call-reject-no-resource, page 472
• threshold call-setup, page 474
• threshold call-setup-failure, page 476
• threshold card-temperature-near-power-off-limit, page 478
• threshold cdr-file-space, page 479
• threshold contfilt-block, page 481
• threshold contfilt-rating, page 483
• threshold cpu-available-memory, page 485
• threshold cpu-load, page 487
• threshold cpu-memory-usage, page 489
• threshold cpu-orbs-crit, page 491
• threshold cpu-orbs-warn, page 493
• threshold cpu-session-throughput, page 495
• threshold cpu-utilization, page 497
• threshold dcca-bad-answers, page 499
• threshold dcca-protocol-error, page 501
• threshold dcca-rating-failed, page 503
• threshold dcca-unknown-rating-group, page 505
• threshold diameter diameter-retry-rate, page 507
• threshold dns-learnt-ip-max-entries, page 509
• threshold dns-learnt-ipv4-max-entries, page 511
• threshold dns-learnt-ipv6-max-entries, page 513
• threshold dns-lookup-failure, page 515
• threshold edr-file-space, page 517
• threshold edr-udr-dropped flow control, page 519
• threshold epdg-current-sessions, page 521
• threshold fng-current-active-sessions, page 523
• threshold fng-current-sessions, page 525
• threshold fw-deny-rule, page 527
• threshold fw-dos-attack, page 529
• threshold fw-drop-packet, page 531
• threshold fw-no-rule, page 533
• threshold license remaining-sessions, page 535
• threshold mgmt-cpu-memory-usage, page 537
• threshold mgmt-cpu-utilization, page 539
• threshold mme-attach-failure, page 541
• threshold mme-auth-failure, page 543
• threshold model, page 545
• threshold monitoring, page 547
• threshold nat-pkt-drop, page 554
• threshold nat-port-chunks-usage, page 556
• threshold npu-utilization, page 558
• threshold packets-filtered-dropped, page 560
• threshold packets-forwarded-to-cpu, page 562
• threshold pdg-current-active-sessions, page 564
• threshold pdg-current-sessions, page 565
• threshold pdif-current-active-sessions, page 566
• threshold pdif-current-sessions, page 567
• threshold per-service-asngw-sessions, page 568
• threshold per-service-ggsn-sessions, page 570
• threshold per-service-gprs-pdp-sessions, page 572
• threshold per-service-gprs-sessions, page 574
• threshold per-service-ha-sessions, page 576
• threshold per-service-lns-sessions, page 578
• threshold per-service-pdg-sessions, page 580
• threshold per-service-pdsn-sessions, page 582
• threshold per-service-samog-sessions, page 584
• threshold per-service-sgsn-pdp-sessions, page 586
• threshold per-service-sgsn-sessions, page 588
• threshold phsgw-auth-failure, page 590
• threshold phsgw-eapol-auth-failure, page 592
• threshold phsgw-handoff-denial, page 594
• threshold phsgw-max-eap-retry, page 596
• threshold phsgw-max-eapol-retry, page 598
• threshold phsgw-network-entry-denial, page 600
• threshold phsgw-session-setup-timeout, page 602
• threshold phsgw-session-timeout, page 604
• threshold phspc-session-setup-timeout, page 606
• threshold phspc-sleep-mode-timeout, page 608
• threshold phspc-sm-entry-denial, page 610
**tacacs mode**

Enters the TACACS+ (Terminal Access Controller Access Control System+) configuration mode. Use this mode to configure up to three TACACS+ servers for use in authenticating administrative users via the TACACS+ protocol.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

*configure*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

tacacs mode

**Usage Guidelines**

Enter TACACS Configuration Mode to configure up to three TACACS+ servers for use in authenticating administrative users via the TACACS+ protocol. For additional information, see the TACACS+ Configuration Mode Commands chapter.

**Examples**

Use the following command to enter TACACS mode:

tacacs mode
**task facility acsmgr**

This command configures ACSMgr task settings.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
`task facility acsmgr start [aggressive | normal]`
`no task facility acsmgr start`

`no`
DisablestheconfiguredACSMgrsetting.

`aggressive`
Specifies to start the maximum possible ACSMgr tasks.

`normal`
Configures the resource subsystem to start/stop ACSMgr tasks on an as-needed basis.

**Usage Guidelines**
This command provides option for the resource subsystem to start maximum possible ACSMgr tasks based on the license configured and the available system configuration.

**Examples**
The following command starts the maximum possible ACSMgr tasks:

```
task facility acsmgr start aggressive
```
**task facility imsimgr**

This command is used to configure the IMSI Manager parameters.

**Product**

SGSN
MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]\host_name{config}#

**Syntax Description**

```plaintext
task facility imsimgr { avoid-sessmgr-broadcast { cpu_threshold percentage_value } | max <integer_value> |
 required-sessmgr no_sess_mgrs | sessmgr-sessions-threshold high-watermark <high_value>
 low-watermark <low_value> } 
no task facility imsimgr | avoid-sessmgr-broadcast | required-sessmgr |
default task facility imsimgr sessmgr-sessions-threshold
```

- **no**
  Disables the selected parameter's functionality in the configuration.

- **default**
  This prefix is only used with the `sessmgr-sessions-threshold` parameter. By default, the threshold levels are set to the maximum allowed sessions per Session Manager based on the card type. Both high and low watermarks are set to "100\%" by default to ensure backward compatibility.

- **avoid-sessmgr-broadcast**
  This keyword configures the IMSIMgr to avoid or disable broadcast requests to all SessMgrs when the IMSIMgr finds a particular IMSI is unknown. With this keyword, broadcasting can be disabled 'on the fly' if CPU usage is too high due to a large number of broadcast messages.

  By default, broadcasting is enabled.
**max integer_value**

This keyword defines the number of IMSI managers spawned for the system. This keyword is supported only on ASR5500 and VPC-DI platforms. A maximum of "4" IMSI Managers can be configured for release prior to 21.0.

---

**Important**

**max** is a boot-time configuration setting. It should be added in the configuration file before any SGSN/MME related configuration is created or any IMSI Manager is started. Run-time (dynamic) configuration of this parameter is stored but not effective until after the next reboot. Any attempt at dynamic configuration of this parameter results in a display of the following error message:

New config requires system restart to be effective. Please save config and restart.

---

**cpu_threshold percentage_value**

The keyword "cpu_threshold" specifies the CPU value of the IMSI Manager in percentage. The "percentage_value" is a percentage integer from 50 up to 70%. The default value is 50%.

---

**required-sessmgr**

SGSN only.

This keyword configures the required number of Session Manager instances at the IMSI Manager. By default, this parameter is disabled to ensure backward compatibility.

no_sess_mgs: The number of required Session Managers can be an integer value from "1" through "384".

---

**sessmgr-sessions-threshold**

This option is used to configure the threshold high and low watermarks, in terms of percentage, for the sessions per Session Manager. The actual session limits are derived based on the card type.

**high-watermark high_value**: The high-watermark value can be a percentage value from "70" through "100". The default percentage value is "100".

**low-watermark low_value**: The low-watermark value can be a percentage value from "50" through "100". The default percentage value is "100".

---

**Usage Guidelines**

**For the MME:**

Typically, the **avoid-sessmgr-broadcast** and **sessmgr-sessions-threshold** keywords are available for configuration but not used.

**For the SGSN:**

This command configures the number of Session Manager instances required at the IMSI Manager before forwarding any calls from the Gb Manager or Link Manager, as well, it configures the high watermark and low watermark threshold levels per Session Manager.

If the required number of Session Managers are configured through this command, once the Link Manager or Gb Manager comes up, it sends a query to the IMSI Manager to verify if the IMSI Manager has learnt the configured number of Session Manager instances. IMSI Manager readiness status is determined based on the number of Session Manager instances present in the list maintained. Once the IMSI Manager has completed learning about all the required number Session Manager instances, it informs the Link Manager and Gb Manager. Runtime enabling and modification of Session Manager instance is disabled except disabling this
configuration. Disabling of this configuration does not affect the call forwarding to the IMSI Manager as the default behavior is to always forward the calls to the IMSI Manager. This configuration is used to avoid the session imbalance across Session Manager instances due to call forwarding to the same Session Manager instance during or after re-load, if the IMSI Manager has learnt only few Session Manager instances. By default, this feature is disabled and Gb Manager or Link Manager start forwarding calls immediately during or after re-load to the IMSI Manager which in turn forwards the request to the available Session Manager instances. It is recommended to have this configuration before re-load. This option is available only under a SGSN license.

The high and low watermark limits allow the IMSI Manager to decide and select the Session Manager for processing new calls and eliminate the chances of it receiving a "call reject" in instances where the Session Manager has reached its maximum allowed session limits and the IMSI Manager is not aware of the same. The IMSI Manager converts the high and low watermark percentage to the maximum session allowed for the configured percentage based on the card type. It uses the calculated session values for both high and low watermark to decide and select the Session Manager for processing new calls. Once the Session Manager active session count reaches the calculated high watermark sessions the IMSI Manager stops forwarding the new calls to the Session Manager until the active session count becomes less than the calculated low watermark value. This option is available only under SGSN and MME licenses.

**Examples**

Use the following command to configure the required session manager count to be learnt by IMSI Manager for processing new calls to "28":

```
  task facility imsimgr required-sessmgr 28
```

Use the following command to configure the threshold for the sessions per Session Manager:

```
  task facility imsimgr avoid-sessmgr-broadcast95 low-watermark 85
```

The following command is used to disable all IMSI Manager Broadcasts:

```
  task facility imsimgr avoid-sessmgr-broadcast
```

The following command is used to disable broadcast after the IMSI Manager CPU reaches 60%:

```
  task facility imsimgr avoid-sessmgr-broadcast cpu_threshold 60
```

The following command enables broadcasting by default but once the CPU reaches a threshold of 50% the broadcast is disabled:

```
  no task facility imsimgr avoid-sessmgr-broadcast
```
task facility ipsecmgr

Configures IPSec manager settings.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description

```
task facility ipsecmgr { ikev1 { task-count { increased | normal } } | task-count { increased | normal } }
ikev1 { task-count { increased | normal } }
```

Default: normal

Adjusts the IPSec manager task count to support EHA for IKEv1. See task-count below.

```
task-count { increased | normal }
```

Default: normal

Adjusts the IPSec manager task count to support EHA.

increased: Starts additional IPSec manager tasks operating on the packet processing cards. In increased mode, they run on all but demux packet processing cards. Also, all the IPSec managers start at the same time when an active non-demux card is detected and IPSec is configured.

normal: Uses the standard algorithm for allocating memory for IPSec manager tasks. In normal mode, IPSec managers do not run on session packet processing cards.

Caution

If task-count is set to normal and session recovery is enabled, IPSec manager tasks are not allowed to start on most packet processing cards. Because the resources are not reserved, IPSec managers in normal mode only run on demux packet processing cards.

Usage Guidelines
Sets IPSec manager parameters for all IPSec managers in the system.
Examples

Use the following command to set the IPSec manager task count to **increased** mode:

```
  task facility ipsecmgr task-count increased
```
**task facility linkmgr**

This command controls the maximum number of Link Managers that can be configured for an SGSN.

**Product**  
SGSN

**Privilege**  
Security Administrator, Administrator.

**Command Modes**  
Exec > Global Configuration  
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

- `task facility linkmgr max max_linkmgrs`
- `default task facility linkmgr max`

**default**

Resets the value to 4.

**max max_linkmgrs**

Sets the maximum number of LinkMgrs configurable for the SGSN.

`max_linkmgrs` is an integer from 1 to 4. With Release 15.0, the range is from 1 to 12.

**Note**

It is recommended to restrict the number of Link Managers for PSC2 to a maximum of "4" due to memory constraints. Similarly the number of Link Managers for PSC3 can be limited to "4" when the minimal hardware configuration of "4" PSC cards is used. If the Link Managers are overloaded, then the number of Link Managers can be increased based on the number of cards available and associated ASP links needs to be updated.

**Usage Guidelines**

By default, 4 LinkMgrs will be started in the system when an SGSN service configuration is present. Use this command to change the maximum number of LinkMgrs to be started in the system.
If a change to the default is needed, this command must be used before configuring any SGSN service-related configuration, including SS7 Routing Domain and SCCP Network configurations.

The number of LinkMgrs configurable impacts the following SS7 routing domain components:

- The number of Application Server Process (ASP) instances that can be configured (maximum of 12).
- The number of peer-servers that can be configured across all SS7RDs (maximum of 512).
- The number of peer-servers that can be configured per SS7RD (maximum of 256).
- The number of Peer-Server Process (PSP) instances that can be configured per SS7 Peer (maximum of 12).

This command cannot be set dynamically. If the LinkMgr count is modified dynamically, the system must be rebooted for the change to take effect.

Examples

Change the maximum number of LinkMgrs that can be configured for an SGSN from 4 to 8:

```sh
task facility linkmgr max 8
```
task facility mmedemux

Configures wait-time and percentage parameters related to the MMEDEMUX. The MMEDEMUX distributes the incoming traffic to the associated MMEMGRs based on the percentage value and wait-time configured in this command.

Product
MME.

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

```
task facility mmedemux { mmemgr-startup-percentage percent_value | mmemgr-startup-wait-time wait_time }
nommemgr-startup-percentage mmemgr-startup-wait-time
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>mmemgr-startup-percentage percent_value</td>
<td>The percentage parameter allows the operator to configure the percentage of MMEMGRs to be associated with the MMEDEMUX.</td>
<td>90% (Default)</td>
</tr>
<tr>
<td>mmemgr-startup-wait-time wait_time</td>
<td>This parameter enables the operator to configure the time (in seconds) that the MMEDEMUX waits for MMEMGRs to start before processing incoming traffic.</td>
<td>600 (10 minutes)</td>
</tr>
</tbody>
</table>

Usage Guidelines
This command gives operators some control over the MMEDEMUX system. It allows operators to configure the percentage of MMEMGRs to be associated with the MMEDEMUX. It also assigns the waiting time before...
processing the incoming traffic. Incoming traffic is distributed to the MMEMGRs based on a combination of the configured values of the two parameters.

By default, the MME waits for ten minutes to check if 90% of the MMEMGRs have started.

**Examples**

The following configures the MMEDEMUX to distribute incoming traffic after a minimum of 5 minutes after the MME starts and as soon as 75% of the MMEMGRs are up and running:

```
task facility mmedemux mmemgr-startup-percentage 75 mmemgr-startup-wait-time 5
```
task facility mmemgr

This command scales up or down the number of MMEmgrs per PSC3/DPC/SF-VM.

**Important**

This command is deprecated from release 19.2 onwards. It was introduced in release 18.0 and is valid until release 19.0. When an operator using this configuration command upgrades to release 19.2, this CLI is mapped to a new CLI command task facility mmemgr per-sesscard-count count.

**Product**

MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

**Syntax Description**

task facility mmemgr per-sesscard-density { high | normal }
default task facility mmemgr per-sesscard-density
default

Resets the task facility mmemgr to normal density per session card/VM.

per-sesscard-density { high | normal }

**Important**

This is a boot-time configuration and should be added in the configuration file before any MME service related configuration is created or any MME Manager is started. Run-time (dynamic) configuration should be saved and will take effect only after reboot.

This keyword sets the maximum number (density) of MMEmgrs per session card. The two options are:

- **high** for High Density, which allows for eNB scaling and provides for a lower number of session cards. Currently, a maximum of 2 MMEmgrs per active session card.
- **normal** for Normal Density, the default model, which supports a max of 1 MMEmgr per active session card.
This CLI command is deprecated as it does not allow the operator to configure the required number of MME managers per session card. This command only allows two predefined modes of either "high" or "normal" density.

New commands are introduced to provide more flexibility to the operator to configure required number of MME managers per session card and to configure the desired number of MME managers per chassis.

Usage Guidelines

It is expected that this command will develop further to take advantage of higher capacity (e.g., the ASR5500) and next generation (e.g., the VPC-DI) platforms.

Examples

Use a command similar to the following to set a maximum of 2 MMEmgrs:

```
task facility mmemgr per-sesscard-density high
```
task facility mmemgr max

This command is used to configure desired number of MME managers per chassis.

Product
SGSN
MME

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description

`task facility mmemgr max value`
`default task facility mmemgr max`

default

This CLI is not configured by default. The keyword `default` resets the number of MME managers per chassis to the default values. Listed below are the default values:

<table>
<thead>
<tr>
<th>Platform/VM and card type</th>
<th>Default number of MME managers per chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR5000</td>
<td>12</td>
</tr>
<tr>
<td>ASR 5500 DPC</td>
<td>24</td>
</tr>
<tr>
<td>ASR 5500 DPC2</td>
<td>48</td>
</tr>
<tr>
<td>SSI MEDIUM/LARGE</td>
<td>1</td>
</tr>
<tr>
<td>SSI FORGE/SMALL</td>
<td>1</td>
</tr>
<tr>
<td>VPC-DI or SCALE LARGE/MEDIUM</td>
<td>24</td>
</tr>
<tr>
<td>ASR 5700</td>
<td>24</td>
</tr>
</tbody>
</table>
max
The keyword `max` is used to set the maximum number of MME managers per chassis.

Listed below is the maximum number of MME managers allowed per chassis based on the platform/VM and card type:

<table>
<thead>
<tr>
<th>Platform/VM and card type</th>
<th>Maximum number of MME managers per chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR5000</td>
<td>12</td>
</tr>
<tr>
<td>ASR 5500 DPC</td>
<td>24</td>
</tr>
<tr>
<td>ASR 5500 DPC2</td>
<td>48</td>
</tr>
<tr>
<td>SSI MEDIUM/LARGE</td>
<td>2</td>
</tr>
<tr>
<td>SSI FORGE/SMALL</td>
<td>1</td>
</tr>
<tr>
<td>VPC-DI or SCALE LARGE/MEDIUM</td>
<td>48</td>
</tr>
<tr>
<td>ASR5700</td>
<td>24</td>
</tr>
</tbody>
</table>

value
The maximum `value` is an integer with range 1 up to 36.

Usage Guidelines
This configuration change will be effective only after a chassis reload. The operator must save the configuration changes prior to a reload. The system issues appropriate warnings to the operator to indicate that configuration changes must be saved and the changes will be effective only after a chassis reload.

The maximum number of MME managers that can be configured per chassis varies based on the platform. However, the upper limit of MME managers per chassis is set to 36.

Examples
Listed below is an example where 5 MME managers are configured per chassis on an ASR5500 platform with DPC2 card:

```plaintext
task facility mmemgr max 5
```

Listed below is an example where default number of MME managers configured per chassis on an ASR5500 platform with DPC card:

```plaintext
default task facility mmemgr max
```
task facility mmemgr per-sesscard-count

This command is introduced to configure the desired number of MME managers per session card.

**Product**

SGSN
MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

task facility mmemgr per-sesscard-count count
default task facility mmemgr per-sesscard-count

default

The keyword **default** resets the number MME managers per session card to the default number of MME managers per session card/VM. By default this CLI is not configured. When this CLI is not configured default number of MME managers per session card will be selected based on platform and card type. Listed below are the default values:

<table>
<thead>
<tr>
<th>Platform/VM and card type</th>
<th>Default number of MME managers per session card</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR5000 PSC/PSC2/PSC3</td>
<td>1</td>
</tr>
<tr>
<td>ASR 5500 DPC</td>
<td>4</td>
</tr>
<tr>
<td>ASR 5500 DPC2</td>
<td>8</td>
</tr>
<tr>
<td>SSI MEDIUM/LARGE</td>
<td>2</td>
</tr>
<tr>
<td>SSI FORGE/SMALL</td>
<td>1</td>
</tr>
<tr>
<td>SCALE LARGE/MEDIUM</td>
<td>1</td>
</tr>
<tr>
<td>ASR 5700</td>
<td>1</td>
</tr>
</tbody>
</table>
per-sesscard-count

This keyword is used to configure the desired number of mmemgrs to be started on each session card.

Listed below is the maximum number of MME managers allowed per session card based on the platform/VM and card type:

<table>
<thead>
<tr>
<th>Platform/VM and card type</th>
<th>Maximum number of MME managers per session card</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR5000 PSC/PSC2/PSC3</td>
<td>2</td>
</tr>
<tr>
<td>ASR 5500 DPC</td>
<td>6</td>
</tr>
<tr>
<td>ASR 5500 DPC2</td>
<td>8</td>
</tr>
<tr>
<td>SSI MEDIUM/LARGE</td>
<td>2</td>
</tr>
<tr>
<td>SSI FORGE/SMALL</td>
<td>1</td>
</tr>
<tr>
<td>SCALE LARGE/MEDIUM</td>
<td>2</td>
</tr>
<tr>
<td>ASR 5700</td>
<td>1</td>
</tr>
</tbody>
</table>

count

Is an integer value from 1 up to 6.

Usage Guidelines

The maximum number of MME managers that can be configured per session card varies based on the platform/VM and card type. However, the upper limit of MME managers that can be configured per session card is set to 6. This configuration change will be effective only after a chassis reload. The operator must save the configuration changes prior to a reload. The system issues appropriate warnings to the operator to indicate that configuration changes must be saved and the changes will be effective only after a chassis reload. This command is not specific to any platform or card type. It is applicable and available to all platforms and card types.

Examples

Listed below is an example where 3 MME managers are configured per session card on an ASR5500 platform with DPC2 card:

```
task facility mmemgr per-sesscard-count 3
```

Listed below is an example where default number of MME managers configured per session card on an ASR5500 platform with DPC card:

```
default task facility mmemgr per-sesscard-count
```
**task facility sessmgr**

Configures system information which is accessible via SNMP.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
task { facility sessmgr start { aggressive | normal } }
```

`facility sessmgr start { aggressive | normal }`

Default: Normal

Specifies the facility options for the session manager.

- **aggressive**: specifies the maximum number of session manager processes are started immediately.

**Caution**

The `task facility sessmgr start aggressive` command should only be used if the system will reach capacity (for the existing configuration) during the first few minutes of service.

**Caution**

This command must only be executed last during configuration (or appended to the end of the configuration file) to ensure the availability of memory resources to contexts and services.

**Usage Guidelines**
Set the session manager start policy to aggressive on heavily utilized systems to avoid undue delays in processing subscriber sessions.

**Examples**

```
task facility sessmgr start aggressive
task facility sessmgr start normal
```
**task resource cpu-memory-low**

Configures the system action for SNMP trap generation and logging whenever CPU memory.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
task resource cpu-memory-low \{ kill | warn \} 
```

- \{ kill | warn \}
- Default: kill

Sets the action for the Resource Manager to take when the amount of free memory on a CPU falls below 12MB. An SNMP TRAP and CORBA notification are generated and the event is logged.

Once the free memory threshold is crossed, The Resource Manager examines all tasks on that cpu and finds the most over limit task and kills it. If there are no over limit tasks nothing happens. Resource Manager takes preference on killing a non-sessmgr task over a sessmgr task.

- **kill**: The task most over memory limit (if any) is killed and recovered.
- **warn**: The event is logged and no tasks are killed.

**Usage Guidelines**
Set the CPU memory low action to only log CPU low memory events.

**Examples**

```
task resource cpu-memory-low warn
```
**tech-support test-commands password**

Configures the password that protects access to the cli test-commands mode in the Exec mode and Global Configuration mode. This command is only visible to a user logged in as a Security Administrator.

**Product**
All

**Privilege**
Security Administrator

---

**Caution**
The cli test-commands are for use by or under the supervision of Cisco TAC.

**Command Modes**
Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
tech-support test-commands [encrypted] password  new_password  [ old-password  old_password ]
no tech-support test-commands password  [ old-password  old_password ]
```

**no**
Disables the use of a test-commands password. All subsequent attempts to execute cli test-commands in Exec or Global Configuration modes will fail. Default: no password, access disabled

**[encrypted]**

If this optional keyword is specified, the new_password is interpreted as an encrypted string containing the password value. If the encrypted keyword is not specified, then new_password is interpreted as the actual plain text value. In the output of show configuration and save configuration commands, only the encrypted option of this command syntax appears.

**new_password**

Specifies the password to be used when executing the cli test-commands command in Exec or Global Configuration modes. For a plain text password, new_password is an alphanumeric string of 1 through 64 characters. For an encrypted password, new_password is an alphanumeric string of 1 through 524 characters.
If a password is not entered via this command, the cli test-commands command remains disabled in the Exec and Global Configuration modes.

Default: no password, access disabled

---

**Important**
An SNMP trap is generated when an administrator enters or edits a password via this command (starTechSupportPasswordChanged). Refer to the SNMP MIB Reference for additional information.

---

**old-password old_password**

If the *new_password* replaces an existing password, you must enter the old password for the change to be accepted.

Entering *old-password old_password* allows you to replace the existing password without being prompted to enter the old password. If you incorrectly enter the old password or do not enter the old password, an error message appears: "Failure: Must enter matching old tech-support password to replace existing password".

---

**Usage Guidelines**
Sets the password required to execute the cli test-commands command in the Exec and Global Configuration mode.

The *show configuration* and *save configuration* commands will *never* output this value in plain text.

*new_password* is the password you wish to configure. It has either never been previously set or is different from a previously configured password. It is an alphanumeric string of 1 to 64 characters.

If the new password replaces an existing password, you must enter the old password for the change to be accepted.

If the old password is not entered or does not match the existing configured value, the following error message appears: "tech-support password is already configured". A prompt then appears to accept entry of the old password: "Enter old tech-support password:"

If *tech-support test-commands password new_password old-password old_password* is included in a script, the password will be changed as long as *old_password* is valid.

---

**Important**
Access to the cli test-commands command also requires that an administrator enables the Global Configuration mode *cli hidden* command.

---

**Examples**
The following command sets the password for cli test-commands to *testCommander*.

```
tech-support test-commands password testCommander
```
### template-session-trace

This command configures a template used for Session Tracing and Cell Traffic Tracing.

**Product**
- GGSN
- HNBGW
- MME
- P-GW
- SAEGW
- S-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```template-session-trace network-element { ggsn | hnbgw | mme | pgw | saegw | sgw } template-name template_name```

- `template_name`
  Specifies the name of the template used for tracing as an alphanumeric string of 1 through 64 characters.

**Usage Guidelines**
Operators have the option of creating a template using the `template-session-trace` command for Session Tracing and Cell Traffic Tracing in the configuration mode for the MME.

Session traces executed in the Exec mode will use this template. Once created, the template can be associated with different subscribers to trace the interfaces configured in the template.

**Examples**
The following configuration shows a template configuration for the Home NodeB network element:

```template-session-trace network-element hnbgw template-name cell-trace```
**terminal**

Configures the Console port on the ASR 5000 SPIO card. This command is *not* supported on the ASR 5500.

**Product**  
All

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
terminal [carrierdetect {off | on}] [databits {7 | 8}] [flowcontrol {hardware {off | on}} | none] [parity {even | none | odd}] [speed {115200 | 19200 | 38400 | 57600 | 9600}] [stopbits {1 | 2}]
```

carrierdetect {off | on}

Specifies whether or not the console port is to use Data Carrier Detect (DCD) when connecting to a terminal.  
Default: off

**off**: Do not use DCD.

**on**: Use DCD.

databits {7 | 8}

Specifies the number of data bits used to transmit and receive characters.  
Default: 8

**7**: Use 7 databits to transmit and receive characters.

**8**: Use 8 databits to transmit and receive characters.

flowcontrol {hardware {off | on}} | none

Specifies how the flow of data is controlled between the SPIO and a terminal.  
Default: none

**hardware**: Enables or disables the use of hardware-based flow control

**off**: Disables the use of Ready to Send (RTS) and Clear to Send (CTS).

**on**: Enables the use of Ready to Send (RTS) and Clear to Send (CTS).
none: Disables the use of DCD, RTS and CTS.

parity \{ even | none | odd \}
Specifies the type of error checking used on the port.
Default: none
- even - Enables error checking by setting the parity bit to 1 (if needed) making the number of 1s in the data bits even.
- none - Disables error checking.
- odd - Enables error checking by setting the parity bit to 1 (if needed) making the number of 1s in the data bits odd.

speed \{ 115200 | 19200 | 38400 | 57600 | 9600 \}
Specifies the flow of data in bits per second between the console port and terminal.
Default: 9600

stopbits \{ 1 | 2 \}
Specifies the number of stop bits between each transmitted character.
Default: 1
- 1: Use one stop bit between each transmitted character.
- 2: Use two stop bits between each transmitted character.

Usage Guidelines
Sets the ASR 5000 SPIO Console port parameters for communication with the terminal device.

Examples
The following command sets the SPIO Console port. The terminal must support these values.
```
terminal carriergate off databits 7 flowcontrol hardware on parity even speed 115200 stopbits 1
```
**threshold 10sec-cpu-utilization**

Configures alarm or alert thresholds that measure a 10-second average of CPU utilization. Its polling interval can be set down to 30 seconds.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
```
configure
```

Entering the above command sequence results in the following prompt:
```
[local] host_name (config)#
```

**Syntax Description**
```
threshold 10sec-cpu-utilization percent | clear percent |
```

**percent**
Default: 0
Configures Specifies the high threshold for 10-second average cpu-utilization. If the monitored CPU utilization is greater than or equal to the specified percentage an alert is sent. Regardless of the length of the polling interval, only one sample at the end of the polling interval is tested.

**clear percent**
Default: 0:
This is a low watermark value that sets the alarm clearing threshold value. If not specified it is taken from the first value.

---

**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 a threshold that sends an alert when CPU utilization over a 10-second average exceeds the limit set.

Alerts or alarms are triggered for 10-second sample of CPU utilization based on the following rules:
**threshold 10sec-cpu-utilization**

- **Enter condition**: 10-second average percentage of CPU utilization is greater than or equal to the high threshold.
- **Clear condition**: 10-second average percentage of CPU utilization is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

---

**Important**

This command is not supported on all platforms.

---

**Examples**

The following command generates an alert when the 10-second average CPU utilization reaches 45 percent:

`threshold 10sec-cpu-utilization 45`
threshold aaa-acct-archive-queue-size

Configures AAA accounting archive, alarm or alert thresholds based on the maximum values of session manager and ACS manager archive queue size.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

command

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

threshold aaa-acct-archive-queue-size1 percent | clear percent |
default threshold aaa-acct-archive-queue-size1 percent | clear percent |
threshold aaa-acct-archive-queue-size2 percent | clear percent |
default threshold aaa-acct-archive-queue-size2 percent | clear percent |
threshold aaa-acct-archive-queue-size3 percent | clear percent |
default threshold aaa-acct-archive-queue-size3 percent | clear percent |

**percent**

Configures Specifies the high threshold for monitoring the accounting message archive queue length. If the queue length is greater than or equal to the specified percentage an alarm is sent.

Default value for aaa-acct-archive-queue-size1: 25%
Default value for aaa-acct-archive-queue-size2: 50%
Default value for aaa-acct-archive-queue-size3: 90%

**clear percent**

This is a low watermark value that sets the alarm clearing threshold value. If not specified it is taken from the first value.

Default value for aaa-acct-archive-queue-size1: 25%
Default value for aaa-acct-archive-queue-size2: 50%
Default value for aaa-acct-archive-queue-size3: 90%
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

In the event that the system cannot communicate with configured AAA accounting servers (RADIUS or CGFs), either due to the server being busy or loss of network connectivity, the system buffers, or archives, the accounting messages.

Accounting message archive queue size thresholds generate alerts or alarms based on the queue length of AAA accounting messages buffered in the archive during the specified polling interval. Accounting requests are counted for all AAA accounting servers that the system is configured to communicate with.

Alerts or alarms are triggered for accounting message archive queue size thresholds based on the following rules:

- **Enter condition**: Actual number of archived messages is greater than or equal to the high threshold.
- **Clear condition**: Actual number of archived messages less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Examples

The following command generates an alarm when 70% of the AAA accounting message archive buffer is filled, and clears the alarm when the buffer size is reduced to 30%:

```
threshold aaa-acct-archive-queue-size 70 clear 30
```
threshold aaa-acct-archive-size

Configures accounting message archive size, alarm or alert thresholds.

**Product**
PDSN
GGSN
HA
ASN-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] `host_name(config)#`

**Syntax Description**

threshold aaa-acct-archive-size \( high\_thresh \) [ clear \( low\_thresh \) ]
default threshold aaa-acct-archive-size

\( high\_thresh \)

Default: 1

Specifies the high threshold number of archived accounting messages that must be met or exceeded within the polling interval to generate an alert or alarm. \( high\_thresh \) is an integer from 0 through 1044000.

\( clear \ low\_thresh \)

Default: 1

Specifies the low threshold number of archived accounting messages that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated. \( low\_thresh \) is an integer from 0 through 1044000.

**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.
In the event that the system cannot communicate with configured AAA accounting servers (RADIUS or CGFs), either due to the server being busy or loss of network connectivity, the system buffers, or archives, the accounting messages.

Accounting message archive size thresholds generate alerts or alarms based on the number of AAA accounting messages buffered in the archive during the specified polling interval. Accounting requests are counted for all AAA accounting servers that the system is configured to communicate with.

Alerts or alarms are triggered for accounting failures based on the following rules:

- **Enter condition**: Actual number of archived messages that is greater than or equal to the high threshold.
- **Clear condition**: Actual number of archived messages that is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

### Examples

The following command configures a high threshold count of 250 AAA accounting archived messages and low threshold of 100 for a system using the Alarm thresholding model:

```plaintext
threshold aaa-acct-archive-size 250 clear 100
```
threshold aaa-acct-failure

Configures accounting failure, alarm or alert thresholds for the system.

**Product**
- PDSN
- GGSN
- HA
- ASN-GW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration
- configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold aaa-acct-failure high_thresh | clear low_thresh |
default threshold aaa-acct-failure
```

**high thresh**

Default: 0

Specifies the high threshold number of accounting failures that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thresh* is an integer from 0 through 10000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of accounting failures that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated. *low_thresh* is an integer from 0 through 10000000. A value of 0 disables the threshold.

**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**

Accounting failure thresholds generate alerts or alarms based on the number of failed AAA accounting message requests that occur during the specified polling interval. Accounting requests are counted for all AAA accounting servers that the system is configured to communicate with.

Alerts or alarms are triggered for accounting failures based on the following rules:

- **Enter condition**: Actual number of failures is greater than or equal to the high threshold.
- **Clear condition**: Actual number of failures is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a high threshold count of 100 AAA accounting failures and low threshold of 25 for a system using the Alarm thresholding model:

```
threshold aaa-acct-failure 100 clear 25
```
threshold aaa-acct-failure-rate

Configures accounting failure rate, alarm or alert thresholds for the system.

**Product**
- PDSN
- GGSN
- HA
- ASN-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local] host_name (config) 
```

**Syntax Description**

```
threshold aaa-acct-failure-rate high_thresh [ clear low_thresh ]
default threshold aaa-acct-failure-rate
```

**high_thresh**
Default: 1
 Specifies the high threshold percent of accounting failures that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thresh* is an integer from 0 and 100.

**clear low_thresh**
Default: 1
 Specifies the low threshold percent of accounting failures that maintains a previously generated alarm condition. If the percentage of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated. *low_thresh* is an integer from 0 through 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

Accounting failure rate thresholds generate alerts or alarms based on the percentage of AAA accounting message requests that failed during the specified polling interval. Accounting requests are counted for all AAA accounting servers that the system is configured to communicate with.

Alerts or alarms are triggered for accounting failure rates based on the following rules:

- **Enter condition**: Actual failure percentage is greater than or equal to the high threshold.
- **Clear condition**: Actual failure percentage is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Examples

The following command configures a AAA accounting failure rate high threshold percentage of 30 and a low threshold percentage of 10 for a system using the Alarm thresholding model:

```
threshold aaa-acct-failure-rate 30 clear 10
```
threshold aaa-auth-failure

Configures authentication failure, alarm or alert thresholds for the system.

**Product**
- PDSN
- GGSN
- HA
- ASN-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration
- configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
```
threshold aaa-auth-failure high_thresh | clear low_thresh |
default threshold aaa-auth-failure
```

**high_thresh**
Default: 0
Specifies the high threshold number of authentication failures that must be met or exceeded within the polling interval to generate an alert or alarm. `high_thresh` is an integer from 0 through 10000000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0
Specifies the low threshold number of authentication failures that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated. `low_thresh` is an integer from 0 through 10000000. A value of 0 disables the threshold.

---

**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.
Authentication failure thresholds generate alerts or alarms based on the number of failed AAA authentication message requests that occur during the specified polling interval. Authentication requests are counted for all AAA authentication servers that the system is configured to communicate with. Alerts or alarms are triggered for authentication failures based on the following rules:

- **Enter condition**: Actual number of failures is greater than or equal to the high threshold.
- **Clear condition**: Actual number of failures is less than the 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 to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

The following command configures a high threshold count of 100 AAA authentication failures for a system using the Alert thresholding model:

```
threshold aaa-auth-failure 100
```
threshold aaa-auth-failure-rate

Configures authentication failure rate, alarm or alert thresholds for the system.

**Product**
PDSN
GGSN
HA
ASN-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`threshold aaa-auth-failure-rate high_thresh [ clear low_thresh ]

default threshold aaa-auth-failure-rate`

**high_thresh**

Default: 5

Specifies the high threshold percent of authentication failures that must be met or exceeded within the polling interval to generate an alert or alarm. `high_thresh` is an integer from 0 through 100.

**clear**

Allows the configuration of Specifies the low threshold.

**low_thresh**

Default: 5

Specifies the low threshold percent of authentication failures that maintains a previously generated alarm condition. If the percentage of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated. `low_thresh` is an integer from 0 through 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**

Authentication failure rate thresholds generate alerts or alarms based on the percentage of AAA authentication message requests that failed during the specified polling interval. Authentication requests are counted for all AAA authentication servers that the system is configured to communicate with.

Alerts or alarms are triggered for authentication failures based on the following rules:

- **Enter condition**: Actual failure percentage is greater than or equal to the high threshold.
- **Clear condition**: Actual failure percentage is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a AAA authentication failure rate high threshold percentage of 30 for a system using the Alert thresholding model:

`threshold aaa-auth-failure-rate 30`
threshold aaa-retry-rate

Configures AAA retry rate, alarm or alert thresholds for the system.

**Product**
- PDSN
- GGSN
- HA
- ASN-GW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration
  - configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold aaa-retry-rate high_thresh [ clear low_thresh ]
default threshold aaa-retry-rate
```

**high_thresh**

Default: 5

Specifies the high threshold percent of AAA request message retries that must be met or exceeded within the polling interval to generate an alert or alarm. `high_thresh` is an integer from 0 through 100.

**clear low_thresh**

Default: 5

Specifies the low threshold percent of AAA request message retries that maintains a previously generated alarm condition. If the percentage of retries falls beneath the low threshold within the polling interval, a clear alarm will be generated. `low_thresh` is an integer from 0 through 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**

AAA request message retry rate thresholds generate alerts or alarms based on the percentage of request messages (both authentication and accounting) that were retried during the specified polling interval. The percentage is based on a message count taken for all AAA authentication and accounting servers that the system is configured to communicate with.

Alerts or alarms are triggered for request message retries based on the following rules:

- **Enter condition**: Actual retry percentage is greater than or equal to the high threshold.
- **Clear condition**: Actual retry percentage is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a AAA message retry rate high threshold percentage of 25 and a low threshold percentage of 10 for a system using the Alarm thresholding model:

```
threshold aaa-retry-rate 25 clear 10
```
**threshold aaamgr-request-queue**

Configures the AAA Manager internal request queue, alarm or alert thresholds.

**Product**
- PDSN
- GGSN
- HA
- ASN-GW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration
  - configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold aaamgr-request-queue high_thresh [ clear low_thresh ]
default threshold aaamgr-request-queue
```

**high_thresh**

Default: 0

Specifies the high threshold number of AAA Manager Requests that must be met or exceeded within the polling interval to generate an alert or alarm. `high_thresh` is an integer from 1 through 100.

**clear**

Allows the configuration of `high_thresh`. `high_thresh` is an integer from 1 through 100.

**low_thresh**

Default: 5

Specifies the low threshold number of AAA Manager Requests that maintains a previously generated alarm condition. If the percentage of failures falls beneath the low threshold within the polling interval, a clear alarm is generated. `low_thresh` is an integer from 0 through 100.
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**

AAA Manager Request thresholds generate alerts or alarms based on the number of AAA Manager Requests for an AAA manager process during the specified polling interval.

Alerts or alarms are triggered for AAA Manager Requests based on the following rules:

- **Enter condition**: Actual number of AAA Manager Requests per AAA manager is greater than or equal to the high threshold.
- **Clear condition**: Actual number of AAA Manager Requests per AAA manager process is less than the low threshold.

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

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a AAA authentication failure rate high threshold percentage of 30 for a system using the Alert thresholding model:

```
threshold aaamgr-request-queue 30
```
**threshold asngw-auth-failure**

Configures authentication failure, alarm or alert thresholds for the ASN-GW system.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold asngw-auth-failure high_thres | clear low_thres |
default threshold asngw-auth-failure
```

**high_thres**

Default: 0

Specifies the high threshold number of authentication failures that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thres` is an integer from 0 through 10000000. A value of 0 disables the threshold.

**clear low_thres**

Default: 0

Specifies the low threshold number of authentication failures that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thres` is an integer from 0 through 10000000. A value of 0 disables the threshold.

---

**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 configure threshold limits to generate alerts or alarms based on the number of failed ASN-GW authentication message requests that occur during the specified polling interval. Authentication
requests are counted for all ASN Gateway authentication servers with which that the system is configured to communicate.

Alerts or alarms are triggered for authentication failures based on the following rules:

- **Enter condition**: Actual number of failures is greater than or equal to the high threshold.
- **Clear condition**: Actual number of failures is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

### Examples

The following command configures a high threshold count of 100 authentication failures for an ASN-GW using the Alert thresholding model:

```
threshold asngw-auth-failure 100
```
threshold asngw-handoff-denial

Configures alarm or alert thresholds for hand-off denials within the ASN-GW service.

**Product**

ASN-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold asngw-handoff-denial high_thresh | clear low_thresh |
default threshold asngw-handoff-denial
```

**high_thresh**

Default: 0

Specifies the high threshold number of hand-off denials that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 10000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of hand-off denials that maintains a previously generated alarm condition. If the number of hand-off denials falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 10000000. A value of 0 disables the threshold.

**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.
Use this command to set threshold limits to generate alerts or alarms based on the number of denied hand-off that occurred during the specified polling interval. Hand-off denial messages are counted for all ASN Gateways that the system is configured to communicate with.

Alerts or alarms are triggered for hand-off denials based on the following rules:

- **Enter condition**: Actual number of failures is greater than or equal to the high threshold.
- **Clear condition**: Actual number of failures is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a high threshold count of 100 hand-off denials using the Alert thresholding model:

```
threshold asngw-handoff-denial 100
```
threshold asngw-max-eap-retry

Configures alarm or alert thresholds for maximum retries for Extensible Authentication Protocol (EAP) authentication within an ASN-GW service.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```configure```
Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```threshold asngw-max-eap-retry high_thresh [ clear low_thresh ]
default threshold asngw-max-eap-retry```

**high_thresh**

Default: 0

Specifies the high threshold number of retries for EAP authentication that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is an integer from 0 through 10000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of retries for EAP authentication that maintains a previously generated alarm condition. If the number of retries falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` is an integer from 0 through 10000000. A value of 0 disables the threshold.

**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 threshold limits to generate alerts or alarms based on the number of retries for EAP authentication that occur during the specified polling interval.

Alerts or alarms are triggered for maximum number of retries for EAP authentication based on the following rules:

- **Enter condition**: Actual number of failures is greater than or equal to the high threshold.
- **Clear condition**: Actual number of failures is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Examples

The following command configures a high threshold count of 100 alerts or alarms generated on maximum number of retries for EAP authentication for an ASN Gateway using the Alert thresholding model:

```
threshold asngw-max-eap-retry 100
```
**threshold asngw-network-entry-denial**

Configures alarm or alert thresholds for denials of network entry to an MS within the ASN-GW service.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```plaintext
threshold asngw-network-entry-denial high_thresh [ clear low_thresh ]
default threshold asngw-network-entry-denial
```

**high_thresh**
Default: 0

Specifies the high threshold number of denial of network entry to an MS that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 10000000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0

Specifies the low threshold number of denial of network entry to an MS that maintains a previously generated alarm condition. If the number of denials falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 10000000. A value of 0 disables the threshold.

---

**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 threshold limits to generate alerts or alarms based on the number of network entry denials that occurred during the specified polling interval. Network denial messages are counted for an MS with which the system is configured to communicate.

Alerts or alarms are triggered for network entry denials based on the following rules:

- **Enter condition**: Actual number of failures is greater than or equal to the high threshold.
- **Clear condition**: Actual number of failures is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Examples

The following command configures a high threshold count of 100 network entry denials for an MS using the Alert thresholding model:

```
threshold asngw-network-entry-denial 100
```
**threshold asngw-r6-invalid-nai**

Configures alarm or alert thresholds for invalid Network Access Identifier (NAI) occurrences in R6 messages.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold asngw-r6-invalid-nai high_thresh [ clear low_thresh ]
default threshold asngw-r6-invalid-nai
```

**high_thresh**
Default: 0

Specifies the high threshold number of invalid NAI's in R6 messages that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is an integer from 0 through 10000000. A value of 0 disables the threshold.

**clear low_thres**
Default: 0

Specifies the low threshold number of invalid NAI's in R6 messages that maintains a previously generated alarm condition. If the number of denials falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thres` is an integer from 0 through 10000000. A value of 0 disables the threshold.

---

**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 threshold limits to generate alerts or alarms based on the number of invalid NAI s in R6 messages that occurred during the specified polling interval. Invalid NAIs are counted for an MS that the system is configured to communicate with or per system for all R6 messages.

Alerts or alarms are triggered for invalid NAIs based on the following rules:

- **Enter condition**: Actual number of failures is greater than or equal to the high threshold.
- **Clear condition**: Actual number of failures is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Examples

The following command configures a high threshold count of 100 invalid NAIs in R6 messages using the Alert thresholding model:

```
threshold asngw-r6-invalid-nai 100
```
**threshold asngw-session-setup-timeout**

Configures alarm or alert thresholds for session setup timeouts in an ASN-GW service.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold asngw-session-setup-timeout high_thresh [ clear low_thresh ]
default threshold asngw-session-setup-timeout
```

**high_thresh**

Default: 0

Specifies the high threshold number of timeouts during session setup that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 10000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of timeouts during session setup that maintains a previously generated alarm condition. If the number of denials falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 10000000. A value of 0 disables the threshold.

---

**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 threshold limits to generate alerts or alarms based on the number of timeouts during session setup that occurred during the specified polling interval.
Alerts or alarms are triggered for session setup timeouts based on the following rules:

- **Enter condition**: Actual number of failures is greater than or equal to the high threshold.
- **Clear condition**: Actual number of failures is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a high threshold count of 100 timeouts during session setup using the Alert thresholding model:

```
threshold asngw-session-setup-timeout 100
```
**threshold asngw-session-timeout**

Configures alarm or alert thresholds for session timeouts in an ASN-GW service.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
   `configure`

Entering the above command sequence results in the following prompt:
   `[local] host_name(config)#`

**Syntax Description**

```
threshold asngw-session-timeout high_thresh [ clear low_thresh ]
default threshold asngw-session-timeout
```

**high_thresh**
Default: 0

Specifies the high threshold number of timeouts during session that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is an integer from 0 through 10000000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0

Specifies the low threshold number of timeouts during session that maintains a previously generated alarm condition. If the number of session timeouts falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` is an integer from 0 through 10000000. A value of 0 disables the threshold.

**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 threshold limits to generate alerts or alarms based on the number of timeouts during a session that occurred during the specified polling interval.
Alerts or alarms are triggered for session timeouts based on the following rules:

• **Enter condition**: Actual number of failures is greater than or equal to the high threshold.

• **Clear condition**: Actual number of failures is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a high threshold count of 100 timeouts during a session using the Alert thresholding model:

`threshold asngw-session-timeout 100`
threshold asnpc-idle-mode-timeout

Configures alarm or alert thresholds for ASNPC Instant Messenger idle mode timeouts.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold asnpc-idle-mode-timeout  high_thresh | clear low_thresh |
```

**high_thresh**

Default: 0

Specifies the high threshold number of ASNPC idle mode timeouts that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 10000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of ASNPC idle mode timeouts during session that maintains a previously generated alarm condition. If the number of session timeouts falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 10000000. A value of 0 disables the threshold.

**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**

Set the maximum number of idle mode timeouts allowed in the ASNPC service.

Alerts or alarms are triggered for session timeouts based on the following rules:
• **Enter condition:** Actual number of timeouts is greater than or equal to the high threshold.

• **Clear condition:** Actual number of timeouts is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures the high threshold for ASNPC idle mode timeouts at 10000:

```
threshold asnpc-idle-mode-timeout 10000
```
threshold asnpc-im-entry-denial

Configures the ASNPC Instant Messenger (IM) entry denial, alarm or alert thresholds.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
threshold asnpc-im-entry-denial  high_thresh | clear low_thresh |

`high_thresh`
Default: 0
Specifies the high threshold number of IM entry denials during session that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is an integer from 0 through 10000000. A value of 0 disables the threshold.

`clear low_thresh`
Default: 0
Specifies the low threshold number of IM entry denials during session that maintains a previously generated alarm condition. If the number of session timeouts falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` is an integer from 0 through 10000000. A value of 0 disables the threshold.

**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**
Set the maximum number of IM session denials allowed in the ASNPC service.

Alerts or alarms are triggered for session timeouts based on the following rules:
- **Enter condition**: Actual number of failures is greater than or equal to the high threshold.
- **Clear condition**: Actual number of failures is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures the high threshold for IM session counts at 10000:

```
threshold asnpc-im-entry-denial 10000
```
threshold asnpc-lu-denial

Configures the alarm or alert thresholds for Location Update (LU) denials.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description
threshold asnpc-lu-denial high_thresh [ clear low_thresh ]

high_thresh
Default: 0
Specifies the high threshold number of LU denials during session that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.

clear low_thresh
Default: 0
Specifies the low threshold number of LU denials during session that maintains a previously generated alarm condition. If the number of session timeouts falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.

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
Set the maximum number of Location Update denials allowed in the ASNPC service.
Examples

The following command configures high threshold of 10000 LU denials:

```
threshold asnp-lu-denial 10000
```
threshold asnpc-session-setup-timeout

Configures alarm or alert thresholds for ASNPC session setup timeouts in an ASN-GW service.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

Syntax Description

threshold asnpc-session-setup-timeout value
default threshold asnpc-session-setup-timeout

value

value is an integer from 1 through 100000.

Usage Guidelines

Use this command to set threshold limits to generate alerts or alarms based on the number of timeouts during session setup that occurred during the specified polling interval.

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 to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

Examples

The following command configures a high threshold count of 100 timeouts during session setup using the Alert thresholding model:

threshold asnpc-session-setup-timeout 100
threshold call-reject-no-resource

Configures alarm or alert thresholds on the system for calls rejected due to insufficient resources.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description
threshold call-reject-no-resource high_thresh [ clear low_thresh ]

high_thresh
Default: 0
Specifies the high threshold number of no-resource call rejects issued by the system that must be met or exceeded within the polling interval to generate an alert or alarm.

The number is an integer from 0 through 100000. A value of 0 disables the threshold.

clear low_thresh
Default: 0
Specifies the low threshold number of no-resource call rejects issued by the system that maintains a previously generated alarm condition. If the number of rejections falls beneath the low threshold within the polling interval, a clear alarm will be generated.

The number is an integer from 0 through 100000. A value of 0 disables the threshold.

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
No resource call reject thresholds generate alerts or alarms based on the total number of calls that were rejected by the system due to insufficient or no resources (memory and/or session licenses) during the specified polling interval.
Alerts or alarms are triggered for no-resource-rejected calls based on the following rules:

- **Enter condition**: Actual number of calls rejected due to no resources is greater than or equal to the high threshold.
- **Clear condition**: Actual number of calls rejected due to no resources is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a high threshold count for the number of calls rejected by the system due to insufficient or no resources to 100 and allow threshold of 40 for a system using the Alarm thresholding model:

```
threshold call-reject-no-resource 100 clear 40
```
threshold call-setup

Configures call setup, alarm or alert thresholds for the system.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

command

Entering the above command sequence results in the following prompt:

[local]\host_name(config)#

Syntax Description

threshold call-setup high_thresh [ clear low_thresh ]

high_thresh

Default: 0

Specifies the high threshold number of calls setup by the system that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 100000. A value of 0 disables the threshold.

clear low_thresh

Default: 0

Specifies the low threshold number of calls setup by the system that maintains a previously generated alarm condition. If the number of setups falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 100000. A value of 0 disables the threshold.

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

Call setup thresholds generate alerts or alarms based on the total number of calls setup by the system during the specified polling interval.
Alerts or alarms are triggered for call setups based on the following rules:

- **Enter condition:** Actual number of call setups is greater than or equal to the high threshold.
- **Clear condition:** Actual number of call setups is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a high threshold count of 100 calls setup for a system using the Alert thresholding model:

```
threshold call-setup 100
```
threshold call-setup-failure

Configures call setup failure, alarm or alert thresholds for the system.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] *host_name* (config) #

**Syntax Description**

`threshold call-setup-failure high_thresh [ clear low_thresh ]`

**high_thresh**

Default: 0

Specifies the high threshold number of call setup failures experienced by the system that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is an integer from 0 through 100000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of call setup failures experienced by the system that maintains a previously generated alarm condition. If the number of setup failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` is an integer from 0 through 100000. A value of 0 disables the threshold.

**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**

Call setup failure thresholds generate alerts or alarms based on the total number of call setup failures experienced by the system during the specified polling interval.
Alerts or alarms are triggered for call setup failures based on the following rules:

- **Enter condition:** Actual number of call setup failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of call setup failures is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a high threshold count of 100 call setup failures and a low threshold of 80 for a system using the Alarm thresholding model:

```
threshold call-setup-failure 100 clear 80
```
threshold card-temperature-near-power-off-limit

Configures alarm or alert thresholds for triggering and clearing high card temperature alarms.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold card-temperature-near-power-off-limit [high_temp] [clear] [low_temp]
```

- **high_thresh**
  - Default: 0
  - Specifies the high card temperature (in degrees Celsius) that must be met or exceeded within the polling interval to generate an alert or alarm.
  - `high_thresh` is an integer from 0 through 100. A value of 0 disables the threshold.

- **clear low_thresh**
  - Default: 0
  - Specifies the low card temperature (in degrees Celsius) before a high temperature alarm is cleared.
  - `low_thresh` is an integer from 0 through 100. A value of 0 disables the threshold.

**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**
Set the high and low temperatures in degrees Celsius that generate and clear alarms.

**Examples**
The following command configures sets the high and low temperatures to 40 and 35 degrees:

```
threshold card-temperature-near-power-off-limit 40 clear 35
```
**threshold cdr-file-space**

Configures, alarm or alert thresholds for monitoring the percentage of total file space allocated for Charging Data Records (CDRs) used during the polling interval.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec & Global Configuration

Execution:

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold cdr-file-space high_thresh [ clear low_thresh ]
default threshold cdr-file-space
```

default
Configures this command with the default threshold settings.

**high_thresh**

Specifies the high threshold for percentage of total allocated CDR file space used that must be met or exceeded at the end of the polling interval to generate an alert or alarm.

*high_thresh* is measured in percentage of total allocated CDR file space used and is an integer from 0 through 100. A value of 0 disables the threshold.

Default: 90

**clear low_thresh**

Specifies the low threshold for percentage of total allocated CDR file space used that maintains a previously generated alarm condition. If the space usage falls below the *low_thresh* within the polling interval, a clear alarm is generated.

*low_thresh* is measured in percentage of total allocated CDR file space used and is an integer from 0 through 100. A value of 0 disables the threshold.

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 Specifies the low threshold.

**Usage Guidelines**

CDR file space usage generate alerts or alarms based on the percentage of total allocated CDR file space used during the polling interval.

Alerts or alarms are triggered for CDR file space usage session based on the following rules:

- **Enter condition**: Actual percentage of allocated CDR file space usage is greater than or equal to the specified percentage of total CDR file space.
- **Clear condition**: Actual CDR file space used is less than the specified clear percentage of total allocated CDR file space usage.

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

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a threshold of 65 percent of total allocated CDR file space usage and a clear threshold of 35 percent:

```
threshold cdr-file-space 65 clear 35
```
threshold contfilt-block

Configures, alarm or alert thresholds for Content Filtering rating operations blocked during a polling interval at which the threshold are raised or cleared.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

   [local]<host_name>{config}#

**Syntax Description**

threshold contfilt-block *high_thresh_value* [ clear *low_thresh_value* ]

*default*

Configures this command with the default threshold settings.

*high_thresh*

Specifies the high threshold for number of rating operations blocked for content filtering service that must be met or exceeded at the end of the polling interval to generate an alert or alarm.

*high_thresh* is measured in numbers of total rating operations blocked and is an integer from 0 through 1000000. A value of 0 disables the threshold.

*clear low_thresh*

Specifies the low threshold for the total number of rating operations blocked for a content filtering service that maintains a previously generated alarm condition. If the threshold falls below *low_thresh* within the polling interval, a clear alarm is generated.

*low_thresh* is measured in numbers of total rating operations blocked and is an integer from 0 through 1000000. A value of 0 disables the threshold.

Default: 0

**Usage Guidelines**

Use this command to configure the threshold for a content filtering service to generates alerts or alarms based on the number of rating operations blocked for a content filtering service during the polling interval.
If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll contfilt-block` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a threshold of 65000 rating operations blocked and a clear threshold of 35000 operations:

```
threshold contfilt-block 65000 clear 35000
```
threshold contfilt-rating

Configures, alarm or alert thresholds for Content Filtering rating operations performed during a polling interval at which the threshold are raised or cleared.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure
Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold contfilt-rating high_thresh_value | clear low_thresh_value | default threshold contfilt-rating
```

default
Configures this command with the default threshold settings.

**high_thresh**
Specifies the high threshold for number of rating operations performed for content filtering service that must be met or exceeded at the end of the polling interval to generate an alert or alarm.

*high_thresh* is measured in numbers of total rating operations performed and is an integer from 0 through 1000000. A value of 0 disables the threshold.

**clear low_thresh**
Specifies the low threshold for the total number of rating operations performed for a content filtering service that maintains a previously generated alarm condition. If the threshold falls below *low_thresh* within the polling interval, a clear alarm is generated.

*low_thresh* is measured inumber of total rating operations performed and is an integer from 0 through 1000000. A value of 0 disables the threshold.

Default: 0

**Usage Guidelines**
Use this command to configure the threshold for a content filtering service to generates alerts or alarms based on the number of rating operations performed for a content filtering service during the polling interval.
If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll contfilt-rating` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a threshold of 65000 percent of total rating operations performed and a clear threshold of 35000 percent:

```
threshold contfilt-rating 65000 clear 35000
```
threshold cpu-available-memory

Configures alarm or alert thresholds for available CPU memory in the system.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
threshold cpu-available-memory low_thresh [ clear high_thresh ]

- **low_thresh**
  Default: 32
  Specifies the low threshold amount of CPU memory that must be met or exceeded at the polling time to generate an alert or alarm.
  low_thresh is measured in megabytes (MB) and is an integer from 0 through 2048.

- **clear high_thresh**
  Default: 32
  Specifies the high threshold amount of CPU memory that maintains a previously generated alarm condition. If the memory amount rises above the high threshold within the polling interval, a clear alarm will be generated.
  high_thresh is measured in megabytes (MB) and is an integer from 0 through 2048.

**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**
CPU available memory thresholds generate alerts or alarms based on the amount of available memory for each packet processing card CPU at the polling time. Although, a single threshold is configured for all CPUs, separate alerts or alarms can be generated for each CPU.
Alerts or alarms are triggered for available CPU memory based on the following rules:

- **Enter condition**: Average measured amount of memory/CPU for the last 5 minutes is less than or equal to the low threshold.
- **Clear condition**: Average measured amount of memory/CPU for the last 5 minutes is greater than the 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.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

---

**Important**

This command is not supported on all platforms.

---

**Examples**

The following command configures a low threshold count of 50 MB CPU memory available and a high threshold of 112 MB for a system using the Alarm thresholding model:

```
threshold cpu-available-memory 50 clear 112
```
threshold cpu-load

Configures alarm or alert thresholds for monitoring packet processing card CPU loads using a 5-minute average measurement. The threshold is enabled by enabling CPU resource monitoring.

Product: All

Privilege: Security Administrator, Administrator

Command Modes: Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local]host_name(config)#

Syntax Description:

threshold cpu-load high_thresh | clear low_thresh |

high_thresh
Default: 0
If the monitored CPU load is greater than or equal to the specified number an alert is sent. high_thresh must be an integer from 0 through 15.

clear low_thresh
Default: 0
This is a low watermark value that sets the alarm clearing threshold value. If not present it is taken from the first value. low_thresh must be an integer from 0 through 15.

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 Specifies the low threshold.

Usage Guidelines:

Use this command to set an alert when the card's CPU load is equal to or greater than the number specified. Alerts or alarms are triggered for CPU load based on the following rules:

• **Enter condition:** Actual CPU load is greater than or equal to the high threshold.
• **Clear condition:** Actual CPU load is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Important**
This command is not supported on all platforms.

**Examples**
To set an alert when the packet processing card CPU load is over 10 and set an alert clear when the CPU load drops down equal or less than 7, enter the following command;

```
threshold cpu-load 10 clear 7
```
threshold cpu-memory-usage

Configures, alarm or alert thresholds for monitoring the percentage of total CPU memory used during the polling interval.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

`threshold cpu-memory-usage high_thresh | clear low_thresh`

`high_thresh`

Default: 0

Specifies the high threshold for percentage of total memory used that must be met or exceeded at the end of the polling interval to generate an alert or alarm.

`high_thresh` is measured as a percentage of total CPU memory used and is an integer from 0 and 100. A value of 0 disables the threshold.

`clear low_thresh`

Default: 0

Specifies the low threshold for percentage of total CPU memory used that maintains a previously generated alarm condition. If the memory usage falls below the low threshold within the polling interval, a clear alarm is generated.

`low_thresh` is measured as a percentage of total CPU memory used and is an integer from 0 and 100. A value of 0 disables the threshold.

**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 `high_thresh`. 
**Usage Guidelines**

CPU memory usage generate alerts or alarms based on the percentage of total CPU memory used during the polling interval.

Alerts or alarms are triggered for CPU memory usage session based on the following rules:

- **Enter condition:** Actual percentage of CPU memory usage is greater than or equal to the specified percentage of total CPU memory.

- **Clear condition:** Actual CPU memory usage is less than the specified clear percentage of total CPU memory usage.

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

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a threshold of 65 percent of total packet processing card CPU memory usage and a clear threshold of 35 percent:

`threshold cpu-memory-usage 65 clear 35`
**threshold cpu-orbs-crit**

Configures thresholds for generating critical-level alerts or alarms based on the percentage of CPU utilization by the Object Request Broker System (ORBS) software task.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

`configure`
Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold cpu-orbs-crit high_thresh [ clear low_thresh ]
[ default ] threshold cpu-orbs-crit
```

- **default**
  Restores this parameter to its default setting.

- **high_thresh**
  Default: 60
  Specifies the high threshold percent of CPU utilization by the ORB software task that must be exceeded as measured at the time of polling to generate a critical-level alert or alarm.
  `high_thresh` is measured in percentage of total CPU utilization and is an integer from 0 through 100. A value of 0 disables the threshold.

- **clear low_thresh**
  Default: 60
  Specifies the low threshold percent of CPU utilization by the ORB software task that maintains a previously generated alarm condition. If the percentage is measured as less than or equal to `low_thresh` at the time of polling, a clear alarm will be generated.
  `low_thresh` is measured in percentage of total CPU utilization and is an integer from 0 through 100. A value of 0 disables the threshold.
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 Specifies the low threshold.

Usage Guidelines

Object Request Broker (ORB) software task CPU utilization thresholds generate critical-level alerts or alarms based on the percentage of packet processing card CPU resources it is consuming at the time of polling. Critical-level alerts or alarms are triggered for CPU usage by the ORBs software task based on the following rules:

- **Enter condition:** Actual CPU usage percentage is greater than the high threshold.
- **Clear condition:** Actual CPU usage percentage is less than or equal to the low threshold.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Examples

The following command configures a critical-level alarm threshold of 35 percent of CPU utilization by the ORBS task and a clear threshold of 30 percent:

```
threshold cpu-orbs-crit 35 clear 30
```
threshold cpu-orbs-warn

Configures thresholds for generating warning-level alerts or alarms based on the percentage of CPU utilization by the Object Request Broker System (ORBS) software task.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

threshold cpu-orbs-warn high_thresh | clear low_thresh |

[ default ] threshold cpu-orbs-warn

default

Restores this parameter to its default setting.

*high_thresh*

Default: 50

Specifies the high threshold percent of CPU utilization by the ORBS software task that must be exceeded as measured at the time of polling to generate a warning-level alert or alarm.

*high_thresh* is measured in percentage of total CPU utilization and is an integer from 0 through 100. A value of 0 disables the threshold.

*clear low_thresh*

Default: 50

Specifies the low threshold percent of CPU utilization by the ORBS software task that maintains a previously generated alarm condition. If the percentage is measured as less than or equal to Specifies the low threshold at the time of polling, a clear alarm will be generated.

*low_thresh* is measured in percentage of total CPU utilization and is an integer from 0 through 100. A value of 0 disables the threshold.
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 specifies the low threshold.

**Usage Guidelines**

Object Request Broker (ORB) software task CPU utilization thresholds generate warning-level alerts or alarms based on the percentage of packet processing card CPU resources it is consuming at the time of polling.

Warning-level alerts or alarms are triggered for CPU usage by the ORBS software task based on the following rules:

- **Enter condition**: Actual CPU usage percentage is greater than the high threshold.
- **Clear condition**: Actual CPU usage percentage is less than or equal to the low threshold.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a warning-level alarm threshold of 25 percent of CPU utilization by the ORBS task and a clear threshold of 20 percent:

```
threshold cpu-orbs-warn 25 clear 20
```
threshold cpu-session-throughput

Configures alarm or alert thresholds for CPU session throughput within the system.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold cpu-session-throughput high_thresh [ clear low_thresh ]
```

**high_thresh**
Default: 0

Specifies the high threshold session throughput that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is measured in kilobytes per second (Kbps) and is an integer from 0 through 1000000000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0

Specifies the low threshold session thereofabout that maintains a previously generated alarm condition. If the throughput falls below specified value within the polling interval, a clear alarm will be generated.

`low_thresh` is measured in kilobytes per second (Kbps) and is an integer from 0 through 1000000000. A value of 0 disables the threshold.

**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

CPU session throughput thresholds generate alerts or alarms based on total throughput for all Session Manager tasks running on each packet processing card CPU during the polling interval. Although, a single threshold is configured for all CPUs, separate alerts or alarms can be generated for each CPU.

Alerts or alarms are triggered for CPU session throughput based on the following rules:

• **Enter condition:** Actual CPU session throughput is greater than or equal to the high threshold.
• **Clear condition:** Actual CPU session throughput is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

---

**Important**

This command is not supported on all platforms.

---

Examples

The following command configures a high threshold count of 900 Kbps session throughput and a low threshold of 500 KBps for a system using the Alarm thresholding model:

`threshold cpu-session-throughput 900 clear 500`
threshold cpu-utilization

Configures alarm or alert thresholds for CPU utilization within the system.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

```configure```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`threshold cpu-utilization high_thresh [ clear low_thresh ]`

- **high_thresh**
  
  Default: 85

  Specifies the high threshold CPU utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.

  `high_thresh` is an integer from 0 through 100.

- **clear low_thresh**
  
  Default: 85

  Specifies the low threshold CPU 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.

  `low_thresh` is an integer from 0 through 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**

CPU utilization thresholds generate alerts or alarms based on the utilization percentage of each packet processing card CPU during the specified polling interval. Although, a single threshold is configured for all CPUs, separate alerts or alarms can be generated for each CPU.
Alerts or alarms are triggered for CPU utilization based on the following rules:

- **Enter condition**: Average measured CPU utilization for the last 5 minutes
- **Clear condition**: Average measured CPU utilization for the last 5 minutes is less than the 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 to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

---

**Important**

This command is not supported on all platforms.

---

**Examples**

The following command configures a high threshold CPU utilization percentage of 90 for a system using the Alert thresholding model:

```
threshold cpu-utilization 90
```
threshold dcca-bad-answers

Configures alarm or alert thresholds for invalid or bad responses to the system from Diameter servers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold dcca-bad-answers high_thresh [ clear low_thresh ]
default threshold dcca-bad-answers
```

**default**
Disables the threshold for configured alarm and sets the `high_thresh` and `low_thresh` values to 0.

**high_thresh**
Default: 0
Specifies the high threshold number of invalid messages or responses that must be met or exceeded within the polling interval to generate an alert or alarm.
`high_thresh` is an integer from 0 through 1000000.

**clear low_thresh**
Default: 0
Specifies the low threshold number of invalid messages/responses that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.
`low_thresh` is an integer from 0 through 1000000.

---

**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

In the event that the system receives invalid message or response from Diameter server dcca-bad-answers is generated.

DCCA bad answer messages size threshold generates alerts or alarms based on the number of invalid response or messages received during the specified polling interval.

Alerts or alarms are triggered for DCCA bad answers based on the following rules:

- **Enter condition**: Actual number of DCCA bad answer messages is greater than or equal to the high threshold.
- **Clear condition**: Actual number of DCCA bad answer messages is less than the 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.

Examples

The following command configures a high threshold count of 250 DCCA bad answer messages and low threshold of 100 for a system using the Alarm thresholding model:

```
threshold dcca-bad-answers 250 clear 100
```
threshold dcca-protocol-error

Configures alarm or alert thresholds for Diameter Credit Control Application (DCCA) protocol errors from the Diameter server.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold dcca-protocol-error high_thresh | clear low_thresh |
default threshold dcca-protocol-error
```

default

Disables the threshold for configured alarm and sets the `high_thresh` and `low_thresh` values to 0.

`high_thresh`

Default: 0

Specifies the high threshold number of protocol error received from Diameter server that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is an integer from 0 through 1000000.

`clear low_thresh`

Default: 0

Specifies the low threshold number of protocol error received from Diameter server that maintains a previously generated alarm condition. If the number of errors falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` is an integer from 0 through 1000000.
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

In the event that the system receives the protocol errors from Diameter server, \texttt{dcca-protocol-error} is generated. DCCA protocol error threshold generates alerts or alarms based on the number of protocol error messages received from Diameter server during the specified polling interval.

Alerts or alarms are triggered for DCCA protocol error based on the following rules:

- **Enter condition**: Actual number of DCCA protocol error is greater than or equal to the high threshold.
- **Clear condition**: Actual number of DCCA protocol errors is less than the 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.

Examples

The following command configures a high threshold count of 250 protocol errors and low threshold of 100 for a system using the Alarm thresholding model:

\texttt{threshold dcca-protocol-error 250 clear 100}
**threshold dcca-rating-failed**

Configures Diameter Credit Control Application (DCCA) Rating Group (content-id) request reject, alarm or alert thresholds.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]\host_name\(config)\$

**Syntax Description**

`threshold dcca-rating-failed high_thresh | clear low_thresh`

default threshold dcca-rating-failed

default

Disables the threshold for configured alarm and sets the `high_thresh` and `low_thresh` values to 0.

`high_thresh`

Default: 0

Specifies the high threshold number of requests for a block of credits due to invalid Rating Group (content-id), rejected from the Diameter server that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is an integer from 0 through 1000000.

`clear low_thresh`

Default: 0

Specifies the low threshold number of requests for a block of credits due to invalid Rating Group (content-id), rejected from the Diameter server that maintains a previously generated alarm condition. If the number of errors falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` is an integer from 0 through 1000000.
**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**
In the event that the Diameter server rejects the system request for a block of credits due to invalid Rating Group, defined as content-id, **dcca-rating-failed** message is generated.

Rating Group failed threshold generates alerts or alarms based on the number of requests rejected from Diameter server during the specified polling interval.

Alerts or alarms are triggered for Rating Group failed based on the following rules:

- **Enter condition**: Actual number of DCCA Rating Group failed is greater than or equal to the high threshold.
- **Clear condition**: Actual number of DCCA Rating Group failed is less than the 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.

**Examples**
The following command configures a high threshold count of 250 requests rejected and low threshold of 100 for a system using the Alarm thresholding model:

```
threshold dcca-rating-failed 250 clear 100
```
**threshold dcca-unknown-rating-group**

Configures alarm or alert thresholds for the unknown Diameter Credit Control Application (DCCA) Rating Group (content-id) messages returned by Diameter servers.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold dcca-unknown-rating-group high_thresh [ clear low_thresh ]
default threshold dcca-unknown-rating-group

default
Disables the threshold for configured alarm and sets the high_thresh and low_thresh values to 0.

(high_thresh)
Default: 0
Specifies the high threshold number of unknown Rating Group (content-id) messages sent by the Diameter server that must be met or exceeded within the polling interval to generate an alert or alarm.

(high_thresh) is an integer from 0 through 1000000.

clear low_thresh
Default: 0
Specifies the low threshold number of unknown Rating Group (content-id) sent by Diameter server and received by system that maintains a previously generated alarm condition. If the number of errors falls beneath the low threshold within the polling interval, a clear alarm will be generated.

(low_thresh) is an integer from 0 through 1000000.
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**

In the event that the Diameter server sends invalid Rating Groups, **content-ids** to the system, **dcca-unk-rating-group** message is generated.

Unknown Rating Group threshold generates alerts or alarms based on the number of unknown Rating Groups received by the system from Diameter server during the specified polling interval. Alerts or alarms are triggered for unknown rating groups based on the following rules:

- **Enter condition**: Actual number of unknown rating groups is greater than or equal to the high threshold.
- **Clear condition**: Actual number of unknown rating groups is less than the 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.

**Examples**

The following command configures a high threshold count of 250 unknown rating groups and low threshold of 100 for a system using the Alarm thresholding model:

```
threshold dcca-unknown-rating-group 250 clear 100
```
threshold diameter diameter-retry-rate

Configures Diameter Retry Rate, alarm or alert thresholds based on the percentage of Diameter requests that were retried during the polling interval.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure
Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold diameter diameter-retry-rate high_thresh [ clear low_thresh ]
default threshold diameter diameter-retry-rate
```

**default**

Configures this command with the default threshold settings.
Default: 0—disabled

**high_thresh**

Specifies the high threshold. If, within the polling interval, the percentage of Diameter requests retried equals or exceeds `high_thresh` an alert or alarm is generated.
`high_thresh` is an integer from 0 through 100.
Default: 0

**clear low_thresh**

Specifies the low threshold. If, within the polling interval, the percentage of Diameter requests retried falls below `low_thresh`, a clear alarm is generated.
`low_thresh` is an integer from 0 through 100.
Default: 0
This value is applicable for the Alarm mode, and ignored for the Alert mode. In addition, if this value is not configured for the Alarm mode, the system assumes it is identical to the high threshold.

Usage Guidelines

Diameter Retry Rate threshold generates alerts or alarms based on the percentage of Diameter requests that were retried during the specified polling interval.

Alerts or alarms are triggered based on the following rules:

- **Enter condition**: Percentage of Diameter requests retried is greater than or equal to the high threshold.
- **Clear condition**: Percentage of Diameter requests retried is less than the 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.

Examples

The following command configures a high threshold of 75 percent, and a low threshold of 50 percent for a system using the Alarm thresholding model:

```
threshold diameter diameter-retry-rate 75 clear 50
```
threshold dns-learnt-ip-max-entries

Configures alarm or alert thresholds for the percentage of total DNS-learnt IP entries in relation to the ACS DNS Snooping feature.

Important
In 16.0 and later releases, this command has been deprecated and replaced by the `threshold dns-learnt-ipv4-max-entries` and `threshold dns-learnt-ipv6-max-entries` commands to configure alarm or alert thresholds for the percentage of total DNS-learnt IPv4 entries and total DNS-learnt IPv6 entries respectively.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
`configure`

Entering the above command sequence results in the following prompt:

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

Syntax Description
`threshold dns-learnt-ip-max-entries high_thresh | clear low_thresh | default` threshold dns-learnt-ip-max-entries

default

Configures this command with the default threshold setting.
Default: 90 percent. It is the same for both high and low thresholds.

`high_thresh`
Default: 90 percent

Specifies the high threshold for percentage of total DNS-learnt IP entries. When the percentage of total DNS-learnt IP entries meets or exceeds the high threshold at the end of the polling interval, an alert or alarm is generated.

When the percentage of total DNS-learnt IPv4 entries meets or exceeds the high threshold, the ECSTotalDNSLearntIPv4Threshold trap is generated.

When the percentage of total DNS-learnt IPv6 entries meets or exceeds the high threshold, the ECSTotalDNSLearntIPv6Threshold trap is generated.
high_thresh is an integer value from 0 through 100. When configured to 0 the threshold is disabled.

**clear low_thresh**

Default: 90 percent

Specifies the low threshold for percentage of total DNS-learnt IP entries. When the percentage of total DNS-learnt IP entries goes below the low threshold within the polling interval, a clear alarm is generated. When the percentage of total DNS-learnt IPv4 entries goes below the low threshold, the ECSTotalDNSLearntIPv4ThresholdClear trap is generated. When the percentage of total DNS-learnt IPv6 entries goes below the low threshold, the ECSTotalDNSLearntIPv6ThresholdClear trap is generated.

low_thresh is an integer value from 0 through 100. When configured to 0 the threshold is disabled.

**Usage Guidelines**

Use this command to configure thresholds for the percentage of total DNS-learnt IP entries in relation to the ACS DNS Snooping feature. Note that this threshold applies to both IPv4 and IPv6 DNS entries.

Alerts or alarms are triggered based on the following rules:

- **Enter condition**: Actual percentage of total DNS-learnt IP entries is greater than or equal to the specified percentage of total DNS-learnt IP entries.

- **Clear condition**: Actual of total DNS-learnt IP entries is less than the specified clear percentage of total DNS-learnt IP entries.

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

Refer to the **threshold poll** command to configure the polling interval, and the **threshold monitoring** command to enable thresholding for this value.

**Examples**

The following command configures a high threshold of 65 percent and a clear threshold of 35 percent for total DNS-learnt IP entries:

**threshold dns-learnt-ip-max-entries 65 clear 35**
**threshold dns-learnt-ipv4-max-entries**

Configures alarm or alert thresholds for the percentage of total DNS-learnt IPv4 entries in relation to the ACS DNS Snooping feature.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold dns-learnt-ipv4-max-entries high_thresh | clear low_thresh |
```

**high_thresh**

Specifies the high threshold for percentage of total DNS-learnt IPv4 entries. When the percentage of total DNS-learnt IPv4 entries meets or exceeds the high threshold at the end of the polling interval, an alert or alarm is generated.

When the percentage of total DNS-learnt IPv4 entries meets or exceeds the high threshold, the ECSTotalDNSLearntIPv4Threshold trap is generated.

*high_thresh* is an integer value from 0 through 100. When configured to 0 the threshold is disabled.
Default: 90 percent

**clear low_thresh**

Specifies the low threshold for percentage of total DNS-learnt IPv4 entries. When the percentage of total DNS-learnt IPv4 entries goes below the low threshold within the polling interval, a clear alarm is generated.

When the percentage of total DNS-learnt IPv4 entries goes below the low threshold, the ECSTotalDNSLearntIPv4ThresholdClear trap is generated.

*low_thresh* is an integer value from 0 through 100. When configured to 0 the threshold is disabled.
Default: 90 percent
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 configure thresholds for the percentage of total DNS-learnt IPv4 entries in relation to the ACS DNS Snooping feature.

Alerts or alarms are triggered based on the following rules:

- **Enter condition**: Actual percentage of total DNS-learnt IPv4 entries is greater than or equal to the specified percentage of total DNS-learnt IPv4 entries.
- **Clear condition**: Actual percentage of total DNS-learnt IPv4 entries is less than the specified clear percentage of total DNS-learnt IPv4 entries.

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

Refer to the `threshold poll` command to configure the polling interval, and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a high threshold of 60 percent and a clear threshold of 30 percent for total DNS-learnt IPv4 entries:

```
threshold dns-learnt-ipv4-max-entries 60 clear 30
```
threshold dns-learnt-ipv6-max-entries

Configures alarm or alert thresholds for the percentage of total DNS-learnt IPv6 entries in relation to the ACS DNS Snooping feature.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold dns-learnt-ipv6-max-entries high_thresh | clear low_thresh
```

**high_thresh**

Specifies the high threshold for percentage of total DNS-learnt IPv6 entries. When the percentage of total DNS-learnt IPv6 entries meets or exceeds the high threshold at the end of the polling interval, an alert or alarm is generated.

When the percentage of total DNS-learnt IPv6 entries meets or exceeds the high threshold, the ECSTotalDNSLearntIPv6Threshold trap is generated.

*high_thresh* is an integer value from 0 through 100. When configured to 0 the threshold is disabled.

Default: 90 percent

**clear low_thresh**

Specifies the low threshold for percentage of total DNS-learnt IPv6 entries. When the percentage of total DNS-learnt IPv6 entries goes below the low threshold within the polling interval, a clear alarm is generated.

When the percentage of total DNS-learnt IPv6 entries goes below the low threshold, the ECSTotalDNSLearntIPv6ThresholdClear trap is generated.

*low_thresh* is an integer value from 0 through 100. When configured to 0 the threshold is disabled.

Default: 90 percent
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 configure thresholds for the percentage of total DNS-learnt IPv6 entries in relation to the ACS DNS Snooping feature.

Alerts or alarms are triggered based on the following rules:

- **Enter condition**: Actual percentage of total DNS-learnt IPv6 entries is greater than or equal to the specified percentage of total DNS-learnt IPv6 entries.

- **Clear condition**: Actual percentage of total DNS-learnt IPv6 entries is less than the specified clear percentage of total DNS-learnt IPv6 entries.

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

Refer to the `threshold poll` command to configure the polling interval, and the `threshold monitoring` command to enable thresholding for this value.

Examples

The following command configures a high threshold of 75 percent and a clear threshold of 45 percent for total DNS-learnt IPv6 entries:

```
threshold dns-learnt-ipv6-max-entries 75 clear 45
```
threshold dns-lookup-failure

Configures alarm or alert thresholds based on the percentage of total DNS lookup failures.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

threshold dns-lookup-failure

**default**
Configures this command with the default threshold setting.
Default: 90 percent. It is the same for both high and low thresholds.

**high_thresh**
Default: 90 percent
Specifies the high threshold for percentage of total DNS lookup failures. When the percentage of total failures meets or exceeds the high threshold at the end of the polling interval, an alert or alarm is generated.
*high_thresh* is an integer value from 0 through 100. When configured to 0 the threshold is disabled.

**clear low_thresh**
Default: 90 percent
Specifies the low threshold for percentage of total DNS lookup failures. When the percentage of total failures goes below the low threshold within the polling interval, a clear alarm is generated.
*low_thresh* is an integer value from 0 through 100. When configured to 0 the threshold is disabled.

---

**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 configure thresholds for the percentage of total DNS lookup failures. Note that this threshold applies to both IPv4 and IPv6 DNS entries.

Alerts or alarms are triggered based on the following rules:

- **Enter condition**: Actual percentage of total DNS lookup failures is greater than or equal to the specified percentage of total DNS lookup failures.

- **Clear condition**: Actual of total DNS lookup failures is less than the specified clear percentage of total DNS lookup failures.

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

Refer to the `threshold poll` command to configure the polling interval, and the `threshold monitoring` command to enable thresholding for this value.

Examples

The following command configures a high threshold of 65 percent and a clear threshold of 35 percent for total DNS lookup failures:

```
threshold dns-lookup-failure 65 clear 35
```
threshold edr-file-space

Configures alarm or alert thresholds for monitoring the percentage of total file space allocated for Event Data Records (EDRs) used during the polling interval.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ default ] threshold edr-file-space high_thresh [ clear low_thresh ]
```

- **high_thresh**
  Default: 90
  Specifies the high threshold for percentage of total allocated EDR file space used that must be met or exceeded at the end of the polling interval to generate an alert or alarm.
  `high_thresh` is measured in percentage of total allocated EDR file space used and is an integer from 0 through 100. A value of 0 disables the threshold.

- **clear low_thresh**
  Default: 0
  Specifies the low threshold for percentage of total allocated EDR file space used that maintains a previously generated alarm condition. If the space usage falls below the low threshold within the polling interval, a clear alarm is generated.
  `low_thresh` is measured in percentage of total allocated EDR file space used and is an integer from 0 through 100. A value of 0 disables the threshold.

**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**

EDR file space usage generate alerts or alarms based on the percentage of total allocated EDR file space used during the polling interval.

Alerts or alarms are triggered for EDR file space usage session based on the following rules:

- **Enter condition**: Actual percentage of allocated EDR file space usage is greater than or equal to the specified percentage of total EDR file space.
- **Clear condition**: Actual EDR file space used is less than the specified clear percentage of total allocated EDR file space usage.

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

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a high threshold of 65 percent and a clear threshold of 35 percent for total allocated EDR file space usage:

```
threshold edr-file-space 65 clear 35
```
**threshold edr-udr-dropped flow control**

Configures alarm or alert thresholds to monitor the total number of Event Data Records (EDRs) and Usage Data Records (UDRs) discarded due to flow control.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`threshold edr-udr-dropped-flow-control high_thresh [ clear low_thresh ]`

default threshold edr-udr-dropped-flow-control

default

Configures this command with the default threshold settings.

Default: High threshold: 90; Low threshold: 10

`high_thresh`

Specifies the high threshold for total number of EDRs + UDRs dropped due to flow control, which must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` must be an integer from 0 through 100000.

A value of 0 disables the threshold.

Default: 90

`clear low_thresh`

Specifies the low threshold for total number of EDRs + UDRs dropped that maintains a previously generated alarm condition. If the total number of EDRs + UDRs dropped falls below `low_thresh` within the polling interval, a clear alarm is generated.

`low_thresh` must be an integer from 0 through 100000 that must be lower than `high_thresh`.

A value of 0 disables the threshold.

Default: 10
Usage Guidelines

Use this command to configure thresholds to monitor the total number of EDRs + UDRs discarded due to flow control. Alerts or alarms are generated based on the total number of EDRs + UDRs dropped during polling interval.

Alerts or alarms are triggered for EDR file space usage session based on the following rules:

- **Enter condition**: Actual number of EDRs + UDRs dropped greater than or equal to the specified number of EDRs + UDRs dropped.
- **Clear condition**: Actual number of EDR + UDRs dropped is less than the specified clear number of EDRs + UDRs dropped.

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

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Examples

The following command configures a high threshold of 90 and a clear threshold of 45 to monitor EDRs + UDRs dropped due to flow control:

```
threshold edr-udr-dropped-flow-control 90 clear 45
```
threshold epdg-current-sessions

Configures alarm or alert thresholds for the number of subscribers currently in Evolved Packet Date Gateway (ePDG) sessions.

**Product**
ePDG

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

> [local] host_name(config)#

**Syntax Description**

- `threshold epdg-current-sessions`
- `default threshold epdg-current-sessions`

**default**
Disables the threshold for configured alarm and sets the `high_thresh` and `low_thresh` values to 0.

**high_thresh**
Default: 0
Specifies the high threshold number of the total number of ePDG subscriber sessions that must be met or exceeded within the polling interval to generate an alert or alarm.

- `high_thresh` is an integer from 0 through 1000000.

**clear low_thresh**
Default: 0
Specifies the low threshold number of the total number of ePDG subscriber sessions that maintains a previously generated alarm condition. If the number of errors falls beneath the low threshold within the polling interval, a clear alarm will be generated.

- `low_thresh` is an integer from 0 through 1000000.
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.

**Important**

**Usage Guidelines**

Sets the upper and power thresholds for the total number of ePDG subscriber sessions that will generate and clear alerts or alarms.

Alerts or alarms are triggered based on the following rules:

- **Enter condition**: Actual number of ePDG subscriber sessions is greater than or equal to the high threshold.

- **Clear condition**: Actual number of ePDG subscriber sessions is less than the 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.

**Examples**

The following command configures sets the upper threshold of ePDG subscriber sessions at 100000 and the lower threshold at 90000:

```
threshold epdg-current-sessions 100000 clear 90000
```
threshold fng-current-active-sessions

Configures alarm or alert thresholds for the number of subscribers currently active Femto Network Gateway (FNG) sessions.

**Product**
FNG

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
| default | threshold fng-current-active-sessions |
```

**default**
Disables the threshold for configured alarm and sets the `high_thresh` and `low_thresh` values to 0.

**high_thresh**
Default: 0
Specifies the high threshold number of the total number of active FNG subscriber sessions that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is an integer from 0 through 1000000.

**clear low_thresh**
Default: 0
Specifies the low threshold number of the total number of active FNG subscriber sessions that maintains a previously generated alarm condition. If the number of errors falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` is an integer from 0 through 1000000.

**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

Sets the upper and power thresholds for the total number of active FNG subscriber sessions that will generate and clear alerts or alarms.

Alerts or alarms are triggered based on the following rules:

- **Enter condition**: Actual number of active FNG subscriber sessions is greater than or equal to the high threshold.
- **Clear condition**: Actual number of active FNG subscriber sessions is less than the 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.

Examples

The following command configures sets the upper threshold of active FNG subscriber sessions at 100000 and the lower threshold at 90000:

```
threshold fng-current-active-sessions 100000 clear 90000
```
threshold fng-current-sessions

Configures alarm or alert thresholds for the number of subscribers currently in Femto Network Gateway (FNG) sessions, including inactive sessions.

**Product**

FNG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

`threshold fng-current-sessions`

`default threshold fng-current-sessions`

**default**

Configures this command with the default threshold settings.

Default: High threshold: 90; Low threshold: 10

**high_thresh**

Default: 0

Specifies the high threshold number of the total number of FNG subscriber sessions that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 1000000.

**clear low_thresh**

Default: 0

Specifies the low threshold number of the total number of FNG subscriber sessions that maintains a previously generated alarm condition. If the number of errors falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 1000000.
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**

Sets the upper and power thresholds for the total number of FNG subscriber sessions that will generate and clear alerts or alarms.

Alerts or alarms are triggered based on the following rules:

- **Enter condition**: Actual number of FNG subscriber sessions is greater than or equal to the high threshold.
- **Clear condition**: Actual number of FNG subscriber sessions is less than the 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.

**Examples**

The following command configures sets the upper threshold of FNG subscriber sessions at 200000 and the lower threshold at 190000:

```
threshold fng-current-sessions 200000 clear 190000
```
**threshold fw-deny-rule**

Configures alarm or alert thresholds for the Stateful Firewall Deny Rule.

**Product**

PSF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`threshold fw-deny-rule high_thresh [ clear low_thresh ]`

`default threshold fw-deny-rule`

`default`

Configures this command with the default threshold settings.

Default: 0—disabled

`high_thresh`

Specifies the Stateful Firewall Deny-Rule threshold value, which if met or exceeded generates an alert or alarm.

`high_thresh` must be an integer from 0 through 1000000.

Default: 0

`clear low_thresh`

Specifies the Stateful Firewall Deny-Rule alarm clear threshold value. If, in the same polling interval, the threshold falls below `low_thresh` a clear alarm is generated.

`low_thresh` must be an integer from 0 through 1000000.

Default: 0
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 the number of Deny-Rule instances exceeds a given value, an alarm or alert is raised; it is cleared when the number of Deny-Rule instances falls below a value within the polling interval.

Refer to the `threshold poll` command to configure the polling interval, and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a Stateful Firewall Deny Rule high threshold of 1000 and a low threshold of 900 for a system using the Alarm Thresholding model:

```
threshold fw-deny-rule 1000 clear 900
```
threshold fw-dos-attack

Configures alarm or alert thresholds for Stateful Firewall Denial-of-Service (DoS) attacks.

**Product**  PSF

**Privilege**  Security Administrator, Administrator

**Command Modes**  Exec > Global Configuration

    configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

- `threshold fw-dos-attack high_thresh [ clear low_thresh ]`
- `default threshold fw-dos-attack`

**default**

Configures this command with the default threshold settings.

Default: 0—disabled

**high_thresh**

Specifies the Stateful Firewall DoS attacks threshold value, which if met or exceeded generates an alert or alarm.

`high_thresh` must be an integer from 0 through 1000000.

Default: 0

**clear low_thresh**

Specifies the Stateful Firewall DoS attacks clear threshold value. If, in the same polling interval, the threshold falls below `low_thresh` a clear alarm is generated.

`low_thresh` must be 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 low threshold.

Usage Guidelines
When the number of DoS attacks exceed a given value, a threshold is raised and it is cleared when the number of DoS attacks fall below a value within the polling interval.

Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

Examples
The following command configures a Stateful Firewall DoS attacks high threshold of 1000 and a low threshold of 100 for a system using the Alarm Thresholding model:

threshold fw-dos-attack 1000 clear 100
**threshold fw-drop-packet**

Configures alarm or alert thresholds for Stateful Firewall dropped packets.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

**Syntax Description**

```
threshold fw-drop-packet high_thresh [ clear low_thresh ]
default threshold fw-drop-packet
```

default

Configures this command with the default threshold settings.
Default: 0—disabled

**high_thresh**

Specifies the Stateful Firewall dropped packets threshold value, which if met or exceeded generates an alert or alarm.

`high_thresh` must be an integer from 0 through 1000000.
Default: 0

**clear low_thresh**

Specifies the Stateful Firewall dropped packets clear threshold value. If, in the same polling interval, the threshold falls below `low_thresh` a clear alarm is generated.

`low_thresh` must be an integer from 0 through 1000000.
Default: 0
threshold fw-drop-packet

**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 the number of dropped packets exceed a given value, a threshold is raised and it is cleared when the number of dropped packets fall below a value within the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**  The following command configures a Stateful Firewall dropped packets high threshold of 1000 and a low threshold of 900 for a system using the Alarm thresholding model:

```
threshold fw-drop-packet 1000 clear 900
```
threshold fw-no-rule

Configures alarm or alert thresholds for Stateful Firewall no rule occurrences.

Product
PSF

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local]host_name(config)#

Syntax Description
threshold fw-no-rule high_thresh [ clear low_thresh ]
default threshold fw-no-rule

default
Configures this command with the default threshold settings.
Default: 0—disabled

high_thresh
Specifies the Stateful Firewall no rules threshold value, which if met or exceeded generates an alert or alarm.
high_thresh must be an integer from 0 through 1000000.
Default: 0

clear low_thresh
Specifies the Stateful Firewall no rules clear threshold value. If, in the same polling interval, the threshold falls below low_thresh a clear alarm is generated.
low_thresh must be 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 low threshold.
Usage Guidelines
When the number of no rule occurrences exceeds a given value, a threshold is raised and it is cleared when the number of no rules fall below a value within the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Examples
The following command configures a Stateful Firewall no rule high threshold of 1000 and a low threshold of 900 for a system using the Alarm Thresholding model:
```
threshold fw-no-rule 1000 clear 900
```
threshold license remaining-sessions

Configures alarm or alert thresholds for the percentage of session license utilization by the system.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no ] threshold license remaining-sessions low_thresh clear high_thresh
```

**no low_thresh**
Disables threshold session license utilization alerts or alarms.

```
remaining-sessions low_thresh
```
Default: 10

Specifies the low threshold session license utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.

`low_thresh` is an integer from 0 through 100.

**clear high_thresh**
Default: 10

Specifies the high threshold session license 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` is an integer from 0 through 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 Specifies the low threshold.
Usage Guidelines

Session license utilization thresholds generate alerts or alarms based on the utilization percentage of all session capacity licenses during the specified polling interval.

The system uses session capacity license to dictate the maximum number of simultaneous sessions that can be supported. There are multiple session types that require licenses. Although, a single threshold is configured for all session types, alerts or alarms can be generated for each type.

Alerts or alarms are triggered for session license utilization based on the following rules:

- **Enter condition**: Actual session license utilization percentage per session type is greater than or equal to the low threshold.
- **Clear condition**: Actual session license utilization percentage per session type is greater than the 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.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Examples

The following command configures a session license low threshold percentage of 10 and a high threshold of 35 for a system using the Alarm thresholding model:

```
threshold license remaining-sessions 10 clear 35
```
threshold mgmt-cpu-memory-usage

Configures alarm or alert thresholds for the percentage of CPU memory usage on management cards.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
`threshold mgmt-cpu-memory-usage high_thresh | clear low_thresh`

- **high_thresh**
  
  Default: 0
  
  Specifies the high threshold percent of CPU memory usage that must be met or exceeded within the polling interval to generate an alert or alarm.

  `high_thresh` is measured in percentage of total memory used and can be configured to an integer from 0 through 100. A value of 0 disables the threshold.

- **clear low_thresh**
  
  Specifies the low threshold percent of CPU memory usage that maintains a previously generated alarm condition. If the percentage falls beneath the low threshold within the polling interval, a clear alarm will be generated.

  `low_thresh` is measured in percentage of total memory used and can be configured to an integer from 0 through 100. A value of 0 disables the threshold.

**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

CPU memory usage thresholds generate alerts or alarms based on memory usage for the SPC, SMC, or MIO CPU during the polling interval. A single threshold enables CPU monitoring for both the active and standby SPCs, SMCs, or MIOs allowing for alerts or alarms to be generated for each CPU.

Alerts or alarms are triggered for SPC, SMC, or MIO CPU memory usage based on the following rules:

- **Enter condition:** Actual CPU memory usage is greater than or equal to the high threshold
- **Clear condition:** Actual CPU memory usage is less than the 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 to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

**Important**

This command is not supported on all platforms.

Examples

The following command configures a threshold of 65 percent of total SPC, SMC, or MIO CPU memory usage and a clear threshold of 35 percent:

`threshold mgmt-cpu-memory-usage 65 clear 35`
threshold mgmt-cpu-utilization

Configures alarm or alert thresholds for the percentage of CPU utilization on management cards.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`threshold mgmt-cpu-utilization high_thresh [ clear low_thresh ]`

- **high_thres**
  
  Default: 0
  
  Specifies the high threshold CPU utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.

  `high_thres` is an integer from 0 through 100.

- **clear low_thres**

  Specifies the low threshold CPU utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls beneath the low threshold within the polling interval, a clear alarm will be generated.

  `low_thres` is an integer from 0 through 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**

CPU utilization thresholds generate alerts or alarms based on the utilization percentage of each SPC, SMC, or MIO CPU during the specified polling interval. Although, a single threshold is configured for both SPC, SMC, or MIO CPUs, separate alerts or alarms can be generated for each CPU.

Alerts or alarms are triggered for SPC, SMC, or MIO CPU utilization based on the following rules:
• **Enter condition**: Average measured CPU utilization for the last 5 minutes is greater than or equal to the high threshold.

• **Clear condition**: Average measured CPU utilization for the last 5 minutes is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

---

**Important**

This command is not supported on all platforms.

---

**Examples**

The following command configures a high threshold SPC, SMC, or MIO CPU utilization percentage of 90 for a system using the Alert thresholding model:

```
threshold mgmt-cpu-utilization 90
```
threshold mme-attach-failure

Configures alarm or alert thresholds for the total number of MME Attach Failure messages across all the MME services in the system.

Product
MME

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description
threshold total-mme-attach-failure high_thresh [ clear low_thresh ]

high_thresh
Default: 0 (Disabled)
Specifies the high threshold number of total MME Attach Failure messages across all services on a system that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh can be configured to an integer from 0 through 100000. A value of 0 disables the threshold.

clear low_thresh
Default: 0 (Disabled)
Specifies the low threshold number of total MME Attach Failure messages across all services on a system that maintains a previously generated alarm condition. If the number of MME Attach Failure messages across all the services in a system, falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 100000. A value of 0 disables the threshold.

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 monitor and set alarms or alerts when the total number of MME Attach Failure message across all the MME services in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for the total number of MME Attach Failure message based on the following rules:

- **Enter condition:** Actual total number of MME Attach Failure messages is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of MME Attach Failure messages is less than the 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 mme-attach-failure` command to configure the polling interval and the `threshold monitoring mme-service` command to enable thresholding for this value.

**Examples**

The following command configures the limit of MME Attach Failure high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold mme-attach-failure 10000
```
threshold mme-auth-failure

Configures alarm or alert thresholds for the total number of MME Auth Failure messages across all the MME services.

**Product**

MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold total-mme-auth-failure high_thresh | clear low_thresh
```

**high_thresh**

Default: 0 (Disabled)

Specifies the high threshold number of total MME Auth Failure messages across all MMM services on a system that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* can be configured to an integer from 0 through 100000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0 (Disabled)

Specifies the low threshold number of total MME Auth Failure messages across all services on a system that maintains a previously generated alarm condition. If the number of MME Attach Failure messages across all the services in a system, falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 100000. A value of 0 disables the threshold.

**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 monitor and set alarms or alerts when the total number of MME Auth Failure message across all the MME services in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for the total number of MME Auth Failure message based on the following rules:

- **Enter condition:** Actual total number of MME Auth Failure messages is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of MME Auth Failure messages is less than the 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 mme-auth-failure` command to configure the polling interval and the `threshold monitoring mme-service` command to enable thresholding for this value.

Examples

The following command configures a total MME Auth Failure high threshold count of `10000` for a system using the Alert thresholding model:

```
threshold mme-auth-failure 10000
```
threshold model

Configures the thresholding model, alarm or alert, for the system to use.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] *host_name*(config)#

**Syntax Description**

threshold model { alarm | alert }

- **alarm**
  Selects the alarm thresholding model as described in the *Usage* section for this command.

- **alert**
  Selects the alert thresholding model as described in the *Usage* section for this command.

**Usage Guidelines**

The system supports the following thresholding models:

- **Alert**: A value is monitored and an alert condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated and/or sent at the end of the polling interval.

In the example shown in the figure below, this model generates alerts during period 2, 3, and 5 at the point where the count exceeded the high threshold.

- **Alarm**: Both high and low threshold are defined for a value. An alarm condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated and/or sent at the end of the polling interval.

The alarm is cleared at the end of the first interval where the measured value is below the low threshold.
In the example shown in the figure below, this model generates an alarm during period 2 when the count exceeds the high threshold. A second alarm is generated in period 6 when the count falls beneath low threshold. The second alarm indicates a "clear" condition.

**Figure 1: Thresholding Model Example**

For certain values the alert or alarm serves to warn of low quantities (such as, memory, session licenses, etc.). In these cases, the low threshold is the condition that must be met or exceeded within the polling interval to generate the alert or alarm. When the high threshold is exceeded during an interval, the low quantity condition is cleared.

Refer to the **threshold monitoring** command for additional information on thresholding.

**Examples**

The following command configures the system to support the Alarm thresholding model:

```
threshold model alarm
```
threshold monitoring

Enables or disables threshold monitoring for the selected value.

**Product**

All

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

**Syntax Description**

| no | default | threshold monitoring { aaa-acct-archive-queue | aaa-acct-archive-size | aaa-acct-failure |
|---|---|---|
|    |    |    | aaa-auth-failure | aaa-retry-rate | aaamgr-request-queue | asngw | call-setup | content-filtering |
|    |    |    | cpu-resource | cpu-session-throughput | diameter | ecs | epdg-service | fa-service | firewall | fw-and-nat |
|    |    |    | ha-service | hnbgw-service | hnbgw-service | hsgw-service | ipsec | license | lma-service | mme-service |
|    |    |    | npu-resource | packets-filtered-dropped | packets-forwarded-to-cpu | pdg-service | pdif-service |
|    |    |    | pdsn-service | pgw-service | phsgw | phspc | route-service | saegw-service | sess-flow-count |
|    |    |    | subscriber | system | tpo |

**no**

Disables threshold monitoring for the specified value.

**default**

Sets or restores the default value assigned to the specified parameter.

**aaa-acct-archive-queue**

Enables threshold monitoring for the AAA accounting archive message queue size.

Refer to the `threshold aaa-acct-archive-queue-size` command for additional information on these values.

**aaa-acct-archive-size**

Enables threshold monitoring for the size of the AAA accounting record archive.

**aaa-acct-failure**

Enables threshold monitoring for AAA accounting failures and AAA accounting failure rate values.
Refer to the `threshold aaa-acct-failure` and `threshold aaa-acct-failure-rate` commands for additional information on these values.

**aaa-auth-failure**
Enables threshold monitoring for AAA authentication failures and AAA authentication failure rate values. Refer to the `threshold aaa-auth-failure` and `threshold aaa-auth-failure-rate` commands for additional information on these values.

**aaa-retry-rate**
Enables threshold monitoring for the AAA retry rate value. Refer to the `threshold aaa-retry-rate` command for additional information on this value.

**aaamgr-request-queue**
Enables threshold monitoring for AAA Manager Requests for each AAA manager process. Refer to the `threshold aaamgr-request-queue` command for additional information on these values.

**asngw**
Enables the threshold monitoring for ASN-GW services.

**call-setup**
Enables threshold monitoring for the call setup, call setup failures, and no-resource rejected call values. Refer to the `threshold call-setup`, `threshold call-setup-failure`, `threshold ppp-setup-fail-rate`, `threshold rp-setup-fail-rate`, and `threshold call-reject-no-resource` commands for additional information on these values.

**cpu-resource**

**cpu-session-throughput**
Enables threshold monitoring for the CPU session throughput value. Refer to the `threshold cpu-session-throughput` command for additional information on this value.

**content-filtering**
Enables threshold monitoring for the Content Filtering in-line service.

**diameter**
Enables threshold monitoring for Diameter.
ecs
Enables threshold monitoring for the Active Charging Service (ACS)/Enhanced Charging Service (ECS).

epdg-service
Enables threshold monitoring for Evolved Packet Data Gateway (ePDG) service.
Refer to the threshold epdg-current-sessions command for additional information on this value.

fa-service
Enables threshold monitoring for Registration Reply errors for each FA service.
Refer to the threshold reg-reply-error FA Service Configuration Mode command for additional information on this value.

firewall
Enables threshold monitoring for the Stateful Firewall in-line service.
Default: Disabled
Refer to the threshold fw-deny-rule, threshold fw-dos-attack, threshold fw-drop-packet, and threshold fw-no-rule commands for additional information on this value.

Important
Stateful Firewall thresholds can only be enabled if the Stateful Firewall license is present.

fw-and-nat
Enables threshold monitoring for the Firewall and NAT in-line service.
Default: Disabled
Refer to the threshold fw-deny-rule, threshold fw-dos-attack, threshold fw-drop-packet, threshold fw-no-rule, threshold nat-pkt-drop, and threshold nat-port-chunks-usage commands for additional information on this value.

ha-service
Enables threshold monitoring for Registration Reply errors, re-registration reply errors, deregistration reply errors, and average calls setup per second for each HA service and average calls setup per second at the context level.
Refer to the threshold init-rrq-rcvd-rate, threshold reg-reply-error, threshold rereg-reply-error, and threshold dereg-reply-error HA Service Configuration Mode commands and the threshold ha-service init-rrq-rcvd-rate Context Configuration mode command for additional information on this value.

henbgw-service
Enables threshold monitoring for HeNB-GW service.
This keyword is required to activate the threshold alarm/alert for HeNB-GW service to use `threshold henb-gw-paging-messages`, `threshold total-henbgw-henb-sessions`, and `threshold total-henbgw-ue-sessions` commands for threshold values.

**Important**

This keyword is required to activate the threshold alarm/alert for HeNB-GW service to use `threshold total-henbgw-hnb-sessions`, `threshold total-henbgw-iu-sessions`, and `threshold total-henbgw-ue-sessions` command for threshold values.

**hnbgw-service**

Enables threshold monitoring for HNBGW sessions including Iu-CS and Iu-PS sessions for HNBGW services on a system at the system level.

**Important**

This keyword is required to activate the threshold alarm/alert for HNBGW service to use `threshold total-henbgw-hnb-sessions`, `threshold total-henbgw-iu-sessions`, and `threshold total-henbgw-ue-sessions` command for threshold values.

**hsgw-service**

Enables threshold monitoring for HSGW services.
Refer to the threshold total-hsgw-sessions for more information on HSGW thresholds.

**ipsec**

Enables monitoring of IPSec thresholds.
Refer to the `HA-Service Configuration Mode` chapter of the *Command Line Interface Reference* for information on the IPSec thresholds.

**license**

Enables threshold monitoring for the session license value.
Refer to the `threshold license` command for additional information on this value.

**lma-service**

Enables threshold monitoring for LMA services.
Refer to the `threshold total-lma-sessions` command for more information on LMA thresholds.

**mme-service**

Default: Disabled.
Enables threshold monitoring for the MME services.
Refer to the `threshold total-mme-sessions` command for additional information on this value.

**npu-resource**

Enables threshold monitoring for the Network Processor Unit (NPU) resources, including NPU utilization.
Refer to the `threshold npu-utilization` command for additional information on this value.
packets-filtered-dropped
Enables threshold monitoring for the filtered/dropped packet value.
Refer to the threshold packets-filtered-dropped command for additional information on this value.

packets-forwarded-to-cpu
Enables threshold monitoring for the forwarded packet value.
Refer to the threshold packets-forwarded-to-cpu command for additional information on this value.

pdg-service
Enables threshold monitoring for PDG service.
Threshold monitoring for PDG service is disabled by default.

pdif-service
Enables threshold monitoring for PDIF service.

pdsn-service
Enables threshold monitoring for average calls setup per second for contexts and for PDSN services, A11 Request.
Refer to the threshold packets-forwarded-to-cpu command for additional information on this value.

pgw-service
Enables threshold monitoring for P-GW services.
Refer to the threshold total-pgw-sessions for more information on P-GW thresholds.

route-service
Enables threshold monitoring for BGP/VRF route services.
Refer to the ip maximum-routes command in Context configuration mode and threshold route-service bgp-routes in this mode for more information on route thresholds.

saegw-service
Enables threshold monitoring for SAEGW services.
Refer to the threshold total-saegw-sessions for more information on SAEGW thresholds.

sess-flow-count
Enables threshold monitoring for Session Flow Count.
Default: 90%
Refer to the threshold sess-flow-count for more information on Session Flow Count Thresholds

sgw-service
Enables threshold monitoring for S-GW services.
Refer to the threshold total-sgw-sessions for more information on S-GW thresholds.
subscriber
Enables threshold monitoring for the subscriber and session values.
Refer to the threshold subscriber active, threshold subscriber total, threshold total-ggsn-sessions, threshold total-gprs-sessions, threshold total-gprs-pdp-sessions, threshold total-ha-sessions, threshold total-lns-sessions, threshold total-pdsn-sessions, threshold total-pgw-sessions, threshold total-sgw-sessions, threshold total-saegw-sessions, threshold total-sgsn-sessions, threshold total-sgsn-pdp-sessions, threshold per-service-ggsn-sessions, threshold per-service-ha-sessions, threshold per-service-lns-sessions, threshold per-service-pdsn-sessions commands for additional information on these values.

system
Enables system (chassis) thresholds monitoring.

tpo

Important
The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

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 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 CLI. The following table indicates the reporting mechanisms supported by each of the above models.

**Table 5: ASR 5000 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>
</tbody>
</table>
### Table 6: ASR 5500 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>Alarm</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

In addition to the values that can be enabled by this command, the system supports the enabling of threshold monitoring for IP pool address availability (refer to the `ip pool` and threshold commands in this reference) and port utilization (refer to the threshold commands in this chapter).

#### Examples

The following command enables thresholding for subscriber totals:

```
threshold monitoring subscriber
```
threshold nat-pkt-drop

Configures alarm or alert thresholds for the percentage of Network Address Translation (NAT) packet drops.

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold nat-pkt-drop high_thresh [ clear low_thresh ]
default threshold nat-pkt-drop
```

**default**

Configures this command with the default threshold settings.

Default: 0—disabled

**high_thresh**

Specifies the high NAT packet drop percentage threshold that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` must be an integer from 0 through 100. A value of 0 disables the threshold.

Default: 0

**clear low_thresh**

Specifies the low NAT packet drop percentage threshold that must be met within the polling interval for a clear alarm to be generated.

`low_thresh` must be an integer from 0 through 100. A value of 0 disables the threshold. If not set, the `high_thresh` will be the high and low threshold setting.

Default: 0

**Usage Guidelines**

Use this command to configure the NAT packet drop threshold settings.
Examples

The following command sets the NAT packet drop threshold settings to a high of 55% and a low of 15%:

```
threshold nat-pkt-drop 55 clear 15
```
threshold nat-port-chunks-usage

Configures alarm or alert thresholds for the percentage of Network Address Translation (NAT) port chunk utilization.

---

**Important**

This command is only available in 8.3 and later releases.

---

**Product**

NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

[local] host_name(config) #

**Syntax Description**

`threshold nat-port-chunks-usage high_thresh [ clear low_thresh ]`

default threshold nat-port-chunks-usage

default

Configures this command with the default threshold settings.
Default: 0—disabled

`high_thresh`

Specifies the high NAT-port-chunks-usage percentage threshold that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` must be an integer from 0 through 100. A value of 0 disables the threshold.
Default: 0

`clear low_thresh`

Specifies the low nat-port-chunks-usage percentage threshold that must be met within the polling interval for a clear alarm to be generated.

`low_thresh` must be an integer from 0 through 100. A value of 0 disables the threshold. If not set, the `high_thresh` will be the high and low threshold setting.
Default: 0

**Usage Guidelines**
Use this command to configure the NAT port chunk utilization threshold settings.

**Examples**
The following command sets the NAT port chunk utilization threshold settings to a high of 75% and a low of 15%:

```
threshold nat-port-chunks-usage 75 clear 15
```
**threshold npu-utilization**

Configures alarm or alert thresholds for the percentage of network processing unit (NPU) utilization.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold npu-utilization high_thresh clear low_thresh
```

default

Configures this command with the default threshold settings.
Default: 0—disabled

**high_thresh**

Specifies the high percentage threshold for NPU utilization that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* must be an integer from 0 through 100. A value of 0 disables the threshold.
Default: 0

**clear low_thresh**

Specifies the low percentage threshold for NPU utilization that must be met within the polling interval for a clear alarm to be generated.

*low_thresh* must be an integer from 0 through 100. A value of 0 disables the threshold. If not set, the *high_thresh* will be the high and low threshold setting.
Default: 0

**Usage Guidelines**

Use this command to configure the NPU utilization threshold settings.
**Examples**

The following command sets the NPU utilization threshold settings to a high of 90% and a low of 75%:

```
threshold npu-utilization 90 clear 75
```
threshold packets-filtered-dropped

Configures alarm or alert thresholds for filtered or dropped packets within the system.

**Product**
- PDSN
- GGSN
- HA
- P-GW
- SAEGW
- SGSN
- ASN-GW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration
- configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold packets-filtered-dropped high_thresh [ clear low_thresh ]
```

**high_thresh**
Default: 0
Specifies the high threshold number of filtered/dropped packets experienced by the system resulting from access control list (ACL) rules that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 1000000000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0
Specifies the low threshold number of filtered/dropped packets experienced by the system resulting from ACL rules that maintains a previously generated alarm condition. If the number of packets falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 1000000000. A value of 0 disables the threshold.
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**
Filtered/dropped packet thresholds generate alerts or alarms based on the total number of packets that were filtered or dropped by the system as a result of ACL rules during the specified polling interval.

Alerts or alarms are triggered for filtered/dropped packets based on the following rules:

- **Enter condition:** Actual number of filtered/dropped packets is greater than or equal to the high threshold.
- **Clear condition:** Actual number of filtered/dropped packets is less than the 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 to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value. In addition, refer to information on ACLs in this reference.

**Examples**
The following command configures a filtered/dropped packet high threshold count of **150000** for a system using the Alert thresholding model:

```
threshold packets-filtered-dropped 150000
```
threshold packets-forwarded-to-cpu

Configures alarm or alert thresholds for packets forwarded to active system CPUs in the system.

**Product**
- PDSN
- GGSN
- HA
- P-GW
- SAEGW
- SGSN
- ASN-GW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration
  - `configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold packets-forwarded-to-cpu high_thresh [ clear low_thresh ]
```

**high_thresh**
- Default: 0
- Specifies the high threshold number of packets forwarded to CPUs that must be met or exceeded within the polling interval to generate an alert or alarm.
- `high_thresh` is an integer from 0 through 1000000000. A value of 0 disables the threshold.

**clear low_thresh**
- Default: 0
- Specifies the low threshold number of packets forwarded to CPUs that maintains a previously generated alarm condition. If the number of packets falls beneath the low threshold within the polling interval, a clear alarm will be generated.
- `low_thresh` is an integer from 0 through 1000000000. A value of 0 disables the threshold.
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 Forwarded packet thresholds generate alerts or alarms based on the total number of packets that were forwarded to active system CPU(s) during the specified polling interval. Packets are forwarded to active system CPUs when the NPUs do not have adequate information to properly route them.

Important Ping and/or traceroute packets are intentionally forwarded to system CPUs for processing. These packet types are included in the packet count for this threshold.

Alerts or alarms are triggered for forwarded packets based on the following rules:

- **Enter condition:** Actual number of forwarded packets is greater than or equal to the high threshold
- **Clear condition:** Actual number of forwarded packets is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Examples The following command configures a forwarded packet high threshold count of 100000 for a system using the Alert thresholding model:

```
threshold packets-forwarded-to-cpu 100000
```
threshold pdg-current-active-sessions

Configures alarm or alert thresholds for monitoring the total number of currently active Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG) sessions.

Product
PDG/TTG

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description
threshold pdg-current-active-sessions high_thresh [ clear low_thresh ]

high_thresh
Configures the total number of active PDG sessions to be monitored on a chassis. high_thresh is an integer from 0 through 1000000.
There is no default, but 0 means that there is no threshold monitoring.

clear low_thresh
Clears the number of sessions being monitored using the high_thresh variable defined above.
low_thresh is an integer from 0 through 1000000.

Usage Guidelines
Thresholds are provided for monitoring the overall PDG usage on a chassis. This command is used to monitor the total number of active PDG sessions for an entire chassis.

Examples
The following command configures a monitoring threshold of 300000 and a clearing threshold of 100000 active PDG sessions on a chassis:

threshold pdg-current-active-sessions 300000 clear 100000
threshold pdg-current-sessions

Configures alarm or alert thresholds for monitoring the total number of current Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG) sessions, including inactive sessions.

**Product**
PDG/TTG

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold pdg-current-sessions high_thresh [ clear low_thresh ]
```

- **high_thresh**
  Configures the total number of PDG sessions on a chassis, both active and inactive. *high_thresh* is any integer from 0 through 1000000.
  There is no default, but 0 means that there is no threshold monitoring.

- **clear low_thresh**
  Clears any number of sessions being monitored using the *high_thresh* variable defined above.
  *low_thresh* is any integer from 0 through 1000000.

**Usage Guidelines**
Thresholds are provided for monitoring the overall PDG usage on a chassis. This command is used to monitor the total number of PDG sessions, both active and inactive, for an entire chassis.

**Examples**
The following command configures a monitoring threshold of 300000 and a clearing threshold of 100000 active and inactive PDG sessions on a chassis:

```
threshold pdg-current-sessions 300000 clear 100000
```
threshold pdif-current-active-sessions

Configures alarm or alert thresholds for monitoring the total number of currently active Packet Data Interworking Function (PDIF) sessions.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold pdif-current-active-sessions high_thresh [ clear low_thresh ]
```

**high_thresh**

Configures the total number of active PDIF sessions to be monitored on a chassis. *high_thresh* is any integer from 0 through 1000000.

There is no default, but 0 means that there is no threshold monitoring.

**clear low_thresh**

Clears the specified number of sessions being monitored using the *high_thresh* variable defined above. *low_thresh* is any integer from 0 through 1000000.

**Usage Guidelines**

Thresholds are provided for monitoring the overall PDIF usage on a chassis. This command is used to monitor the total number of active PDIF sessions for an entire chassis.

**Examples**

The following command configures a monitoring threshold of 300000 and a clearing threshold of 100000 active PDIF sessions on a chassis:

```
threshold pdif-current-active-sessions 300000 clear 100000
```
threshold pdif-current-sessions

Configures alarm or alert thresholds for monitoring the total number of current Packet Data Interworking Function (PDIF) sessions, including inactive sessions.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

`threshold pdif-current-sessions high_thresh [ clear low_thresh ]`

*high_thresh*

Configures the total number of PDIF sessions on a chassis, both active and inactive. *high_thresh* is an integer from 0 through 1000000.

There is no default, but 0 means that there is no threshold monitoring.

*clear low_thresh*

Clears the specified number of sessions being monitored using the *high_thresh* variable defined above. *low_thresh* is an integer from 0 through 1000000.

**Usage Guidelines**

Thresholds are provided for monitoring the overall PDIF usage on a chassis. This command is used to monitor the total number of PDIF sessions, both active and inactive, for an entire chassis.

**Examples**

The following command configures a monitoring threshold of 300000 and a clearing threshold of 100000 active and inactive PDIF sessions on a chassis:

`threshold pdif-current-sessions 300000 clear 100000`
threshold per-service-asngw-sessions

Configures alarm or alert thresholds for the number of sessions per ASN-GW service in the system.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

**Syntax Description**

`threshold per-service-asngw-sessions high_thresh [ clear low_thresh ]`

- **high_thresh**
  
  Default: 0
  
  Specifies the high threshold number of PDP contexts for any one ASN-GW service that must be met or exceeded within the polling interval to generate an alert or alarm.
  
  `high_thresh` is an integer from 0 through 2500000. A value of 0 disables the threshold.

- **clear low_thresh**
  
  Default: 0
  
  Specifies the low threshold number of PDP contexts for any one ASN-GW service that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  
  `low_thresh` is an integer from 0 through 2500000. A value of 0 disables the threshold.

**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**

Monitor and set alarms or alerts when the number of PDP contexts for any ASN-GW service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition:** Actual number of PDP contexts for any ASN-GW service is greater than or equal to the high threshold
- **Clear condition:** Actual number of PDP contexts is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a high threshold count of 10000 subscriber attaches per ANS-GW service for the Alert thresholding model:

```
threshold per-service-asngw-sessions 10000
```
threshold per-service-ggsn-sessions

Configures alarm or alert thresholds for the number of PDP contexts per GGSN service in the system.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`threshold per-service-ggsn-sessions high_thresh [ clear low_thresh ]`

*high_thresh*

Default: 0

Specifies the high threshold number of PDP contexts for any one GGSN service that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is an integer from 0 through 4000000. A value of 0 disables the threshold.

*clear low_thresh*

Default: 0

Specifies the low threshold number of PDP contexts for any one GGSN service that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` is an integer from 0 through 4000000. A value of 0 disables the threshold.

**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**

Monitor and set alarms or alerts when the number of PDP contexts for any GGSN service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition:** Actual number of PDP contexts for any GGSN service is greater than or equal to the high threshold
- **Clear condition:** Actual number of PDP contexts is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a high threshold count of 10000 subscriber attaches per GGSN service for the Alert thresholding model:

```
threshold per-service-ggsn-sessions 10000
```
threshold per-service-gprs-pdp-sessions

Configures alarm or alert thresholds for the number of 2G-activated PDP contexts per GPRS service.

Product
SGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local]host_name(config)#

Syntax Description
threshold per-service-gprs-pdp-sessions high_thresh | clear low_thresh |

**high_thresh**
Default: 0
Specifies the high threshold number of 2G-activated PDP contexts for any one GPRS service. This number must be met or exceeded within the polling interval to generate an alert or alarm.

**clear low_thresh**
Default: 0
Specifies the low threshold number of 2G-activated PDP contexts for any one GPRS service. This number or higher maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, then a clear alarm will be generated.

**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
Monitor and set alarms or alerts when the number of 2G-activated PDP contexts for any GPRS service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition:** Actual number of PDP contexts for any GPRS service is greater than or equal to the high threshold.
- **Clear condition:** Actual number of PDP contexts is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a high threshold count of 10000 2G-activated PDP contexts per GPRS service for the Alert thresholding model:

```plaintext
threshold per-service-gprs-sessions 10000
```
threshold per-service-gprs-sessions

Configures alarm or alert thresholds for the number of 2G-attached subscribers per GPRS service.

Product
SGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

threshold per-service-gprs-sessions high_thresh [ clear low_thresh ]

**high_thresh**
Default: 0
Specifies the high threshold number of 2G-attached subscribers for any one GPRS service. This threshold number must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 2000000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0
Specifies the low threshold number of 2G-attached subscribers for any one GPRS service. The number of subscribers must remain above this threshold in order to maintain a previously generated alarm condition. If the number of 2G subscribers falls beneath the low threshold within the polling interval, then a clear alarm will be generated.

low_thresh is an integer from 0 through 2000000. A value of 0 disables the threshold.

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
Monitor and set alarms or alerts when the number of 2G-attached subscribers for any GPRS service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition**: Actual number of 2G-attached subscribers for any GPRS service is greater than or equal to the high threshold.
- **Clear condition**: Actual number of 2G-attached subscribers is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a high threshold count of 10000 2G-attaches per GPRS service for the Alert thresholding model:

```
threshold per-service-gprs-sessions 10000
```
threshold per-service-ha-sessions

Configures alarm or alert thresholds for the number of HA sessions per Home Agent (HA) service in the system.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold per-service-ha-sessions high_thresh | clear low_thresh
```

**high_thresh**

Default: 0

Specifies the high threshold number of HA sessions for any one HA service that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 4000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of HA sessions for any one HA service that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 4000000. A value of 0 disables the threshold.

**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**

Monitor and set alarms or alerts when the number of HA sessions for any HA service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for HA sessions based on the following rules:

- **Enter condition:** Actual number of HA sessions for any HA service is greater than or equal to the high threshold.
- **Clear condition:** Actual number of HA sessions is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a HA session per service high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold per-service-ha-sessions 10000
```
threshold per-service-lns-sessions

Configures alarm or alert thresholds for the number of L2TP Network Server (LNS) sessions per LNS service in the system.

**Product**
- PDSN
- GGSN
- HA
- ASN-GW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration

  configure

Entering the above command sequence results in the following prompt:

  [local]host_name(config)#

**Syntax Description**

  threshold per-service-lns-sessions **high_thresh** [ clear **low_thresh** ]

  **high_thresh**

  Default: 0

  Specifies the high threshold number of LNS sessions for any one LNS service that must be met or exceeded within the polling interval to generate an alert or alarm.

  *high_thresh* is an integer from 0 through 2500000. A value of 0 disables the threshold.

  **clear low_thresh**

  Default: 0

  Specifies the low threshold number of LNS sessions for any one LNS service that maintains a previously generated alarm condition. If the number of LNS sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

  *low_thresh* is an integer from 0 through 2500000. A value of 0 disables the threshold.
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**

Monitor and set alarms or alerts when the number of LNS sessions for any LNS service in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for LNS sessions based on the following rules:

- **Enter condition:** Actual number of LNS sessions for any LNS service is greater than or equal to the high threshold.
- **Clear condition:** Actual number of LNS sessions is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a LNS session per service high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold per-service-lns-sessions 10000
```
threshold per-service-pdg-sessions

Configures alarm or alert thresholds for the number of Packet Data Gateway (PDG) sessions per PDG service in the system.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

Syntax Description

threshold per-service-pdg-sessions high_thresh [ clear low_thresh ]

high_thresh

Default: 0

Specifies the high threshold number of PDG sessions for any one PDG service that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 1000000. A value of 0 disables the threshold.

clear low_thresh

Default: 0

Specifies the low threshold number of PDG sessions for any one PDG service that maintains a previously generated alarm condition. If the number of PDG sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 1000000. A value of 0 disables the threshold.

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

Monitor and set alarms or alerts when the number of PDG sessions for any PDG service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDSN sessions based on the following rules:

- **Enter condition**: Actual number of PDG sessions for any PDG service is greater than or equal to the high threshold.
- **Clear condition**: Actual number of PDSN sessions is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a PDG session per service high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold per-service-pdg-sessions 10000
```
threshold per-service-pdsn-sessions

Configures alarm or alert thresholds for the number of Packet Data Serving Node (PDSN) sessions per PDSN service in the system.

Product
PDSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]\host_name(config)#

Syntax Description
threshold per-service-pdsn-sessions high_thresh | clear low_thresh |

high_thresh
Default: 0
Specifies the high threshold number of PDSN sessions for any one PDSN service that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 2500000. A value of 0 disables the threshold.

clear low_thresh
Default: 0
Specifies the low threshold number of PDSN sessions for any one PDSN service that maintains a previously generated alarm condition. If the number of PDSN sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 2500000. A value of 0 disables the threshold.

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
Monitor and set alarms or alerts when the number of PDSN sessions for any PDSN service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDSN sessions based on the following rules:

- **Enter condition**: Actual number of PDSN sessions for any PDSN service is greater than or equal to the high threshold.
- **Clear condition**: Actual number of PDSN sessions is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a PDSN session per service high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold per-service-pdsn-sessions 10000
```
**threshold per-service-samog-sessions**

Configures alarm or alert thresholds for the number of S2a Mobility over GTP (SaMOG) sessions per SaMOG service in the system.

**Product**
SaMOG

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold per-service-samog-sessions high_thresh | clear low_thresh
```

**high_thresh**

Default: 0

Specifies the high threshold number of SaMOG sessions for any one SaMOG service that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 4,000,000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of SaMOG sessions for any one SaMOG service that maintains a previously generated alarm condition. If the number of SaMOG sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 4,000,000. A value of 0 disables the threshold.

**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**

Monitor and set alarms or alerts when the number of SaMOG sessions for any SaMOG service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for SaMOG sessions based on the following rules:

- **Enter condition**: Actual number of SaMOG sessions for any SaMOG service is greater than or equal to the high threshold.
- **Clear condition**: Actual number of SaMOG sessions is less than the 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 to configure the polling interval for this value.

**Examples**

The following command configures a SaMOG session per service high threshold count of 15000 for a system using the Alert thresholding model:

```
threshold per-service-samog-sessions 15000
```
threshold per-service-sgsn-pdp-sessions

Configures alarm or alert thresholds for the number of 3G-activated PDP contexts per SGSN service on the system.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description

threshold per-service-sgsn-pdp-sessions high_thresh | clear low_thresh |

high_thresh

Default: 0

Specifies the high threshold number of 3G-activated PDP contexts for any one SGSN service. This number must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

clear low_thresh

Default: 0

Specifies the low threshold number of 3G-activated PDP contexts for any one SGSN service. This number or higher maintains a previously generated alarm condition. If the number of 3G-activated PDP contexts falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 2400000. A value of 0 disables the threshold.

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

Monitor and set alarms or alerts when the number of 3G-activated PDP contexts for any SGSN service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition:** Actual number of 3G-activated PDP contexts for any SGSN service is greater than or equal to the high threshold.
- **Clear condition:** Actual number of 3G-activated PDP contexts is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

### Examples

The following command configures a high threshold count of 10000 3G-activated PDP contexts per SGSN service for the system's Alert thresholding model:

```
threshold per-service-sgsn-sessions 10000
```
threshold per-service-sgsn-sessions

Configures alarm or alert thresholds for the number of 3G-attached subscribers per SGSN service in the system.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold per-service-sgsn-sessions high_thresh | clear low_thresh
```

**high_thresh**

Default: 0

Specifies the high threshold number of 3G-attached subscribers for any one SGSN service. This number must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is an integer from 0 through 2000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of 3G-attached subscribers for any one SGSN service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` is an integer from 0 through 2000000. A value of 0 disables the threshold.

---

**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**

Monitor and set alarms or alerts when the number of 3G-attached subscribers for any one SGSN service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition**: Actual number of 3G-attached subscribers for any single SGSN service is greater than or equal to the high threshold.
- **Clear condition**: Actual number of 3G-attached subscribers for any single SGSN service is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

### Examples

The following command configures a high threshold count of 10000 3G-attached subscribers per SGSN service for a system using the Alert thresholding model:

```
threshold per-service-sgsn-sessions 10000
```
threshold phsgw-auth-failure

Configures alarm or alert thresholds for the number of authentication failures in Personal Handyphone Service Gateway (PHSGW) service.

**Product**

PHSGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

**Syntax Description**

threshold phsgw-auth-failure high_thresh  [ clear low_thresh ]

*high_thresh*

Default: 0

Specifies the high threshold number for PHSGW authentication failures in any one PHSGW service. This number must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 1000000. A value of 0 disables the threshold.

*clear low_thresh*

Default: 0

Specifies the low threshold number of PHSGW authentication failures in any one PHSGW service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 1000000. A value of 0 disables the threshold.

---

**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**

Set the monitoring and clearing thresholds for PHSGW authentication failures.
Alerts or alarms are triggered for authentication failures based on the following rules:

- **Enter condition**: Actual number of PHSGW authentication failures in any one PHSGW service is greater than or equal to the high threshold.
- **Clear condition**: Actual number of PHSGW authentication failures in any one PHSGW service is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSGW authentication failures:

```
threshold phsgw-auth-failure 100000 clear 50000
```
threshold phsgw-eapol-auth-failure

Configures alarm or alert thresholds for authentication failures for a PHSGW service using Extensible Authentication Protocol Over LAN (EAPOL).

Product
PHSGW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name(config) #

Syntax Description
threshold phsgw-eapol-auth-failure high_thresh | clear low_thresh |

high_thresh
Default: 0
Specifies the high threshold number for PHSGW EAPOL failures in any one PHSGW service. This number must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 1000000. A value of 0 disables the threshold.

clear low_thresh
Default: 0
Specifies the low threshold number of PHSGW EAPOL failures in any one PHSGW service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 1000000. A value of 0 disables the threshold.

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
Set the monitoring and clearing thresholds for PHSGW EAPOL failures.
Alerts or alarms are triggered for EAPOL failures based on the following rules:

- **Enter condition**: Actual number of PHSGW EAPOL failures in any one PHSGW service is greater than or equal to the high threshold.

- **Clear condition**: Actual number of PHSGW EAPOL failures in any one PHSGW service is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSGW EAPOL failures:

`threshold phsgw-eapol-auth-failure 100000 clear 50000`
threshold phsgw-handoff-denial

Configures alarm or alert thresholds for handoff denials in PHSGW.

**Product**
PHSGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

threshold phsgw-handoff-denial high_thresh [clear low_thresh]

**high_thresh**
Default: 0
Specifies the high threshold number of handoff denials for any one PHSGW service. This number must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 1000000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0
Specifies the low threshold number of handoff denials for any one PHSGW service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 1000000. A value of 0 disables the threshold.

**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**
Set the monitoring and clearing thresholds for PHSGW handoff denials.
Alerts or alarms are triggered for handoff denials based on the following rules:
• **Enter condition:** Actual number of PHSGW handoff denials in any one PHSGW service is greater than or equal to the high threshold.

• **Clear condition:** Actual number of PHSGW handoff denials in any one PHSGW service is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSGW handoff denials:

```
threshold phsgw-handoff-denial 100000 clear 50000
```
threshold phsgw-max-eap-retry

Configures alarm or alert thresholds for the maximum number of Extensible Authentication Protocol (EAP) retries in PHSGW.

**Product**

PHSGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

`threshold phsgw-max-eap-retry high_thresh | clear low_thresh`

**high_thresh**

Default: 0

Specifies the high threshold number of EAP retries for any one PHSGW service. This number must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is an integer from 0 through 1000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of EAP retries for any one PHSGW service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` is an integer from 0 through 1000000. A value of 0 disables the threshold.

**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**

Set the monitoring and clearing thresholds for PHSGW EAP retries.
Alerts or alarms are triggered for handoff denials based on the following rules:

- **Enter condition:** Actual number of PHSGW EAP retries in any one PHSGW service is greater than or equal to the high threshold.

- **Clear condition:** Actual number of PHSGW EAP retries in any one PHSGW service is less than the 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 to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

**Examples**

The following command configures a monitoring threshold of $100000$ and a clearing threshold of $50000$ for PHSGW EAP retries:

```
threshold phsgw-max-eap-retry 100000 clear 50000
```
threshold phsgw-max-eapol-retry

Configures alarm or alert thresholds for the maximum number of Extensible Authentication Protocol over LAN (EAPOL) retries in PHSGW.

Product

PHSGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description

threshold phsgw-max-eapol-retry high_thresh | clear low_thresh |

high_thresh

Default: 0

Specifies the high threshold number of EAPOL retries for any one PHSGW service. This number must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 1000000. A value of 0 disables the threshold.

clear low_thresh

Default: 0

Specifies the low threshold number of EAPOL retries for any one PHSGW service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 1000000. A value of 0 disables the threshold.

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

Set the monitoring and clearing thresholds for PHSGW EAPOL retries.
Alerts or alarms are triggered for handoff denials based on the following rules:

- **Enter condition**: Actual number of PHSGW EAPOL retries in any one PHSGW service is greater than or equal to the high threshold.
- **Clear condition**: Actual number of PHSGW EAPOL retries in any one PHSGW service is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSGW EAPOL retries:

```
threshold phsgw-max-eapol-retry 100000 clear 50000
```
threshold phsgw-network-entry-denial

Configures, alarm or alert thresholds for the number of network entry denials in PHSGW.

**Product**
PHSGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold phsgw-max-network-entry-denial high_thresh  [ clear low_thresh ]
```

**high_thresh**

Default: 0

Specifies the high threshold number of network entry denials for any one PHSGW service. This number must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 1000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of network entry denials for any one PHSGW service. This number must be met or exceeded to maintain a previously generated alert condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 1000000. A value of 0 disables the threshold.

---

**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**
Set the monitoring and clearing thresholds for PHSGW network entry denials.

Alerts or alarms are triggered for handoff denials based on the following rules:
• **Enter condition**: Actual number of PHSGW network entry denials in any one PHSGW service is greater than or equal to the high threshold.

• **Clear condition**: Actual number of PHSGW network entry denials in any one PHSGW service is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSGW network entry denials:

`threshold phsgw-network-entry-denial 100000 clear 50000`
threshold phsgw-session-setup-timeout

Configures alarm or alert thresholds for the number of PHSGW sessions that timed out during setup.

Product
PHSGW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local]\(host\_name\)(config)#

Syntax Description
threshold phsgw-session-setup-timeout \(high\_thresh\) | clear \(low\_thresh\) |

\(high\_thresh\)
Default: 0
Specifies the high threshold number of session setup timeouts for any one PHSGW service. This number must be met or exceeded within the polling interval to generate an alert or alarm.
\(high\_thresh\) is an integer from 0 through 1000000. A value of 0 disables the threshold.

clear \(low\_thresh\)
Default: 0
Specifies the low threshold number of session setup timeouts for any one PHSGW service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.
\(low\_thresh\) is an integer from 0 through 1000000. A value of 0 disables the threshold.

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
Set the monitoring and clearing thresholds for PHSGW session setup timeouts.
Alerts or alarms are triggered for handoff denials based on the following rules:
• **Enter condition**: Actual number of PHSGW session setup timeouts in any one PHSGW service is greater than or equal to the high threshold.

• **Clear condition**: Actual number of PHSGW session setup timeouts in any one PHSGW service is less than the 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 to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

**Examples**

The following command configures a monitoring threshold of `100000` and a clearing threshold of `50000` for PHSGW session setup timeouts:

```
threshold phsgw-session-setup-timeout 100000 clear 50000
```
**threshold phsgw-session-timeout**

Configures alarm or alert thresholds for the number of PHSGW sessions that timed out.

**Product**
PHSGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold phsgw-session-timeout high_thresh [ clear low_thresh ]
```

- **high_thresh**
  Default: 0
  Specifies the high threshold number of session timeouts for any one PHSGW service. This number must be met or exceeded within the polling interval to generate an alert or alarm.
  `high_thresh` is an integer from 0 through 1000000. A value of 0 disables the threshold.

- **clear low_thresh**
  Default: 0
  Specifies the low threshold number of session timeouts for any one PHSGW service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  `low_thresh` is an integer from 0 through 1000000. A value of 0 disables the threshold.

- **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**
Set the monitoring and clearing thresholds for PHSGW session timeouts.

Alerts or alarms are triggered for handoff denials based on the following rules:
• **Enter condition:** Actual number of PHSGW session timeouts in any one PHSGW service is greater than or equal to the high threshold.

• **Clear condition:** Actual number of PHSGW session timeouts in any one PHSGW service is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

### Examples

The following command configures a monitoring threshold of **100000** and a clearing threshold of **50000** for PHSGW session timeouts:

```
threshold phsgw-session-timeout 100000 clear 50000
```
threshold phspc-session-setup-timeout

Configures alarm or alert thresholds for the number of Personal Handyphone System - Personal Computer (PHSPC) sessions that timed out during setup.

Product PHSGW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration
                    configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description threshold phspc-session-setup-timeout high_thresh [ clear low_thresh ]

high_thresh
Default: 0
Specifies the high threshold number of session setup timeouts for any one PHSPC service. This number must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 1000000. A value of 0 disables the threshold.

clear low_thresh
Default: 0
Specifies the low threshold number of session setup timeouts for any one PHSPC service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 1000000. A value of 0 disables the threshold.

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 Set the monitoring and clearing thresholds for PHSPC session setup timeouts.
Alerts or alarms are triggered for handoff denials based on the following rules:

- **Enter condition:** Actual number of PHSPC session setup timeouts in any one PHSGW service is greater than or equal to the high threshold.
- **Clear condition:** Actual number of PHSPC session setup timeouts in any one PHSGW service is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSPC session setup timeouts:

```
threshold phspc-session-setup-timeout 100000 clear 50000
```
threshold phspc-sleep-mode-timeout

Configures alarm or alert thresholds for the number of PHSPC sessions that timed out when the personal computer went into sleep mode.

Product

PHSGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description

```
threshold phspc-sleep-mode-timeout high_thresh | clear low_thresh
```

**high_thresh**

Default: 0

Specifies the high threshold number of sleep mode timeouts for any one PHSPC service. This number must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 1000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of sleep mode timeouts for any one PHSPC service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 1000000. A value of 0 disables the threshold.

**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

Set the monitoring and clearing thresholds for PHSPC sleep mode timeouts.
Alerts or alarms are triggered for handoff denials based on the following rules:

- **Enter condition:** Actual number of PHSPC sleep mode timeouts in any one PHSGW service is greater than or equal to the high threshold.
- **Clear condition:** Actual number of PHSPC sleep mode timeouts in any one PHSGW service is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSPC sleep mode timeouts:

```
threshold phspc-sleep-mode-timeout 100000 clear 50000
```
threshold phspc-sm-entry-denial

Configures alarm or alert thresholds for the number of denied PHSPC short message (SM) sessions.

**Product** PHSGW

**Privilege** Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold phspc-sm-entry-denial high_thresh | clear low_thresh
```

*high_thresh*

Default: 0

Specifies the high threshold number of SM entry denials for any one PHSPC service. This number must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is an integer from 0 through 1000000. A value of 0 disables the threshold.

*clear low_thresh*

Default: 0

Specifies the low threshold number of SM entry denials for any one PHSPC service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` is an integer from 0 through 1000000. A value of 0 disables the threshold.

**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**

Set the monitoring and clearing thresholds for PHSPC SM entry denials.

Alerts or alarms are triggered for handoff denials based on the following rules:
Enter condition: Actual number of PHSPC SM entry denials in any one PHSPC service is greater than or equal to the high threshold.

Clear condition: Actual number of PHSPC SM entry denials in any one PHSPC service is less than the 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 to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

Examples

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSPC SM entry denials:

```
threshold phsgw-sm-entry-denial 100000 clear 50000
```
threshold phspc-sm-entry-denyal
Global Configuration Mode Commands (threshold poll commands A - N)

The Global Configuration Mode is used to configure basic system-wide parameters.

This section includes the commands `threshold poll 10sec-cpu-utilization interval` through `threshold poll npu-utilization interval`.

**Command Modes**

Exec > Global Configuration

```bash
configure
```

Entering the above command sequence results in the following prompt:

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

**Important**

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

- `threshold poll 10sec-cpu-utilization interval`, page 617
- `threshold poll a11-ppp-send-discard interval`, page 619
- `threshold poll a11-rac-msg-discard interval`, page 621
- `threshold poll aa11-rrp-failure interval`, page 623
- `threshold poll a11-rrq-msg-discard interval`, page 625
- `threshold poll aaa-acct-archive-queue-size interval`, page 627
- `threshold poll aaa-acct-archive-size interval`, page 629
- `threshold poll aaa-acct-failure interval`, page 630
- `threshold poll aaa-acct-failure-rate interval`, page 632
- `threshold poll aaa-auth-failure interval`, page 634
- `threshold poll aaa-auth-failure-rate interval`, page 636
• threshold poll aaa-retry-rate interval, page 638
• threshold poll aaamgr-request-queue interval, page 640
• threshold poll active-subscriber interval, page 642
• threshold poll asngw-auth-failure interval, page 644
• threshold poll asngw-handoff-denial interval, page 646
• threshold poll asngw-max-eap-retry interval, page 648
• threshold poll asngw-network-entry-denial interval, page 650
• threshold poll asngw-r6-invalid-nai interval, page 652
• threshold poll asngw-session-setup-timeout interval, page 654
• threshold poll asngw-session-timeout interval, page 656
• threshold poll asnpc-idle-mode-timeout interval, page 658
• threshold poll asnpc-im-entry-denial interval, page 660
• threshold poll asnpc-lu-denial interval, page 662
• threshold poll asnpc-session-setup-timeout interval, page 664
• threshold poll available-ip-pool-group interval, page 666
• threshold poll call-reject-no-resource interval, page 668
• threshold poll call-setup interval, page 670
• threshold poll call-setup-failure interval, page 672
• threshold poll call-setup-failures interval, page 674
• threshold poll call-total-active interval, page 676
• threshold poll card-temperature-near-power-off-limit interval, page 678
• threshold poll cdr-file-space interval, page 680
• threshold poll contfilt-block interval, page 682
• threshold poll contfilt-rating interval, page 684
• threshold poll cpu-available-memory interval, page 686
• threshold poll cpu-load interval, page 688
• threshold poll cpu-memory-usage interval, page 690
• threshold poll cpu-orbs-crit interval, page 692
• threshold poll cpu-orbs-warn interval, page 694
• threshold poll cpu-session-throughput interval, page 696
• threshold poll cpu-utilization interval, page 698
• threshold poll dcca-bad-answers interval, page 700
• threshold poll dcca-protocol-error interval, page 702
- threshold poll dcca-rating-failed interval, page 704
- threshold poll dcca-unknown-rating-group interval, page 706
- threshold poll dereg-reply-error interval, page 708
- threshold poll diameter-retry-rate interval, page 710
- threshold poll disconnect-reason, page 712
- threshold poll edr-file-space interval, page 714
- threshold poll edr-udr-dropped-flow-control interval, page 715
- threshold poll epdg-current-sessions interval, page 716
- threshold poll epdg-ikev2-authentication-failures, page 718
- threshold poll epdg-ikev2-setup-attempts, page 719
- threshold poll epdg-ikev2-setup-failure, page 720
- threshold poll epdg-ikev2-setup-failure-rate, page 721
- threshold poll epdg-ikev2-setup-success, page 722
- threshold poll fa-reg-reply-error interval, page 723
- threshold poll fng-current-active-sessions interval, page 725
- threshold poll fng-current-sessions interval, page 727
- threshold poll fw-deny-rule interval, page 729
- threshold poll fw-dos-attack interval, page 731
- threshold poll fw-drop-packet interval, page 733
- threshold poll fw-no-rule interval, page 735
- threshold poll ha-init-rrq-rcvd-rate interval, page 737
- threshold poll ha-svc-init-rrq-rcvd-rate interval, page 739
- threshold poll henbgw-paging-messages interval, page 741
- threshold poll ip-pool-free interval, page 742
- threshold poll ip-pool-hold interval, page 744
- threshold poll ip-pool-release interval, page 746
- threshold poll ip-pool-used interval, page 748
- threshold poll ipsec-call-req-rej interval, page 750
- threshold poll ipsec-ike-failrate interval, page 752
- threshold poll ipsec-ike-failures interval, page 754
- threshold poll ipsec-ike-requests interval, page 756
- threshold poll ipsec-tunnels-established interval, page 758
- threshold poll ipsec-tunnels-setup interval, page 760
• threshold poll license-remaining-session interval, page 762
• threshold poll mgmt-cpu-memory-usage interval, page 763
• threshold poll mgmt-cpu-utilization interval, page 764
• threshold poll mme-attach-failure interval, page 765
• threshold poll mme-auth-failure interval, page 767
• threshold poll nat-pkt-drop, page 769
• threshold poll nat-port-chunks-usage interval, page 771
• threshold poll npu-utilization interval, page 773
threshold poll 10sec-cpu-utilization interval

Configures the polling interval over which to measure a 10-second average of CPU utilization.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration

configure
Entering the above command sequence results in the following prompt:

[local] host_name(config)#

Syntax Description

threshold poll 10sec-cpu-utilization interval duration
default threshold poll 10sec-cpu-utilization interval

default
Restores the specified parameter to its default value 300 seconds.

interval duration
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration is an integer from 30 through 60000 in multiples of 30.

Usage Guidelines

This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshCPUUtilization10Sec` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the 10-second CPU utilization threshold:

```
threshold poll 10sec-cpu-utilization 600
```
threshold poll a11-ppp-send-discard interval

Configures the polling interval for PDSN service over which to count the number of packets that the PPP protocol processing layer internally discarded on transmit for any reason.

Product
PDSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

- `threshold poll a11-ppp-send-discard interval duration`
- `default threshold poll a11-ppp-send-discard interval`

- `default`
  Restores the specified parameter to its default value 0 seconds.

- `interval duration`
  Default: 0 seconds.
  Specifies the amount of time (in seconds) that comprises the polling interval.
  `duration` is an integer from 60 through 900 in multiples of 30.

Usage Guidelines

This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` `ThreshPDSNSvcA11PPPSendDiscard` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the A11 PPP send discard threshold:

```
threshold poll a11-ppp-send-discard interval 600
```
**threshold poll a11-rac-msg-discard interval**

Configures the polling interval for PDSN service over which to count the number of Discarded A11 Registration Acknowledgements.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll a11-rac-msg-discard interval duration
default threshold poll a11-rac-msg-discard interval

default
Restores the specified parameter to its default value 0 seconds.

interval duration
Default: 0 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration is an integer from 60 through 900 in multiples of 30.
```

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPDSNSvcA11RACMsgDiscard` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the A11 RAC message discard threshold:

```
threshold poll a11-rac-msg-discard interval 600
```
threshold poll aa11-rrp-failure interval

Configures the polling interval for PDSN service over which to count A11 Registration Response failures.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll a11-rrp-failure interval duration
default threshold poll a11-rrp-failure interval
```

- **default**
Restores the specified parameter to its default value 0 seconds.

- **interval duration**
Default: 0 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.

*duration* is an integer from 60 through 900 in multiples of 30.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPDSNSvcA11RRPFailure` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the A11 RRP failure threshold:

```
threshold poll a11-rrp-failure interval 600
```
threshold poll a11-rrq-msg-discard interval

Configures the polling interval for PDSN service over which to count how many A11 Registration Request messages are discarded.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll a11-rrq-msg-discard interval duration

default threshold poll a11-rrq-msg-discard interval

default

Restores the specified parameter to its default value 0 seconds.

interval duration

Default: 0 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

duration is an integer from 60 through 900 in multiples of 30.
```

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.
Important

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` `ThreshPDSNSvcA11RRQMsgDiscard` command in this mode.

Examples

The following command configures the polling interval to 600 seconds for the A11 RRQ message discard threshold:

```
threshold poll a11-rrq-msg-discard interval 600
```
**threshold poll aaa-acct-archive-queue-size interval**

Configures the polling interval over which to measure AAA accounting archive message queue size.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

```
threshold poll aaa-acct-archive-queue-size1 interval duration
default threshold poll aaa-acct-archive-queue-size1 interval
threshold poll aaa-acct-archive-queue-size2 interval duration
default threshold poll aaa-acct-archive-queue-size2 interval
threshold poll aaa-acct-archive-queue-size3 interval duration
default threshold poll aaa-acct-archive-queue-size3 interval
```

default
Restores the specified parameter to its default value 900 seconds.

```
interval duration
```

Default: 900 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

*duration* is an integer from 60 through 60000 in multiples of 30.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` `ThreshAAAAccountQueue-<1-3>` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the AAA accounting archive queue size 1 threshold:

```
threshold poll aaa-acct-archive-queue-size1 interval 600
```
**threshold poll aaa-acct-archive-size interval**

Configures the polling interval over which to count archived AAA accounting messages.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

- `threshold poll aaa-acct-archive-size interval duration`
- `default threshold poll aaa-acct-archive-size interval`

- `default`
  Restores the specified parameter to its default value 300 seconds.

- `interval duration`
  Default: 300 seconds.
  Specifies the amount of time (in seconds) that comprises the polling interval.
  `duration` is an integer from 60 through 60000 in multiples of 30.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system's support for thresholds in this chapter.

**Examples**

The following command configures the polling interval to 600 seconds for the AAA accounting archive size threshold:

```
threshold poll aaa-acct-archive-size interval 600
```
threshold poll aaa-acct-failure interval

Configures the polling interval over which to count failed AAA accounting requests.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll aaa-acct-failure interval duration
default threshold poll aaa-acct-failure interval
```

```
default
Restores the specified parameter to its default value 300 seconds.
```

```
interval duration
Default: 300 seconds.
```

Specifies the amount of time (in seconds) that comprises the polling interval.

```
duration is an integer from 60 through 60000 in multiples of 30.
```

**Usage Guidelines**
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshAAAAcctFail` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the AAA accounting failure threshold:

```plaintext
threshold poll aaa-acct-failure interval 600
```
threshold poll aaa-acct-failure-rate interval

Configures the polling interval over which to measure the percentage of AAA accounting failures.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

**Syntax Description**

threshold poll aaa-acct-failure-rate interval *duration*

default threshold poll aaa-acct-failure-rate interval

default

Restores the specified parameter to its default value 300 seconds.

**interval duration**

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

*duration* is an integer from 60 through 60000 in multiples of 30.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the **snmp trap enable ThreshAAAActFailRate** command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the AAA accounting failure rate threshold:

```
threshold poll aaa-acct-failure-rate interval 600
```
threshold poll aaa-auth-failure interval

Configures the polling interval over which to count failed authentication requests.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description
threshold poll aaa-auth-failure interval duration
default threshold poll aaa-auth-failure interval
default
Restores the specified parameter to its default value 300 seconds.

interval duration
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration is an integer from 60 through 60000 in multiples of 30.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshAAAAuthFail` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the AAA authentication failure threshold:

```
threshold poll aaa-auth-failure interval 600
```
threshold poll aaa-auth-failure-rate interval

Configures the polling interval over which to measure the percentage of AAA authentication failures.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll aaa-auth-failure-rate interval duration
default threshold poll aaa-auth-failure-rate interval
```

- **default**
  Restores the specified parameter to its default value 300 seconds.

- **interval duration**
  Default: 300 seconds.
  Specifies the amount of time (in seconds) that comprises the polling interval.
  `duration` is an integer from 60 through 60000 in multiples of 30.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmptrapenableThreshAAAAuthFailRate` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the AAA authentication failure rate threshold:

```
thresholdpollaaa-auth-failure-rateinterval600
```
**threshold poll aaa-retry-rate interval**

Configures the polling interval over which to measure the percent of AAA request message retries.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll aaa-retry-rate interval duration
default threshold poll aaa-retry-rate interval
```

**default**

Restores the specified parameter to its default value 300 seconds.

**interval duration**

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

`duration` is an integer from 60 through 60000 in multiples of 30.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshAAARetryRate` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the AAA retry rate threshold:

```
threshold poll aaa-retry-rate interval 600
```
threshold poll aaamgr-request-queue interval

Configures the polling interval over which to count the number of AAA Manager Requests for each AAA manager process.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure
Entering the above command sequence results in the following prompt:
[local] host_name (config) #

**Syntax Description**
threshold poll aaamgr-request-queue interval *duration*
default threshold poll aaamgr-request-queue interval

default
Restores the specified parameter to its default value 0 seconds.

interval *duration*
Default: 0 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
*duration* is an integer from 60 through 60000 in multiples of 30.

**Usage Guidelines**
This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshAAAMgrQueue` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the AAA manager request queue threshold:

```
threshold poll aaamgr-request-queue interval 600
```
threshold poll active-subscriber interval

Configures the polling interval over which to count the total number of active subscriber sessions.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll active-subscriber interval duration
default threshold poll active-subscriber interval
```

- **default**
  Restores the specified parameter to its default value 300 seconds.

- **interval duration**
  Default: 300 seconds.
  Specifies the amount of time (in seconds) that comprises the polling interval.
  *duration* is an integer from 60 through 60000 in multiples of 30.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.
Important

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshSubscriberActive` command in this mode.

Examples

The following command configures the polling interval to 600 seconds for the active subscriber threshold:

`threshold poll active-subscriber interval 600`
threshold poll asngw-auth-failure interval

Configures the polling interval over which to count or measure the thresholding value for ASN Gateway authentication failure.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

Syntax Description
threshold poll asngw-auth-failure interval dur
default threshold poll asngw-auth-failure interval

default
Restores the specified parameter to its default value 300 seconds.

interval dur
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
dur is an integer from 30 through 60000 in multiples of 30.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshASNGWAuthFail` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the ASN Gateway authentication failure threshold:

```
threshold poll asgw-auth-failure interval 600
```
threshold poll asngw-handoff-denial interval

Configures the polling interval over which to count or measure the thresholding value for ASN Gateway hand-off denial.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description
threshold poll asngw-handoff-denial interval dur
default threshold poll asngw-handoff-denial interval

default
Restores the specified parameter to its default value 300 seconds.

interval dur
Default: 300 seconds.
Specifies the polling interval time in seconds.
dur is an integer from 30 through 60000 in multiples of 30.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` `ThreshASNGWHandoffDenial` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the hand-off denial threshold:

`threshold poll asngw-handoff-denial interval 600`
threshold poll asngw-max-eap-retry interval

Configures the polling interval over which to count or measure the thresholding value for maximum Extensible Authentication Protocol (EAP) authentication retries.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description
threshold poll asngw-max-eap-retry interval dur
default threshold poll asngw-max-eap-retry interval

default
Restores the specified parameter to its default value 300 seconds.

interval dur
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
dur is an integer from 30 through 60000 in multiples of 30.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the maximum EAP authentication retry threshold:

```
threshold poll asngw-max-eap-retry interval 600
```
threshold poll asngw-network-entry-denial interval

Configures the polling interval over which to count or measure the thresholding value for network entry denial to an MS.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

Syntax Description
threshold poll asngw-network-entry-denial interval dur
default threshold poll asngw-network-entry-denial interval

default
Restores the specified parameter to its default value 300 seconds.

interval dur
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
dur is an integer from 30 through 60000 in multiples of 30.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
Important: To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` `ThreshASNGWNWEntryDenial` command in this mode.

Examples: The following command configures the polling interval to 600 seconds for the network entry denial threshold:
```
threshold poll asngw-network-entry-denial interval 600
```
threshold poll asngw-r6-invalid-nai interval

Configures the polling interval over which to count or measure the thresholding value for invalid Network Access Identifiers (NAIs) in R6 messages.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

`threshold poll asngw-r6-invalid-nai interval dur`

`default threshold poll asngw-r6-invalid-nai interval`

`default`

Restores the specified parameter to its default value 300 seconds.

`interval dur`

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

`dur` is an integer from 30 through 60000 in multiples of 30.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing. 

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshASNGWR6InvNai` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the invalid NAIs in R6 messages threshold:

```
threshold poll asngw-r6-invalid-nai interval 600
```
threshold poll asngw-session-setup-timeout interval

Configures the polling interval over which to count or measure the thresholding value for session setup timeout.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local]host_name(config)#

Syntax Description
threshold poll asngw-session-setup-timeout interval dur
default threshold poll asngw-session-setup-timeout interval
default
Restores the specified parameter to its default value 300 seconds.
interval dur
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
dur is an integer from 30 through 60000 in multiples of 30.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` `ThreshASNGWSessSetupTimeout` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the session setup timeout threshold:

```
threshold poll asngw-session-setup-timeout interval 600
```
threshold poll asngw-session-timeout interval

Configures the polling interval over which to count or measure the thresholding value for session timeout.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local]host_name(config)#

Syntax Description

threshold poll asngw-session-timeout interval *dur*
default threshold poll asngw-session-timeout interval

default
Restores the specified parameter to its default value (300 seconds).

interval *dur*
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
dur is an integer from 30 through 60000 in multiples of 30.

Usage Guidelines

This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` `ThreshASNGWSessTimeout` command in this mode.

**Important**

**Examples**

The following command configures the polling interval to 600 seconds for the session timeout threshold:

```
threshold poll asngw-session-timeout interval 600
```
threshold poll asnpc-idle-mode-timeout interval

Configures the polling interval over which to count the number of ASNPC Instant Messenger idle mode timeouts.

**Product**

ASN-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll asnpc-idle-mode-timeout interval dur
default threshold poll asnpc-idle-mode-timeout interval
```

default

Restores the specified parameter to its default value (300 seconds).

```
interval dur
```

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

`dur` is an integer from 30 through 60000 in multiples of 30.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` `ThreshASNPCIIdleModeTimeout` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the idle mode timeout threshold:

```
threshold poll asnpc-idle-mode-timeout interval 600
```
**threshold poll asnpc-im-entry-denial interval**

Configures the polling interval over which to count the number of ASNPC Instant Messenger entry denials.

**Product**

ASN-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll asnpc-im-entry-denial interval <dur>
default threshold poll asnpc-im-entry-denial interval

default
Restores the specified parameter to its default value (300 seconds).

interval <dur>
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
<dur> is an integer from 30 through 60000 in multiples of 30.
```

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the IM entry denial threshold:

```
threshold poll asnpc-im-entry-denial interval 600
```
threshold poll asnpc-lu-denial interval

Configures the polling interval over which to count the number of ASNPC Location Update (LU) denials.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description
threshold poll asnpc-lu-denial interval

default threshold poll asnpc-lu-denial interval interval

default
Restores the specified parameter to its default value (300 seconds).

interval dur
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
dur is an integer from 30 through 60000 in multiples of 30.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshASNPCIuDenial` command in this mode.

**Important**

**Examples**

The following command configures the polling interval to 600 seconds for the LU denial threshold:

```
threshold poll asnpc-lu-denial interval 600
```
threshold poll asnpc-session-setup-timeout interval

Configures the polling interval over which to count the number of times an ASNPC session timed out before setup completion.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll asnpc-session-setup-timeout interval  
default threshold poll asnpc-session-setup-timeout interval

default
Restores the specified parameter to its default value (300 seconds).

interval *dur*
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.

*dur* is an integer from 30 through 60000 in multiples of 30.
```

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` `ThreshASNPCSessSetupTimeout` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the session setup timeout threshold:

```
threshold poll asnpc-session-setup-timeout interval 600
```
threshold poll available-ip-pool-group interval

Configures the polling interval over which to measure IP pool utilization.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description
threshold poll available-ip-pool-group interval \( \text{dur} \)
default threshold poll available-ip-pool-group interval

default
Restores the specified parameter to its default value (300 seconds).

interval \( \text{dur} \)
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
\( \text{dur} \) is an integer from 30 through 60000 in multiples of 30.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
Important

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshIPPoolAvail` command in this mode.

Examples

The following command configures the polling interval to 600 seconds for available IP pool threshold:

```
threshold poll available-ip-pool-group interval 600
```
threshold poll call-reject-no-resource interval

Configures the polling interval over which to measure IP pool utilization.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local] host_name (config) #

Syntax Description
threshold poll call-reject-no-resource interval  \textit{dur}
default threshold poll call-reject-no-resource interval

default
Restores the specified parameter to its default value (900 seconds).

interval \textit{dur}
Default: 900 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
\textit{dur} is an integer from 30 through 60000 in multiples of 30.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

\begin{center}
\textbf{Important}
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.
\end{center}

Refer to the \textit{threshold monitoring} and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshCallRejectNoResource` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for call reject no-resource threshold:

```
threshold poll call-reject-no-resource interval 600
```
threshold poll call-setup interval

Configures the polling interval over which to count the number of calls that were setup.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure
Entering the above command sequence results in the following prompt:
[local]host_name(config)#

Syntax Description
threshold poll call-setup interval  dur

default threshold poll call-setup interval

default
Restores the specified parameter to its default value (900 seconds).

interval dur
Default: 900 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
dur is an integer from 30 through 60000 in multiples of 30.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
Important  To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshCallSetup` command in this mode.

Examples  The following command configures the polling interval to 600 seconds for the call setup threshold: `threshold poll call-setup interval 600`
threshold poll call-setup-failure interval

Configures the polling interval over which to count the number of calls that failed to setup.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll call-setup-failure interval  dur
default threshold poll call-setup-failure interval
```

```
default
```
Restores the specified parameter to its default value (900 seconds).

```
interval dur
```
Default: 900 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

`dur` is an integer from 30 through 60000 in multiples of 30.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshCallSetupFailure` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for call setup failure threshold:

`threshold poll call-setup-failure interval 600`
threshold poll call-setup-failures interval

Configures the polling interval over which to count the number of CSCF call setup failures.

Product

SCM

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

threshold poll call-setup-failures interval  dur

default threshold poll call-setup-failures interval

default
Restores the specified parameter to its default value (300 seconds).

interval dur
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.

dur is an integer from 60 through 60000 in multiples of 30.

Usage Guidelines

This command sets the time period over which to monitor the specified value for threshold crossing.

Important

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` `ThreshCSCFSvcTotalCallFailure` command in this mode.

**Important**

**Examples**

The following command configures the polling interval to 600 seconds for CSCF session timeout threshold:

```
threshold poll call-setup-failures interval 600
```
threshold poll call-total-active interval

Configures the polling interval over which to count the total number of CSCF active calls.

**Product**

SCM

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

threshold poll call-total-active interval  *dur*

default threshold poll call-total-active interval

default

Restores the specified parameter to its default value (300 seconds).

**interval dur**

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

*dur* is an integer from 60 through 60000 in multiples of 30.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshCSCFSvcTotalActiveCalls` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for session timeout threshold:

```
threshold poll call-total-active interval 600
```
**threshold poll card-temperature-near-power-off-limit interval**

Configures the polling interval over which to count the number of times card temperatures reached the power-off limit.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

- `threshold poll card-temperature-near-power-off-limit interval dur`
- `default threshold poll card-temperature-near-power-off-limit interval`

**default**
Restores the specified parameter to its default value (300 seconds).

**interval dur**
Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

`dur` is an integer from 60 through 60000 in multiples of 30.

**Usage Guidelines**
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable
ThreshCardTemperatureNearPowerOffLimit` command in this mode.

**Important**

**Examples**

The following command configures the polling interval to 600 seconds for session timeout threshold:

```
threshold poll card-temperature-near-power-off-limit interval 600
```
threshold poll cdr-file-space interval

Configures the polling interval for Charging Data Record (CDR) File Space Usage threshold.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll cdr-file-space interval duration
default threshold poll cdr-file-space interval
```

- **default**
  Uses the default polling interval.
  Default: 300 seconds

- **interval duration**
  Specifies the polling interval (in seconds) for the CDR File Space Usage threshold.
  `duration` must be an integer from 60 through 60000.

**Usage Guidelines**

This command configures the polling interval for CDR File Space Usage threshold.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshCDRFileSpace` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the CDR file space usage threshold:

```
threshold poll cdr-file-space interval 600
```
threshold poll contfilt-block interval

Configures the polling interval Content Filtering Block threshold.

Product

CF

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description

threshold poll contfilt-block interval duration
default threshold poll contfilt-block interval

default
Uses the default threshold polling interval.
Default: 300 seconds

interval duration
Specifies the polling interval (in seconds) for the Content Filtering Block threshold.
duration must be an integer from 60 through 60000.

Usage Guidelines
This command configures the polling interval Content Filtering Block threshold.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshContFiltBlock` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the content filtering blocking threshold:

```
threshold poll contfilt-block interval 600
```
threshold poll contfilt-rating interval

Configures the polling interval for the Content Filtering Rating threshold.

**Product**

CF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

`threshold poll contfilt-rating interval duration`

`default threshold poll contfilt-rating interval`

`interval dur`

Specifies the polling interval (in seconds) for the Content Filtering Rating threshold. `duration` must be an integer from 60 through 60000.

**Usage Guidelines**

This command configures the polling interval for the Content Filtering Rating threshold.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshContFiltRating` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the content filtering rating processing threshold:

```
threshold poll contfilt-rating interval 600
```
threshold poll cpu-available-memory interval

Configures the polling interval over which to measure the percentage of total packet processing card CPU memory used.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local]host_name(config)#

Syntax Description
threshold poll cpu-available-memory interval duration
default threshold poll cpu-available-memory interval
default
Uses the default threshold polling interval.
Default: 300 seconds
interval dur
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
Important

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshCPUMemory` command in this mode.

Examples

The following command configures the polling interval to 600 seconds for the CPU available memory threshold:

```
threshold poll cpu-available-memory interval 600
```
threshold poll cpu-load interval

Configures the polling interval over which to monitor packet processing card CPU loads using a 5-minute average measurement.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

**Syntax Description**

threshold poll cpu-load interval  *duration*

default threshold poll cpu-load interval

default

Uses the default threshold polling interval.

Default: 300 seconds

interval *dur*

Specifies the amount of time (in seconds) that comprises the polling interval.

*duration* must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshCPULoad` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the CPU load threshold:

```
threshold poll cpu-load interval 600
```
threshold poll cpu-memory-usage interval

Configures the polling interval over which to measure the percentage of total packet processing card CPU memory used.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure
Entering the above command sequence results in the following prompt:

```
[local]\host_name(config)#
```

**Syntax Description**
threshold poll cpu-memory-usage interval *duration*
default threshold poll cpu-memory-usage interval
default
Uses the default threshold polling interval.
Default: 300 seconds

interval *dur*
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

**Usage Guidelines**
This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshCPUMemUsage` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the CPU memory usage threshold:

```
threshold poll cpu-memory-usage interval 600
```
threshold poll cpu-orbs-crit interval

Configures the polling interval over which to measure the percentage of CPU utilization by the ORBS software task for critical-level alerts.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description
threshold poll cpu-orbs-crit interval duration
default threshold poll cpu-orbs-crit interval
default
Uses the default threshold polling interval.
Default: 300 seconds

interval dur
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 60 through 60000.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshCPUOrbsCritical` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the CPU ORBS critical threshold:

```
threshold poll cpu-orbs-crit interval 600
```
threshold poll cpu-orbs-warn interval

Configures the polling interval over which to measure the percentage of CPU utilization by the ORBS software task for warning-level alerts.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name(config) #

Syntax Description

threshold poll cpu-orbs-warn interval duration
default threshold poll cpu-orbs-warn interval
default

Uses the default threshold polling interval.
Default: 300 seconds

interval dur

Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 60 through 60000.

Usage Guidelines

This command sets the time period over which to monitor the specified value for threshold crossing.

Important

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshCPUOrbsWarn` command in this mode.

**Examples**
The following command configures the polling interval to 600 seconds for the CPU ORBS warning threshold:
`threshold poll cpu-orbs-warn interval 600`
threshold poll cpu-session-throughput interval

Configures the polling interval over which to measure total throughput for all Session Manager tasks running on each packet processing card CPU.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`threshold poll cpu-session-throughput interval duration`

`default threshold poll cpu-session-throughput interval`

- **default**
  
  Uses the default threshold polling interval.
  
  Default: 300 seconds

- **interval dur**
  
  Specifies the amount of time (in seconds) that comprises the polling interval.
  
  `duration` must be an integer from 60 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` `ThreshSessCPUThroughput` command in this mode.

### Examples

The following command configures the polling interval to 600 seconds for the CPU session throughput threshold:

```
threshold poll cpu-session-throughput interval 600
```
threshold poll cpu-utilization interval

Configures the polling interval over which to measure the percentage of CPU utilization.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```plaintext
threshold poll cpu-utilization interval duration
default threshold poll cpu-utilization interval
default
interval dur
```

- **default**
  Uses the default threshold polling interval.
  Default: 300 seconds

- **interval dur**
  Specifies the amount of time (in seconds) that comprises the polling interval.
  `duration` must be an integer from 60 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshCPUUtilization` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the CPU utilization threshold:

```
threshold poll cpu-utilization interval 600
```
**threshold poll dcca-bad-answers interval**

Configures the polling interval for DCCA Bad Answers threshold—invalid or bad response to the system from the Diameter server.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
```
threshold poll dcca-bad-answers interval duration
default threshold poll dcca-bad-answers interval
```

- **default**
  Uses the default threshold polling interval.
  Default: 900 seconds

- **interval duration**
  Specifies the polling interval (in seconds) for the DCCA Bad Answers threshold.
  `duration` must be an integer from 60 through 60000.

**Usage Guidelines**

This command configures the polling interval for DCCA Bad Answers threshold.

---

**Important**
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system's support for thresholding in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` `ThreshDCCABadAnswers` command in this mode.

Examples

The following command configures the polling interval to 600 seconds for invalid or bad response threshold to the system from Diameter server:

```
threshold poll dcca-rating-failed interval 600
```
threshold poll dcca-protocol-error interval

Configures the polling interval for Diameter Credit-Control Application (DCCA) Protocol Error threshold.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local]host_name(config)#

Syntax Description
threshold poll dcca-protocol-error interval duration
default threshold poll dcca-protocol-error interval

default
Uses the default threshold polling interval.
Default: 900 seconds

interval duration
Specifies the polling interval (in seconds) for the DCCA Protocol Error threshold.
duration must be an integer from 60 through 6000.

Usage Guidelines
Use this the polling interval for DCCA Protocol Error threshold.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholding in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshDCCAProtocolError` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the DCCA protocol error threshold:

`threshold poll dcca-protocol-error interval 600`
threshold poll dcca-rating-failed interval

Configures the polling interval for Diameter Credit-Control Application (DCCA) Rating Failed threshold.

Product

ACS

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

threshold poll dcca-rating-failed interval duration
default threshold poll dcca-rating-failed interval

default
Uses the default polling interval.
Default: 900 seconds

interval duration
Specifies the polling interval (in seconds) for the DCCA Rating Failed threshold.
duration must be an integer from 60 through 60000.

Usage Guidelines

This command configures the polling interval for DCCA Rating Failed threshold.

Important

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholding in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshDCCARatingFailed` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the Diameter Credit Control Application (DCCA) Rating Group (content-id) request reject thresholds:

```
threshold poll dcca-rating-failed interval 600
```
threshold poll dcca-unknown-rating-group interval

Configures the polling interval for Diameter Credit-Control Application (DCCA) Unknown Rating Group threshold.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local] host_name (config) #

Syntax Description
threshold poll dcca-unknown-rating-group interval duration
default threshold poll dcca-unknown-rating-group interval

default
Uses the default polling interval.
Default: 900 seconds

interval duration
Specifies duration (in seconds) for the DCCA Unknown Rating Group threshold.
duration must be an integer from 60 through 60000.

Usage Guidelines
This command configures the polling interval for DCCA Unknown Rating Group threshold.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholding in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshDCCAUnknownRatingGroup` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds to threshold for the unknown DCCA Rating Group (content-id) returned by Diameter to system:

```
threshold poll dcca-unknown-rating-group interval 600
```
threshold poll dereg-reply-error interval

Configures the polling interval to count the number of de-registration reply errors per HA service.

Product
HA

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description
threshold poll dereg-reply-error interval duration

default threshold poll dereg-reply-error interval

default
Uses the default polling interval.
Default: 300 seconds

interval duration
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 60 through 60000. The input will be rounded up to the closest multiple of 30.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands in this chapter for additional information on the system's support for thresholding.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` 
`ThreshHASvcDeregReplyError` command in this mode.

**Examples**

The following command configures the HA de-registration reply error threshold polling interval to 600 seconds:

```
threshold poll dereg-reply-error interval 600
```
### threshold poll diameter-retry-rate interval

Configures the polling interval for the Diameter Credit-Control Application (DCCA) Diameter Retry Rate threshold.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

```
[local]\host_name(config)#
```

**Syntax Description**

- `threshold poll diameter-retry-rate interval duration`
- `default threshold poll diameter-retry-rate interval`

**default**

Uses the default polling interval.

Default: 300 seconds

**interval duration**

Specifies the polling interval (in seconds) for the Diameter Retry Rate threshold.

`duration` must be an integer from 60 through 60000. The input will be rounded up to the closest multiple of 30.

**Usage Guidelines**

This command specifies the polling interval for Diameter Retry Rate threshold.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands in this chapter for additional information on the system's support for thresholding.
Important

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshDiameterRetryRate` command in this mode.

Examples

The following command configures the Diameter Retry Rate threshold polling interval to 600 seconds:

```
threshold poll diameter-retry-rate interval 600
```
threshold poll disconnect-reason

Configures alarm and clear thresholds based on the number of specified disconnects on a chassis.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[l-local]host_name(config)#

Syntax Description
| default |threshold poll disconnect-reason| disc-reason_name| polling_interval_seconds|

default
Restores the threshold polling interval to 900 seconds (15 minutes).

disc-reason_name

disc-reason_name must be an alphanumeric string of 1 through 47 characters.
Enter the disc-reason name exactly as shown in the Statistics and Counters Reference or the output of the show session disconnect-reasons verbose command. Do not include the number assigned to the disconnect reason shown in parentheses "(nnn)" at the end of the name.

polling_interval_seconds
Default: 300 seconds.
polling_interval_seconds must be an integer from 300 to 6,000. Configures the threshold polling interval in seconds.

Important
The operator can configure a maximum of 30 disconnect reasons for monitoring. When a disconnect reason crosses the threshold, a trap is generated and corrective actions are taken.

Usage Guidelines
Use this command to configure alarm and clear thresholds based on the number of specified disconnects on a chassis.
If a specific disconnect-reason crosses a set limit of threshold, this feature provides the operator the ability to see alarms and react to potential network events in a more timely manner. This feature now allows an operator the ability to configure thresholds (percentage) for all disconnect reasons (600+) using the show disconnect CLI command. This will display the disconnect reason as well as the threshold set for that particular disconnect reason. Once a threshold is exceeded, an alarm is generated. Approximately 30 (maximum) disconnect reasons can be configured at any time.

**Important**  
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

**Examples**  
The following command configures threshold polling interval for admin-disconnect to 900:

```
threshold disconnect-reason admin-disconnect interval 900
```
threshold poll edr-file-space interval

Command configures the polling interval for Event Data Record (EDR) File Space Usage threshold.

Product
ACS

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description
threshold poll edr-file-space interval duration

interval duration
Default: 300 seconds.
Specifies the polling interval (in seconds) for the EDR File Space Usage threshold.
duration must be an integer from 60 through 60000.

Usage Guidelines
This command configures the polling interval for EDR File Space Usage threshold.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

Important
To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshEDRFileSpace command in this mode.

Examples
The following command configures the polling interval to 600 seconds for the EDR file space usage threshold:

threshold poll edr-file-space interval 600
threshold poll edr-udr-dropped-flow-control interval

Configures the polling interval to count the total number of Event Data Records (EDRs) and Usage Data Records (UDRs) discarded due to ACSMGR flow control.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**
threshold poll edr-udr-dropped-flow-control interval *duration*

interval *duration*

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

*duration* must be an integer from 60 through 60000.

**Usage Guidelines**
This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

**Examples**
The following command configures the polling interval to 600 seconds for the EDR/UDR drops due to flow control threshold:

`threshold poll edr-udr-dropped-flow-control interval 600`
threshold poll epdg-current-sessions interval

Configures the polling interval to count the total number of subscribers currently in Evolved Packet Date Gateway (ePDG) sessions.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

*configure*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll epdg-current-sessions interval duration
```

interval `duration`

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

`duration` must be an integer from 60 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshEPDGCurrSess` command in this mode.
Examples

The following command configures the polling interval to 600 seconds for the ePDG sessions threshold:

```
threshold poll epdg-current-sessions interval 600
```
threshold poll epdg-ikev2-authentication-failures

Configures threshold polling interval for IKEv2 Authentication Failures per ePDG service.

Product  ePDG

Privilege  Security Administrator, Administrator

Command Modes  Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

Syntax Description  | default | threshold poll epdg-ikev2-authentication-failures interval interval

default

Sets / Restores default value assigned for threshold polling interval for IKEv2 Authentication Failures per ePDG service.

interval interval

Configures threshold polling interval in seconds.

interval is an integer from 60 through 60000.

Usage Guidelines  Use this command to configure threshold polling interval for IKEv2 Authentication Failures per ePDG service.

Examples  The following command configures threshold polling interval as 75 seconds for IKEv2 Authentication Failures per ePDG service.

threshold poll epdg-ikev2-authentication-failures interval 75
threshold poll epdg-ikev2-setup-attempts

Configures threshold polling interval for IKEv2 Setup Attempts per ePDG service.

**Product**
ePDG

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

**configure**
Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ default ] threshold poll epdg-ikev2-setup-attempts interval interval
```

*default*
Sets / Restores default value assigned for threshold polling interval for IKEv2 Setup Attempts per ePDG service.

*interval interval*
Configures threshold polling interval in seconds.

*interval* is an integer from 60 through 60000.

**Usage Guidelines**
Use this command to configure threshold polling interval for IKEv2 Setup Attempts per ePDG service.

**Examples**
The following command configures threshold polling interval as 65 seconds for IKEv2 Setup Attempts per ePDG service.

```
threshold poll epdg-ikev2-setup-attempts interval 65
```
**threshold poll epdg-ikev2-setup-failure**

Configures threshold polling interval for IKEv2 Setup Failure per ePDG service.

**Product**
ePDG

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
| default | threshold poll epdg-ikev2-setup-failure interval interval |
```

**default**
Sets / Restores default value assigned for threshold polling interval for IKEv2 Setup Failure per ePDG service.

**interval interval**
Configures threshold polling interval in seconds.

**Usage Guidelines**
Use this command to configure threshold polling interval for IKEv2 Setup Failure per ePDG service.

**Examples**
The following command configures threshold polling interval as 90 seconds for IKEv2 Setup Failure per ePDG service.

```
threshold poll epdg-ikev2-setup-failure 90
```
threshold poll epdg-ikev2-setup-failure-rate

Configures threshold polling interval for IKEv2 Setup Failure Rate per ePDG service.

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

**Command Modes**

Exec > Global Configuration

```bash
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

<table>
<thead>
<tr>
<th>default</th>
<th>threshold poll epdg-ikev2-setup-failure-rate interval</th>
<th>interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Sets / Restores default value assigned for threshold polling interval for IKEv2 Setup Failure Rate per ePDG service.</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to configure threshold polling interval for IKEv2 Setup Failure Rate per ePDG service.

**Examples**

The following command configures threshold polling interval as 900 seconds for IKEv2 Setup Failure Rate per ePDG service.

```
threshold poll epdg-ikev2-setup-failure-rate 900
```
threshold poll epdg-ikev2-setup-success

Configures threshold polling interval for IKEv2 Setup Success per ePDG service.

**Product**
ePDG

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
| default | threshold poll epdg-ikev2-setup-success interval interval |
```

- **default**
  
  Sets / Restores default value assigned for threshold polling interval for IKEv2 Setup Success per ePDG service.

- **interval interval**
  
  Configures threshold polling interval in seconds.
  
  *interval* is the integer between 60 and 60000.

**Usage Guidelines**

Use this command to configure threshold polling interval for IKEv2 Setup Success per ePDG service.

**Examples**

The following command configures threshold polling interval as 600 seconds for IKEv2 Setup Success per ePDG service.

```
threshold poll epdg-ikev2-setup-success 600
```
**threshold poll fa-reg-reply-error interval**

Configures the polling interval over which to measure the number of registration reply errors for Foreign Agent (FA) services.

**Product**
FA

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
```
threshold poll fa-reg-reply-error interval duration
```

- **interval** duration
  - Default: 0 seconds.
  - Specifies the amount of time (in seconds) that comprises the polling interval.
  - duration must be an integer from 60 through 60000.

**Usage Guidelines**
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

**Important**
To enable an SNMP trap for monitoring this threshold use the **snmp trap enable**
**ThreshFASvcRegReplyError** command in this mode.
Examples

The following command configures the polling interval to 600 seconds for the FA registration reply errors threshold:

`threshold poll fa-reg-reply-error interval 600`
threshold poll fng-current-active-sessions interval

Configures the polling interval in seconds over which to count Femto Network Gateway (FNG) current active sessions.

**Product**
FNG

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll fng-current-active-sessions interval duration
```

- **interval duration**
- Default: 0 seconds.
- Specifies the amount of time (in seconds) that comprises the polling interval.
- `duration` must be an integer from 60 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshFNGCurrActSess` command in this mode.
The following command configures the polling interval to 600 seconds for the FNG current active sessions threshold:

```
threshold poll fng-current-active-sessions interval 600
```
**threshold poll fng-current-sessions interval**

Configures the polling interval in seconds over which to count Femto Network Gateway (FNG) current sessions, including inactive sessions.

**Product**
FNG

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_{name}{config}#

**Syntax Description**

```
threshold poll fng-current-sessions interval duration
```

- **interval duration**

  Default: 0 seconds.
  Specifies the amount of time (in seconds) that comprises the polling interval.
  *duration* must be an integer from 60 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the *snmp trap enable ThreshFNGCurrSess* command in this mode.
Examples

The following command configures the polling interval to 600 seconds for the FNG current sessions threshold:

```plaintext
threshold poll fng-current-sessions interval 600
```
threshold poll fw-deny-rule interval

Configures the Stateful Firewall Deny Rule threshold polling interval.

Product
PSF

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local] host_name(config)#

Syntax Description
threshold poll fw-deny-rule interval duration

interval duration
Default: 900 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 60 through 900.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshFWDenyRule command in this mode.
Examples

The following command configures the polling interval to 600 seconds for the Stateful Firewall Deny Rule threshold:

```
threshold poll fw-deny-rule interval 600
```
**threshold poll fw-dos-attack interval**

Configures the Stateful Firewall Denial of Service (DoS) Attacks threshold polling interval.

**Product**

PSF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`threshold poll fw-dos-attack interval duration`

- `interval duration`
  
  Default: 900 seconds.
  
  Specifies the amount of time (in seconds) that comprises the polling interval.
  
  `duration` must be an integer from 60 through 900.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system's support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshFWDosAttack` command in this mode.
Examples

The following command configures the polling interval to 600 seconds for the Stateful Firewall DoS Attacks threshold:

```
threshold poll fw-dos-attack interval 600
```
threshold poll fw-drop-packet interval

Configures the Stateful Firewall Drop-Packet threshold polling interval.

Product

PSF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]<host_name>(config)#

Syntax Description

threshold poll fw-drop-packet interval duration

interval duration

Default: 900 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

duration must be an integer from 60 through 900.

Usage Guidelines

This command sets the time period over which to monitor the specified value for threshold crossing.

Important

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

Important

To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshFWDropPacket command in this mode.
Examples

The following command configures the polling interval to 600 seconds for the Stateful Firewall Drop-Packet threshold:

```
threshold poll fw-drop-packet interval 600
```
**threshold poll fw-no-rule interval**

Configures the Stateful Firewall No-Rule threshold polling interval.

**Product**

PSF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

```bash
configure
```

Entering the above command sequence results in the following prompt:

```bash
[local] host_name(config)#
```

**Syntax Description**

`threshold poll fw-no-rule interval duration`

- `interval duration`

  Default: 900 seconds.

  Specifies the amount of time (in seconds) that comprises the polling interval.

  `duration` must be an integer from 60 through 900.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshFWNoRule` command in this mode.
threshold poll fw-no-rule interval

**Examples**

The following command configures the polling interval to 600 seconds for the Stateful Firewall No-Rule threshold:

```
threshold poll fw-no-rule interval 600
```
threshold poll ha-init-rrq-rcvd-rate interval

Configures the polling interval for Home Agent (HA) service over which to measure the average number of calls setup per minute.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

Syntax Description

threshold poll ha-init-rrq-rcvd-rate interval duration

interval duration
Default: 0 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 60 through 900.

Usage Guidelines

This command sets the time period over which to monitor the specified value for threshold crossing.

Important

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

Important

To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshHACallSetupRate command in this mode.
threshold poll ha-init-rrq-rcvd-rate interval

**Examples**

The following command configures the polling interval to 600 seconds for the average number of HA calls setup per minute:

```
threshold poll ha-init-rrq-rcvd-rate interval 600
```
threshold poll ha-svc-init-rrq-rcvd-rate interval

Configures the polling interval over which to measure the average number of calls setup per minute for HA services.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

threshold poll ha-svc-init-rrq-rcvd-rate interval duration

*interval duration*

Default: 0 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

duration must be an integer from 60 through 900.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThresholdHASvcCallSetupRate command in this mode.
Examples

The following command configures the polling interval to 600 seconds for the average number of calls setup per minute for HA services:

```
threshold poll ha-svc-init-rrq-rcvd-rate interval 600
```
threshold poll henbgw-paging-messages interval

Configures how frequently the HeNBGW paging messages are polled.

**Product**

HeNBGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`threshold poll henbgw-paging-messages interval duration`

- **interval duration**
  - Default: 0 seconds.
  - Specifies the amount of time (in seconds) that comprises the polling interval.
  - `duration` must be an integer from 30 through 6000.

**Usage Guidelines**

This command configures how frequently the HeNB-GW paging messages are polled.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system's support for thresholds in this chapter.

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThresholdHeNBGW PagingMessages` command in this mode.

**Examples**

The following command configures the polling interval to 6000 seconds for the HeNB-GW service:

```
threshold poll henbgw-paging-messages interval 6000
```
threshold poll ip-pool-free interval

Configures the polling interval over which to measure the percentage of the IP pool addresses that are in the Free state.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll ip-pool-free interval duration
```

*interval duration*

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

*duration* must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system's support for thresholds in this chapter.

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshIPPoolFree` command in this mode.
Examples

The following command configures the polling interval to 600 seconds for the average number of Free IP pools:

```
threshold poll ip-pool-free interval interval 600
```
threshold poll ip-pool-hold interval

Configures the polling interval over which to measure the percentage of the IP pool addresses that are in the Hold state.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description

threshold poll ip-pool-hold interval duration

interval duration

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

duration must be an integer from 30 through 60000.

Usage Guidelines

This command sets the time period over which to monitor the specified value for threshold crossing.

Important

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

Important

To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshIPPoolHold command in this mode.
Examples

The following command configures the polling interval to 600 seconds for the average number of IP pool addresses in Hold state:

```
threshold poll ip-pool-hold interval 600
```
threshold poll ip-pool-release interval

Configures the polling interval over which to measure the percentage of IP pool addresses that are in the Release state.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local]host_name(config)#

Syntax Description

threshold poll ip-pool-release interval duration

interval duration
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 6000.

Usage Guidelines

This command sets the time period over which to monitor the specified value for threshold crossing.

Important

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

Important

To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshIPPoolRelease command in this mode.
Examples

The following command configures the polling interval to 600 seconds for the average number of IP pool addresses in Release state:

```
threshold poll ip-pool-release interval 600
```
threshold poll ip-pool-used interval

Configures the polling interval over which to measure the percentage of the IP pool addresses that are used.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

**Syntax Description**

threshold poll ip-pool-used interval duration

interval duration

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

duration must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

**Important**

To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshIPPoolUsed command in this mode.
Examples

The following command configures the polling interval to 600 seconds for the average number of used IP pool addresses:

```plaintext
threshold poll ip-pool-used interval 600
```
threshold poll ipsec-call-req-rej interval

Configures the polling interval over which to count the IPSec call requests that are rejected.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```bash
configure
```

Entering the above command sequence results in the following prompt:

```bash
[local]host_name(config)#
```

**Syntax Description**

```bash
threshold poll ipsec-call-req-rej interval duration
```

**interval duration**

Default: 900 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

*duration* must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshIPSECCallReqRej` command in this mode.
Examples

The following command configures the polling interval to 600 seconds for the average number of rejected IPSec IKE calls:

```
threshold poll ipsec-call-req-rej interval 600
```
threshold poll ipsec-ike-failrate interval

Configures the polling interval over which to count the IPSec IKE failure rate.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local]host_name(config)#

**Syntax Description**
threshold poll ipsec-ike-failrate interval *duration*

interval *duration*
Default: 900 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.
*duration* must be an integer from 30 through 60000.

**Usage Guidelines**
This command sets the time period over which to monitor the specified value for threshold crossing.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.</td>
</tr>
</tbody>
</table>

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>To enable an SNMP trap for monitoring this threshold use the <strong>snmp trap enable ThreshIPSECIKEFailRate</strong> command in this mode.</td>
</tr>
</tbody>
</table>
Examples

The following command configures the polling interval to 600 seconds for the average rate for IPSec IKE failures:

threshold poll ipsec-ike-failrate interval 600
threshold poll ipsec-ike-failures interval

Configures the polling interval over which to count the number of IPSec IKE failures.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

**Syntax Description**

threshold poll ipsec-ike-failures interval *duration*

interval *duration*

Default: 900 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

*duration* must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshIPSECIKEFailures` command in this mode.
Examples

The following command configures the polling interval to 600 seconds for the average number of IPSec IKE failures:

```
threshold poll ipsec-ike-failures interval 600
```
threshold poll ipsec-ike-requests interval

Configures the polling interval over which to count the number of IPSec IKE requests.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

threshold poll ipsec-ike-requests interval `duration`

`interval duration`

Default: 900 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

`duration` must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshIPSECIKERequests` command in this mode.
Examples

The following command configures the polling interval to 600 seconds for the average number of IPSec call requests:

```
threshold poll ipsec-ike-requests interval 600
```
threshold poll ipsec-tunnels-established interval

Configures the polling interval over which to count the number of IPSec tunnels that have been established.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

Syntax Description
threshold poll ipsec-tunnels-established interval duration

interval duration
Default: 900 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important
To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThresholdIPSEC TunnelEstablished command in this mode.
Examples

The following command configures the polling interval to 600 seconds for the number of established IPSec tunnels:

```
threshold poll ipsec-tunnels-established interval 600
```
threshold poll ipsec-tunnels-setup interval

Configures the polling interval over which to count the number of IPSec tunnels that have been setup.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local]host_name(config)#

Syntax Description
threshold poll ipsec-tunnels-setup interval duration

interval duration
Default: 900 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

Important
To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshIPSECTunSetup command in this mode.
Examples

The following command configures the polling interval to 600 seconds for the number of IPSec tunnels that have been setup:

```
threshold poll ipsec-tunnels-setup interval 600
```
**threshold poll license-remaining-session interval**

Configures the polling interval over which to measure session license utilization.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`threshold poll license-remaining-session interval duration`

`interval duration`

Default: 900 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

`duration` must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshLicense` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for the utilization of session licenses:

`threshold poll license-remaining-session interval 600`
threshold poll mgmt-cpu-memory-usage interval

Configures the polling interval over which to measure management card CPU memory usage.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`threshold poll mgmt-cpu-memory-usage interval duration`

`interval duration`

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

`duration` must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

**Examples**

The following command configures the polling interval to 600 seconds for management card CPU memory usage:

`threshold poll mgmt-cpu-memory-usage interval 600`
threshold poll mgmt-cpu-utilization interval

Configures the polling interval over which to measure management card CPU utilization.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll mgmt-cpu-utilization interval duration
```

**interval duration**

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

**Examples**

The following command configures the polling interval to 600 seconds for management card CPU memory usage:

```
threshold poll mgmt-cpu-utilization interval 600
```
threshold poll mme-attach-failure interval

Configures the polling interval to count the MME Attach Failure messages across all MME services in the system.

**Product**

MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]\host_name\(config)#

**Syntax Description**

threshold poll mme-attach-failure interval *dur*

default threshold poll mme-attach-failure interval

default

Restores the polling interval value to its default value of 900 seconds.

interval *dur*

Default: 900 seconds.

Specifies the polling interval (in seconds) for counting MME Attach Failure messages across all MME services in the system.

*dur* must be an integer from 30 through 60000 in multiples of 30.

**Usage Guidelines**

Use this command to configure the polling interval to count the MME Attach Failure messages across all MME services in the system to generate threshold value.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring mme-service and other threshold commands for additional information on the system’s support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshMMEAttachFail` command in this mode.

**Examples**

The following command configures the polling interval of 600 seconds to count the MME Attach Failure messages for threshold limit:

```
threshold poll mme-attach-failure interval 600
```
threshold poll mme-auth-failure interval

Configures the polling interval to count the MME Authentication Failure messages across all MME services in the system.

**Product**

MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

threshold poll mme-auth-failure interval \( dur \)

default threshold poll mme-auth-failure interval

default

Restores the specified poll interval value to its default value of 900 seconds.

interval \( dur \)

Default: 900 seconds.

Specifies the polling interval (in seconds) for counting MME Authentication Failure messages across all MME services in the system.

\( dur \) must be an integer from 30 through 60000 in multiples of 30.

**Usage Guidelines**

Use this command to configure the polling interval to count the MME Auth Failure messages across all MME services in the system to generate threshold value.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring mme-service and other threshold commands for additional information on the system’s support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshMMEAuthFail` command in this mode.

**Examples**

The following command configures the polling interval of 600 seconds to count the MME Auth Failure messages for threshold limit:

```
threshold poll mme-auth-failure interval 600
```
threshold poll nat-pkt-drop

Configures the polling interval over which to measure the percentage of Network Address Translation (NAT) packet drops.

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

threshold poll nat-pkt-drop interval duration
default threshold poll nat-pkt-drop interval

default
Restores the specified poll interval value to its default value of 900 seconds.

interval duration
Specifies the amount of time (in seconds) that comprises the polling interval.

duration must be an integer from 30 through 60000.

Default: 900 seconds.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**
The configured polling interval will be rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable [ ThreshNATPktDrop | ThreshclearNATPktDrop ]` command in this mode.

**Examples**

The following command configures the polling interval to 500 seconds for NAT packet drops:
```
threshold poll nat-pkt-drop interval 500
```
threshold poll nat-port-chunks-usage interval

Configures the polling interval over which to measure the percentage of Network Address Translation (NAT) port chunk utilization.

**Product**

NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

threshold poll nat-port-chunks-usage interval *duration*

default threshold poll nat-port-chunks-usage interval

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.
To enable an SNMP trap for monitoring this threshold use the **snmp trap enable** command in this mode.

### Examples

The following command configures the polling interval to 600 seconds for (NAT) port chunk utilization:

```
threshold poll nat-port-chunks-usage interval 600
```
threshold poll npu-utilization interval

Configures the polling interval over which to measure the percentage of network processing unit (NPU) utilization.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

threshold poll npu-utilization interval duration

interval duration

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

duration must be an integer from 30 through 60000.

Usage Guidelines

This command sets the time period over which to monitor the specified value for threshold crossing.

Important

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

Important

To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshNPUUtilization command in this mode.
Examples

The following command configures the polling interval to 600 seconds for NPU utilization:

```
threshold poll npu-utilization interval 600
```
Global Configuration Mode Commands (threshold poll commands O - Z)

The Global Configuration Mode is used to configure basic system-wide parameters.

This section includes the commands `threshold poll packets-filtered-dropped interval` through `threshold poll tpo-rto-timeout`.

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] `host_name` (config) #

Important

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

- `threshold poll packets-filtered-dropped interval`, page 778
- `threshold poll packets-forwarded-to-cpu interval`, page 779
- `threshold poll pdg-current-active-sessions interval`, page 781
- `threshold poll pdg-current-sessions interval`, page 783
- `threshold poll pdif-current-active-sessions interval`, page 785
- `threshold poll pdif-current-sessions interval`, page 787
- `threshold poll pdsn-init-rrq-rcvd-rate interval`, page 789
- `threshold poll pdsn-svc-init-rrq-rcvd-rate interval`, page 791
- `threshold poll per-service-asngw-sessions interval`, page 793
- `threshold poll per-service-ggsn-sessions interval`, page 795
- `threshold poll per-service-gprs-pdp-sessions interval`, page 797
• threshold poll per-service-gprs-sessions interval, page 799
• threshold poll per-service-ha-sessions interval, page 801
• threshold poll per-service-lns-sessions interval, page 803
• threshold poll per-service-pdg-sessions interval, page 805
• threshold poll per-service-pdsn-sessions interval, page 807
• threshold poll per-service-samog-sessions interval, page 809
• threshold poll per-service-sgsn-pdp-sessions interval, page 811
• threshold poll per-service-sgsn-sessions interval, page 813
• threshold poll phsgw-auth-failure interval, page 815
• threshold poll phsgw-eapol-auth-failure interval, page 817
• threshold poll phsgw-handoff-denial interval, page 819
• threshold poll phsgw-max-eap-retry interval, page 820
• threshold poll phsgw-max-eapol-retry interval, page 822
• threshold poll phsgw-network-entry-denial interval, page 824
• threshold poll phsgw-session-setup-timeout interval, page 825
• threshold poll phsgw-session-timeout interval, page 827
• threshold poll phspc-session-setup-timeout interval, page 829
• threshold poll phspc-sleep-mode-timeout interval, page 831
• threshold poll phspc-sm-entry-denial interval, page 833
• threshold poll port-high-activity interval, page 835
• threshold poll port-rx-utilization interval, page 837
• threshold poll port-tx-utilization, page 839
• threshold poll ppp-setup-fail-rate interval, page 841
• threshold poll reg-reply-error interval, page 843
• threshold poll rereg-reply-error interval, page 845
• threshold poll route-service interval, page 846
• threshold poll rp-setup-fail-rate interval, page 848
• threshold poll sess-flow-count interval, page 850
• threshold poll storage-utilization interval, page 851
• threshold poll system-capacity interval, page 853
• threshold poll total-asngw-sessions interval, page 855
• threshold poll total-ggsn-sessions interval, page 857
• threshold poll total-gprs-pdp-sessions interval, page 859
• threshold poll total-gprs-sessions interval, page 861
• threshold poll total-ha-sessions interval, page 863
• threshold poll total-henbgw-henb-sessions, page 865
• threshold poll total-henbgw-ue-sessions, page 867
• threshold poll total-hnbgw-hnb-sessions, page 869
• threshold poll total-hnbgw-ue-sessions, page 871
• threshold poll total-hnbgw-iu-sessions, page 873
• threshold poll total-hsgw-sessions interval, page 875
• threshold poll total-lma-sessions interval, page 877
• threshold poll total-lns-sessions interval, page 879
• threshold poll total-mme-sessions, page 881
• threshold poll total-pdsn-sessions interval, page 883
• threshold poll total-pgw-sessions interval, page 885
• threshold poll total-saegw-sessions interval, page 887
• threshold poll total-sgsn-pdp-sessions interval, page 889
• threshold poll total-sgsn-sessions interval, page 891
• threshold poll total-sgw-sessions interval, page 893
• threshold poll total-subscriber interval, page 895
threshold poll packets-filtered-dropped interval

Configures the polling interval over which to count the filtered/dropped packets.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll packets-filtered-dropped interval duration
```

**interval duration**

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

*duration* must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPacketsFilteredDropped` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds for filtered/dropped packets:

```
threshold poll packets-filtered-dropped interval 600
```
**threshold poll packets-forwarded-to-cpu interval**

Configures the polling interval over which to count packets forwarded to active system CPUs in the system.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

**Syntax Description**

```
threshold poll packets-forwarded-to-cpu interval duration
```

**interval duration**

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

`duration` must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPacketsForwarded` command in this mode.
Examples

The following command configures the polling interval to 600 seconds for packets forwarded to active system CPUs in the system:

```
threshold poll packets-forwarded-to-cpu interval 600
```
threshold poll pdg-current-active-sessions interval

Configures the polling interval over which to count the total number of currently active Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG) sessions.

**Product**
- PDG
- TTG

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration
  - configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll pdg-current-active-sessions interval duration
```

- **interval duration**
  - Default: 300 seconds.
  - Specifies the amount of time (in seconds) that comprises the polling interval.
  - `duration` must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPDGCurrActSess` command in this mode.
Examples

The following command configures the polling interval to 600 seconds for PDG/TTG sessions:

```
threshold poll pdg-current-active-sessions interval 600
```
threshold poll pdg-current-sessions interval

Configures the polling interval over which to count the total number of current Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG) sessions, including inactive sessions.

**Product**

PDG/TTG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

*configure*

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

`threshold poll pdg-current-sessions interval duration`

**interval duration**

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval. `duration` must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPDGCurrSess` command in this mode.
The following command configures the polling interval to 600 seconds for PDG/TTG sessions:

```
threshold poll pdg-current-sessions interval 600
```
threshold poll pdif-current-active-sessions interval

Configures the polling interval over which to count the total number of currently active Packet Data Interworking Function (PDIF) sessions.

**Product**

PDIF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

`threshold poll pdif-current-active-sessions interval duration`

`interval duration`

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

`duration` must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPDIFCurrActSess` command in this mode.
Examples

The following command configures the polling interval to 600 seconds for PDIF sessions:
threshold poll pdif-current-active-sessions interval 600
threshold poll pdif-current-sessions interval

Configures the polling interval over which to count the total number of current Packet Data Interworking Function (PDIF) sessions, including inactive sessions.

Product
PDIF

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description
threshold poll pdif-current-sessions interval duration

interval duration
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

Important
To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshPDIFCurrSess command in this mode.
Examples

The following command configures the polling interval to 600 seconds for PDIF sessions:

```
threshold poll pdif-current-sessions interval 600
```
threshold poll pdsn-init-rrq-rcvd-rate interval

Configures the polling interval over which to count the total number of current Packet Data Serving Node (PDSN) sessions, including inactive sessions.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

**Syntax Description**

threshold poll pdsn-init-rrq-rcvd-rate interval duration

interval duration

Default: 0 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

duration must be an integer from 60 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

**Important**

To enable an SNMP trap for monitoring this threshold use the snmp trap enable

ThreshPDSNCallSetupRate command in this mode.
The following command configures the polling interval to 600 seconds for PDSN sessions:
\[ \text{threshold poll pdsn-init-rrq-rcvd-rate interval 600} \]
threshold poll pdsn-svc-init-rrq-rcvd-rate interval

Configures the polling interval over which to count the total number of current Packet Data Serving Node (PDSN) sessions, including inactive sessions.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll pdsn-svc-init-rrq-rcvd-rate interval duration
```

**interval duration**

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

*duration* must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the **snmp trap enable ThreshPDSNSvcCallSetupRate** command in this mode.
Examples

The following command configures the polling interval to 600 seconds for PDSN sessions:

```
threshold poll pdsn-svc-init-rrq-rcvd-rate interval 600
```
threshold poll per-service-asngw-sessions interval

Configures the polling interval in seconds over which to count the number of PDP contexts per ASN-GW service in the system.

**Product**

ASN-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

threshold poll per-service-asngw-sessions interval duration

interval duration

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

duration must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the **snmp trap enable ThreshPerServiceASNGWSessions** command in this mode.
The following command configures the polling interval to 600 seconds for ASN-GW sessions:

```plaintext
threshold poll per-service-asngw-sessions interval 600
```
**threshold poll per-service-ggsn-sessions interval**

Configures the polling interval in seconds over which to count the number of PDP contexts per GGSN service in the system.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll per-service-ggsn-sessions interval duration
```

*interval duration*

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

`duration` must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPerServiceGGSNSessions` command in this mode.
Examples

The following command configures the polling interval to 600 seconds for GGSN sessions:

```
threshold poll per-service-ggsn-sessions interval 600
```
 threshold poll per-service-gprs-pdp-sessions interval

Configures the polling interval in seconds over which to count the number of 2G-activated PDP contexts per GPRS service.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

threshold poll per-service-gprs-pdp-sessions interval duration

interval duration
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

Usage Guidelines

This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

Important
To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshPerServiceGPRSPDPSessions command in this mode.
threshold poll per-service-gprs-pdp-sessions interval

**Examples**
The following command configures the polling interval to 600 seconds for 2G PDP contexts:

```
threshold poll per-service-gprs-pdp-sessions interval 600
```
**threshold poll per-service-gprs-sessions interval**

Configures the polling interval in seconds over which to count the number of 2G-attached subscribers per GPRS service.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`threshold poll per-service-gprs-sessions interval duration`

* `interval duration`
  Default: 300 seconds.
  Specifies the amount of time (in seconds) that comprises the polling interval.
  `duration` must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system's support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPerServiceGPRSSessions` command in this mode.
Examples

The following command configures the polling interval to 600 seconds for 2G GPRS sessions:

```
threshold poll per-service-gprs-sessions interval 600
```
threshold poll per-service-ha-sessions interval

Configures the polling interval in seconds over which to count the number of HA sessions per Home Agent (HA) service in the system.

**Product:** HA

**Privilege:** Security Administrator, Administrator

**Command Modes:**
- Exec > Global Configuration
- configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description:**

```
threshold poll per-service-ha-sessions interval duration
```

- **interval duration**
  - Default: 300 seconds.
  - Specifies the amount of time (in seconds) that comprises the polling interval.
  - `duration` must be an integer from 30 through 60000.

**Usage Guidelines:**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system's support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` `ThreshPerServiceHASessions` command in this mode.
Examples

The following command configures the polling interval to 600 seconds for HA sessions:

```
threshold poll per-service-ha-sessions interval 600
```
threshold poll per-service-lns-sessions interval

Configures the polling interval in seconds over which to count the number of L2TP Network Server (LNS) sessions per LNS service in the system.

Product
LNS

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local] host_name (config) #

Syntax Description
threshold poll per-service-lns-sessions interval duration

interval duration
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

Important
To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshPerServiceLNSSessions command in this mode.
Examples

The following command configures the polling interval to 600 seconds for LNS sessions:

```
threshold poll per-service-lns-sessions interval 600
```
threshold poll per-service-pdg-sessions interval

Configures the polling interval in seconds over which to count the number of Packet Data Gateway (PDG) sessions per PDG/TTG service in the system.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]\host_name\(config)\#

Syntax Description

threshold poll per-service-pdg-sessions interval duration

interval duration

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval. duration must be an integer from 30 through 60000.

Usage Guidelines

This command sets the time period over which to monitor the specified value for threshold crossing.

Important

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

Important

To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshPerServicePDGSessions command in this mode.
Examples

The following command configures the polling interval to 600 seconds for PDG/TTG sessions:

```
threshold poll per-service-pdg-sessions interval 600
```
threshold poll per-service-pdsn-sessions interval

Configures the polling interval in seconds over which to count the number of Packet Data Serving Node (PDSN) sessions per PDSN service in the system.

Product
PDSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description
threshold poll per-service-pdsn-sessions interval duration

interval duration
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

Important
To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshPerServicePDNSessions command in this mode.
Examples

The following command configures the polling interval to 600 seconds for PDSN sessions:

```
threshold poll per-service-pdsn-sessions interval 600
```
threshold poll per-service-samog-sessions interval

Configures the polling interval in seconds over which to count the number of S2a Mobility over GTP (SaMOG) contexts per SaMOG service in the system.

**Product**
SaMOG

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

**Syntax Description**
threshold poll per-service-samog-sessions interval duration

**Usage Guidelines**
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

**Important**
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPerServiceSAMOGSessions` command in this mode.
Examples

The following command configures the polling interval to 600 seconds for SaMOG sessions:

```
threshold poll per-service-samog-sessions interval 600
```
**threshold poll per-service-sgsn-pdp-sessions interval**

Configures the polling interval in seconds over which to count the number of 3G-activated PDP contexts per SGSN service on the system.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll per-service-sgsn-pdp-sessions interval duration
```

*interval duration*

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

`duration` must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPerServiceSGSNPDPSessions` command in this mode.
Examples

The following command configures the polling interval to 600 seconds for 3G PDP contexts:

```
threshold poll per-service-sgsn-pdp-sessions interval 600
```
threshold poll per-service-sgsn-sessions interval

Configures the polling interval in seconds over which to count the number of 3G-attached subscribers per SGSN service in the system.

Product
SGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

threshold poll per-service-sgsn-sessions interval duration

interval duration
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

Important
To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshPerServiceSGSNSessions command in this mode.
Examples

The following command configures the polling interval to 600 seconds for SGSN sessions:

```
threshold poll per-service-sgsn-sessions interval 600
```
threshold poll phsgw-auth-failure interval

Configures the polling interval in seconds over which to count the number of Personal Handyphone System Gateway (PHSGW) authentication failures.

Product
PHSGW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description
threshold poll phsgw-auth-failure interval duration

interval duration
Default: 0 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

Important
To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshPHSGWAuthFail command in this mode.
Examples

The following command configures the polling interval to 600 seconds for PHSGW authentication failures:
```
threshold poll phsgw-auth-failure interval 600
```
threshold poll phsgw-eapol-auth-failure interval

Configures the polling interval in seconds over which to count the number of authentication failures for a PHSGW service using Extensible Authentication Protocol Over LAN (EAPOL).

**Product**

PHSGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`threshold poll phsgw-eapol-auth-failure interval duration`

`interval duration`

Default: 0 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

`duration` must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPHSGWEAPOLAuthFailure` command in this mode.
### Examples

The following command configures the polling interval to 600 seconds for PHSGW EAPOL failures:

```bash
threshold poll phsgw-eapol-auth-failure interval 600
```
threshold poll phsgw-handoff-denial interval

Configures the polling interval in seconds over which to count the number of handoff denials in PHSGW.

**Product**
PHSGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
threshold poll phsgw-handoff-denial interval duration

**interval duration**
Default: 0 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

**Usage Guidelines**
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

**Important**
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPHSGWMaxEAPOLRetry` command in this mode.

**Examples**
The following command configures the polling interval to 600 seconds for PHSGW handoff denials:

```
threshold poll phsgw-handoff-denial interval 600
```
threshold poll phsgw-max-eap-retry interval

Configures the polling interval in seconds over which to count the maximum number of Extensible Authentication Protocol (EAP) retries in PHSGW.

**Product**

PHSGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config) #

**Syntax Description**

threshold poll phsgw-max-eap-retry interval **duration**

interval **duration**

Default: 0 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the **snmp trap enable ThreshPHSGWMaxEAPRetry** command in this mode.
**Examples**

The following command configures the polling interval to 600 seconds for PHSGW EAP retries:

```
threshold poll phsgw-max-eap-retry interval 600
```
**threshold poll phsgw-max-eapol-retry interval**

Configures the polling interval in seconds over which to count the maximum number of Extensible Authentication Protocol Over LAN (EAPOL) retries in PHSGW.

**Product**

PHSGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`threshold poll phsgw-max-eapol-retry interval duration`

- **interval duration**
  - Default: 0 seconds.
  - Specifies the amount of time (in seconds) that comprises the polling interval.
  - `duration` must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPHSGWMaxEAPOLRetry` command in this mode.
Examples

The following command configures the polling interval to 600 seconds for PHSGW EAPOL retries:

```
threshold poll phsgw-max-eapol-retry interval 600
```
threshold poll phsgw-network-entry-denial interval

Configures the polling interval in seconds over which to count the number of network entry denials in PHSGW.

Product
PHSGW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

Syntax Description
threshold poll phsgw-network-entry-denial interval duration

interval duration

Default: 0 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

duration must be an integer from 30 through 60000.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important
To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshPHSGWEntryDenial command in this mode.

Examples
The following command configures the polling interval to 600 seconds for PHSGW network entry denials:

threshold poll phsgw-network-entry-denial interval 600
threshold poll phsgw-session-setup-timeout interval

Configures the polling interval in seconds over which to count the number of PHSGW sessions that timed out during setup.

**Product**
PHSGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]\host_name\(config)#
```

**Syntax Description**
threshold poll phsgw-session-setup-timeout interval duration

`interval duration`

Default: 0 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

`duration` must be an integer from 30 through 60000.

**Usage Guidelines**
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system's support for thresholds in this chapter.

**Important**
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThresholdPHSGWSessSetupTimeout` command in this mode.
Examples

The following command configures the polling interval to 600 seconds for PHSGW session setup timeouts:

```
threshold poll phsgw-session-setup-timeout interval 600
```
**threshold poll phsgw-session-timeout interval**

Configures the polling interval in seconds over which to count the number of PHSGW sessions that timed out.

**Product**
PHSGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]\host_name\(config)\#```

**Syntax Description**

```
threshold poll phsgw-session-timeout interval duration
```

**interval duration**

Default: 0 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

`duration` must be an integer from 30 through 60000.

**Usage Guidelines**
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system's support for thresholds in this chapter.

**Important**
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThresholdPHSgwSessTimeout` command in this mode.
Examples

The following command configures the polling interval to 600 seconds for PHSGW session timeouts:

threshold poll phsgw-session-timeout interval 600
### threshold poll phspc-session-setup-timeout interval

Configures the polling interval in seconds over which to count the number of Personal Handyphone System - Personal Computer (PHSPC) sessions that timed out during setup.

**Product**  
PHSGW

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration  
configure  

Entering the above command sequence results in the following prompt:  

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

**Syntax Description**  
`threshold poll phspc-session-setup-timeout interval duration`

- **interval duration**
  - Default: 0 seconds.
  - Specifies the amount of time (in seconds) that comprises the polling interval.
  - `duration` must be an integer from 30 through 60000.

**Usage Guidelines**  
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**  
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system's support for thresholds in this chapter.

**Important**  
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPHSPCSessionSetupTimeout` command in this mode.
The following command configures the polling interval to 600 seconds for PHSPC session setup timeouts:

```
threshold poll phspc-session-setup-timeout interval 600
```
threshold poll phspc-sleep-mode-timeout interval

Configures the polling interval in seconds over which to count the number of PHSPC sessions that timed out when the personal computer went into sleep mode.

**Product**
PHSGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll phspc-sleep-mode-timeout interval duration
```

*interval duration*

Default: 0 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

*duration* must be an integer from 30 through 60000.

**Usage Guidelines**
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

**Important**
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPHSPC$SleepModeTimeout` command in this mode.
The following command configures the polling interval to 600 seconds for PHSPC sleep mode timeouts:

```
threshold poll phspc-sleep-mode-timeout interval 600
```
threshold poll phspc-sm-entry-denial interval

Configures the polling interval in seconds over which to count the number of denied PHSPC short message (SM) sessions.

**Product**

PHSGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll phspc-sm-entry-denial interval duration
```

- **interval duration**
  - Default: 0 seconds.
  - Specifies the amount of time (in seconds) that comprises the polling interval.
  - `duration` must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPHSPCEntryDenial` command in this mode.
Examples

The following command configures the polling interval to 600 seconds for PHSPC SM session denials:

```
threshold poll phspc-sm-entry-denial interval 600
```
**threshold poll port-high-activity interval**

Configures the polling interval in seconds over which to measure the overall percentage of port utilization.

**Product**
All

**Privilege**
Administrator Security Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[l0cal] host_name(config)#

**Syntax Description**
threshold poll port-high-activity interval *seconds*

**interval seconds**
Configures the threshold polling interval in multiples of 30 seconds. *seconds* is an integer from 30 through 60000. Default is 300 seconds.

**Usage Guidelines**
High port activity thresholds generate alerts or alarms based on the peak 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 peak utilization of a port is greater than or equal to the high threshold.

Clear condition: Actual percent peak utilization of a port is less than the 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. This threshold is configured on a per-port basis configured using the port `port-type slot#/port#` command syntax.

**Important**
This command is not available on all platforms

**Important**
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPortHighActivity` command in this mode.
Use the following example to configure the polling interval over which to measure for high port activity to
300 seconds:

`threshold poll port-high-activity interval 300`
threshold poll port-rx-utilization interval

Configures the polling interval in seconds over which to measure the overall percentage of incoming traffic received over system ports.

**Product**

All

**Privilege**

Administrator Security Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`threshold poll port-rx-utilization interval seconds`

- `interval seconds`

Configures the threshold polling interval in multiples of 30 seconds. `seconds` is an integer from 30 to 60000. Default is 300 seconds.

**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 configured using the port `port-type slot#/port#` command syntax.

---

**Important**

This command is not available on all platforms

---

**Important**

Ports configured for half-duplex do not differentiate between data received and data transmitted. (The transmitted and received percentages are combined.) Therefore, to avoid redundant alarms, it is recommended that only the receive or transmit utilization threshold be configured.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPortRxUtil` command in this mode.
Examples

Use the following example to configure a threshold poll interval of 300 seconds (5 minutes)

```plaintext
threshold poll port-rx-utilization interval 300
```
threshold poll port-tx-utilization

Configures the polling interval in seconds over which to measure the overall percentage of outgoing traffic sent over system ports.

**Product**
All

**Privilege**
Administrator Security Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`threshold poll port-tx-utilization interval seconds`

`interval seconds`

Configures the threshold polling interval in multiples of 30 seconds. `seconds` is an integer from 30 through 60000. Default is 300 seconds.

**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 configured using the port `port-type slot#/port#` command syntax.

**Important**
This command is not available on all platforms

**Important**
Ports configured for half-duplex do not differentiate between data received and data transmitted. (The transmitted and received percentages are combined.) Therefore, to avoid redundant alarms, it is recommended that only the receive or transmit utilization threshold be configured.

**Important**
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPortTxUtil` command in this mode.
threshold poll port-tx-utilization

**Examples**

Use the following example to configure a threshold poll interval of 300 seconds (5 minutes).

```
threshold poll port-tx-utilization interval 300
```
**threshold poll ppp-setup-fail-rate interval**

Configures the polling interval in seconds over which to measure for the percentage of point-to-point protocol (PPP) setup failures.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll ppp-setup-fail-rate interval duration
```

- **interval duration**
  - Default: 900 seconds.
  - Specifies the amount of time (in seconds) that comprises the polling interval.
  - `duration` must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPPPSetupFailRate` command in this mode.
The following command configures the polling interval to 600 seconds for PPP setup failures:

```
threshold poll ppp-setup-fail-rate interval 600
```
threshold poll reg-reply-error interval

Configures the polling interval over which to measure number of registration reply errors for Home Agent (HA) services.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
`configure`
Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll reg-reply-error interval duration
```

**interval duration**
Default: 0 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
`duration` must be an integer from 30 through 60000.

**Usage Guidelines**
This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system's support for thresholds in this chapter.

---

**Important**
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshHASvcRegReplyError` command in this mode.
Examples

The following command configures the polling interval to 600 seconds for HA registration errors:

```
threshold poll reg-reply-error interval 600
```
threshold poll rereg-reply-error interval

Configures the polling interval over which to measure number of re-registration reply errors for HA services.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:
```
[local] host_name(config)#
```

**Syntax Description**

```
threshold poll rereg-reply-error interval duration
```

- **interval duration**
  - Default: 0 seconds.
  - Specifies the amount of time (in seconds) that comprises the polling interval.
  - *duration* must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system's support for thresholds in this chapter.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshHASvcReregReplyError` command in this mode.

---

**Examples**
The following command configures the polling interval to 600 seconds for HA re-registration reply errors:
```
threshold poll rereg-reply-error interval 600
```
**threshold poll route-service interval**

Configures the polling interval over which to count or measure the thresholding value for BGP route services on the system.

**Product**
All

**Privilege**
Administrator Security Administrator

**Command Modes**
Exec > Global Configuration
   configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll route-service interval *dur*
```

default threshold poll route-service interval

default

Restores the threshold poll interval value to its default value of 900 seconds.

```
interval *time*
```

Default: 900 seconds

Specifies the amount of time (in seconds) that comprises the polling interval.

*dur* is any integer from 30 through 60000.

**Usage Guidelines**
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold model** and **threshold monitoring** commands for additional information on the system's support for thresholding.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshBGPRoutes` command in this mode.

**Examples**

The following command configures the polling interval for the total BGP routes threshold polling duration value to 600 seconds (10 minutes):

```
threshold poll route-service interval 600
```
threshold poll rp-setup-fail-rate interval

Configures the polling interval over which to measure the percentage of RAN PDSN (RP) setup failures.

Product  PDSN

Privilege  Administrator Security Administrator

Command Modes  Exec > Global Configuration
  configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description  threshold poll rp-setup-fail-rate interval dur
  default threshold poll route-service interval

  default
  Restores the threshold poll interval value to its default value of 900 seconds.

  interval time
  Default: 900 seconds
  Specifies the amount of time (in seconds) that comprises the polling interval.
  dur is any integer from 30 through 60000.

Usage Guidelines  This command sets the time period over which to monitor the specified value for threshold crossing.

Important  All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold model and threshold monitoring commands for additional information on the system’s support for thresholding.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshRPSetupFailRate` command in this mode.

**Examples**

The following command configures the polling interval for the RP setup fail rate polling duration value to 600 seconds (10 minutes):

```
threshold poll rp-setup-fail-rate interval 600
```
threshold poll sess-flow-count interval

Configures the polling interval over which to measure the percentage of session manager flow count.

**Product**
All

**Privilege**
Administrator Security Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll sess-flow-count interval dur
default threshold poll route-service interval
```

- **default**
  Restores the threshold poll interval value to its default value.

- **interval dur**
  Specifies the amount of time (in seconds) that comprises the polling interval.
  `dur` is any integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold model** and **threshold monitoring** commands for additional information on the system's support for thresholding.

**Examples**

The following command configures the polling interval for session manager flow count polling duration value to 600 seconds (10 minutes):

```
threshold poll sess-flow-count interval 600
```
threshold poll storage-utilization interval

Configures the polling interval over which to measure the percentage of management card flash memory utilization.

**Product**
All

**Privilege**
Administrator Security Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll storage-utilization interval dur
default threshold poll route-service interval
```

default
Restores the threshold poll interval value to its default value of 900 seconds.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold model** and **threshold monitoring** commands for additional information on the system's support for thresholding.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshStorageUtilization` command in this mode.

**Examples**

The following command configures the polling interval for flash memory utilization polling duration value to 600 seconds (10 minutes):

```
threshold poll storage-utilization interval 600
```
threshold poll system-capacity interval

Configures the polling interval over which to measure the percentage of current system capacity.

**Product**

All

**Privilege**

Administrator Security Administrator

**Command Modes**

Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`threshold poll system-capacity interval dur`

`default threshold poll route-service interval`

**default**

Restores the threshold poll interval value to its default value of 900 seconds.

**interval time**

Default: 900 seconds

Specifies the amount of time (in seconds) that comprises the polling interval.

`dur` is any integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold model` and `threshold monitoring` commands for additional information on the system's support for thresholding.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshSystemCapacity` command in this mode.

**Examples**

The following command configures the polling interval for flash memory utilization polling duration value to 600 seconds (10 minutes):

```
threshold poll system-capacity interval 600```

threshold poll total-asngw-sessions interval

Configures the polling interval over which to count or measure the thresholding value for the total number of sessions across all the ASN-GW services on a system to trigger an alert or alarm.

Product

ASN-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

```
threshold poll total-asngw-sessions interval time
default threshold poll total-asngw-sessions interval
```

default
Restores the threshold polling interval value to its default value of 300 seconds.

interval time
Default: 300 seconds
Specifies the amount of time (in seconds) that comprises the polling interval.

time must be an integer from 30 through 60000.

Usage Guidelines

This command sets the time period over which to monitor the specified value for threshold crossing.

Important

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold model and threshold monitoring commands for additional information on the system's support for thresholding.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshASNGWSessions` command in this mode.

**Examples**

The following command configures the polling interval for counting the total number of ASN-GW sessions across all the ASN-GW services on a system, to 600 seconds (10 minutes):

```
threshold poll total-asngw-sessions interval 600
```
threshold poll total-ggsn-sessions interval

Configures the polling interval over which to count or measure the thresholding value for the total number of sessions across all the GGSN services on a system to trigger an alert or alarm.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll total-ggsn-sessions interval time
default threshold poll total-ggsn-sessions interval
```

**default**
Restores the threshold polling interval value to its default value of 300 seconds.

**interval time**
Default: 300 seconds

Specifies the amount of time (in seconds) that comprises the polling interval.

**time** must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold model** and **threshold monitoring** commands for additional information on the system's support for thresholding.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshGGSNSessions` command in this mode.

**Examples**

The following command configures the polling interval for counting the total number of GGSN sessions across all the GGSN services on a system, to 600 seconds (10 minutes):

```
threshold poll total-ggsn-sessions interval 600
```
threshold poll total-gprs-pdp-sessions interval

Configures the polling interval over which to count the total number of 2G-activated PDP contexts per GPRS sessions on the system.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll total-gprs-pdp-sessions interval time
```

```
default threshold poll total-gprs-pdp-sessions interval
```

```
default
```

Restores the threshold polling interval value to its default value of 300 seconds.

```
interval time
```

Default: 300 seconds

Specifies the amount of time (in seconds) that comprises the polling interval.

`time` must be an integer from 30 through 60000.

**Usage Guidelines**
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold model` and `threshold monitoring` commands for additional information on the system's support for thresholding.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshGPRSPDPSessions` command in this mode.

**Examples**

The following command configures the polling interval for counting the total number of 2G-activated PDP contexts per GPRS sessions, to 600 seconds (10 minutes):

```
threshold poll total-gprs-pdp-sessions interval 600
```
threshold poll total-gprs-sessions interval

Configures the polling interval over which to count the total number of 2G-attached subscribers on the system.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll total-gprs-sessions interval time
default threshold poll total-gprs-sessions interval
```

- **default**
  Restores the threshold polling interval value to its default value of 300 seconds.

- **interval time**
  Default: 300 seconds
  Specifies the amount of time (in seconds) that comprises the polling interval.
  *time* must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold model** and **threshold monitoring** commands for additional information on the system's support for thresholding.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshGPRSSessions` command in this mode.

**Examples**

The following command configures the polling interval for counting the total number of 2G-attached subscribers, to 600 seconds (10 minutes):

`threshold poll total-gprs-sessions interval 600`
threshold poll total-ha-sessions interval

Configures the polling interval over which to count the total number of Home Agent (HA) sessions on the system.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

threshold poll total-ha-sessions interval *time*

default threshold poll total-ha-sessions interval

default

Restores the threshold polling interval value to its default value of 300 seconds.

interval *time*

Default: 300 seconds

Specifies the amount of time (in seconds) that comprises the polling interval.

*time* must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold model** and **threshold monitoring** commands for additional information on the system's support for thresholding.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshHASessions` command in this mode.

### Examples

The following command configures the polling interval for counting the total number of HA sessions on the system, to 600 seconds (10 minutes):

```
threshold poll total-ha-sessions interval 600
```
threshold poll total-henbgw-henb-sessions

Configures the polling interval on how frequently the thresholds are polled for total HeNB-GW HeNB sessions.

**Product**  
HeNB-GW

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration  
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll total-henbgw-henb-sessions interval time  
default threshold poll total-henbgw-henb-sessions interval
```

- **default**
  Restores the threshold polling interval value to its default value of 900 seconds.

- **interval time**
  Default: 900 seconds
  Specifies the amount of time (in seconds) that comprises the polling interval.
  `time` must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold model** and **threshold monitoring** commands for additional information on the system's support for thresholding.
To enable SNMP trap for threshold monitoring of this threshold use `snmp trap enable` `ThreshHeNBGWHenbSessions` command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds (10 minutes):

```
threshold poll total-henbgw-henb-sessions interval 600
```
threshold poll total-henbgw-ue-sessions

Configures the polling interval on how frequently the thresholds are polled for total HeNB-GW UE sessions.

**Product**
HeNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

**configure**
Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**

`threshold poll total-henbgw-ue-sessions interval time`

`default threshold poll total-henbgw-ue-sessions interval`

- **default**
Restores the threshold polling interval value to its default value of 900 seconds.

- **interval time**
Default: 900 seconds
Specifies the amount of time (in seconds) that comprises the polling interval.
`time` must be an integer from 30 through 60000.

**Usage Guidelines**
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold model and threshold monitoring commands for additional information on the system's support for thresholding.
Important

To enable SNMP trap for threshold monitoring of this threshold use **snmp trap enable ThresholdHenBGWUESessions** command in this mode.

**Examples**

The following command configures the polling interval to 600 seconds (10 minutes) for HeNB-GW UE sessions:

```
threshold poll total-henbgw-henb-sessions interval 600
```
threshold poll total-hnbgw-hnb-sessions

Configures the polling interval over which to count or measure the thresholding value for the total number of IuH sessions between the HNB and HNB-GW to count across all the HNB-GW services on a system to trigger an alert or alarm.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll total-hnbgw-hnb-sessions interval time
default threshold poll total-hnbgw-hnb-sessions interval
```

**default**
Restores the threshold polling interval value to its default value of 900 seconds.

**interval time**
Default: 900 seconds
Specifies the amount of time (in seconds) that comprises the polling interval.

```
time must be an integer from 30 through 60000.
```

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold model** and **threshold monitoring** commands for additional information on the system's support for thresholding.
To enable SNMP trap for threshold monitoring of this threshold use **snmp trap enable**

**ThreshTotalHNBGWHnbSess** command in this mode.

**Examples**

The following command configures the polling interval for counting the total number of HNB sessions between HNB and HNB-GW across all the HNB-GW services on a system, to 600 seconds (10 minutes):

```
threshold poll total-hnb-gw-hnb-sessions interval 600
```
**threshold poll total-hnbgw-iu-sessions**

Configures the polling interval over which to count or measure the thresholding value for the total number of subscriber sessions on HNB-GW service (over Iu-CS/Iu-PS interface) to count across all the HNB-GW services on a system to trigger alert or alarm.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll total-hnbgw-iu-sessions interval time
default threshold poll total-hnbgw-iu-sessions interval
```

- **default**
  Restores the threshold poll interval value to its default value of 300 seconds.

- **interval time**
  Default: 300 seconds
  Specifies the amount of time (in seconds) that comprises the polling interval.
  The `time` must be an value from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold model** and **threshold monitoring** commands for additional information on the system's support for thresholding.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshTotalHNBGW1uSess` command in this mode.

**Examples**

The following command configures the polling interval for counting the total number of subscriber sessions across all the HNB-GW services on a system, to 600 seconds (10 minutes):

```
threshold poll total-hnbgw-iu-sessions interval 600
```
**threshold poll total-hnbgw-ue-sessions**

Configures the polling interval over which to count or measure the thresholding value for the total number of UEs connected to HNB-GW service to count across all the HNB-GW services on a system to trigger alert or alarm.

<table>
<thead>
<tr>
<th><strong>Product</strong></th>
<th>HNB-GW</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Privilege</strong></td>
<td>Security Administrator, Administrator</td>
</tr>
</tbody>
</table>
| **Command Modes** | Exec > Global Configuration  
  configure |

Entering the above command sequence results in the following prompt:

```
[local]<host_name>(config)#
```

**Syntax Description**

`threshold poll total-hnbgw-ue-sessions interval time`

`default threshold poll total-hnbgw-ue-sessions interval`

**default**

Restores the threshold poll interval value to its default value of 300 seconds.

**interval time**

Default: 300 seconds

Specifies the amount of time (in seconds) that comprises the polling interval.

`time` must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold model` and `threshold monitoring` commands for additional information on the system's support for thresholding.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshTotalHNBGWUeSess` command in this mode.

**Examples**

The following command configures the polling interval for the total number of UEs connected to an HNB-GW service across all the HNB-GW services on a system, to 600 seconds (10 minutes):

```
threshold poll total-hnbgw-ue-sessions interval 600
```
threshold poll total-hsgw-sessions interval

Configures the polling interval over which to count the total number of HRPD Serving Gateway (HSGW) sessions across all services in the system.

Product

HSGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

threshold poll total-hsgw-sessions interval time
default threshold poll total-hsgw-sessions interval
default
Restores the threshold poll interval value to its default value of 300 seconds.

interval time
Default: 300 seconds
Specifies the amount of time (in seconds) that comprises the polling interval.

Important

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold model and threshold monitoring commands for additional information on the system's support for thresholding.

Usage Guidelines

This command sets the time period over which to monitor the specified value for threshold crossing.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshHSGWSessions` command in this mode.

**Examples**

The following command configures the polling interval for the total number of HSGW sessions across all the HSGW services on a system, to 600 seconds (10 minutes):

```
threshold poll total-hsgw-sessions interval 600
```
threshold poll total-lma-sessions interval

Configures the polling interval over which to count the total number of Local Mobility Anchor (LMA) sessions across all services in the system.

Product
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description
threshold poll total-lma-sessions interval time
default threshold poll total-lma-sessions interval
default
Restores the threshold poll interval value to its default value of 300 seconds.

interval time
Default: 300 seconds
Specifies the amount of time (in seconds) that comprises the polling interval.
time must be an integer from 30 through 60000.

Usage Guidelines
This command sets the time period over which to monitor the specified value for threshold crossing.

Important
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold model and threshold monitoring commands for additional information on the system's support for thresholding.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshLMASessions` command in this mode.

**Examples**

The following command configures the polling interval for the total number of LMA sessions across all the LMA sessions on a system, to 600 seconds (10 minutes):

```
threshold poll total-lma-sessions interval 600
```
**threshold poll total-lns-sessions interval**

Configures the polling interval over which to count the total number of L2TP Network Server (LNS) sessions in the system.

**Product**
- PDSN
- GGSN
- HA

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration
  - `configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll total-lns-sessions interval time
default threshold poll total-lns-sessions interval
```

**default**

Restores the threshold poll interval value to its default value of 300 seconds.

**interval time**

Default: 300 seconds

Specifies the amount of time (in seconds) that comprises the polling interval.

*time* must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold model` and `threshold monitoring` commands for additional information on the system's support for thresholding.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshLNSSessions` command in this mode.

**Examples**

The following command configures the polling interval for the total number of LNS sessions across all the LNS sessions on a system, to 600 seconds (10 minutes):

```
threshold poll total-lns-sessions interval 600
```
threshold poll total-mme-sessions

Configures the polling interval over which to count or measure the thresholding value for MME sessions on the system.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll total-mme-sessions interval time
default threshold poll total-mme-sessions interval
```

- **default**
  Restores the threshold poll interval value to its default value of 900 seconds.

- **interval time**
  Default: 900 seconds
  Specifies the polling interval (in seconds) for counting the total number of MME sessions on the system.
  `time` must be any integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold model` and `threshold monitoring` commands for additional information on the system's support for thresholding.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshMMESessions` command in this mode.

**Examples**

The following command configures the polling interval for the total MME session threshold polling duration value to 600 seconds (10 minutes):

```
threshold poll total-mme-sessions interval 600
```
**threshold poll total-pdsn-sessions interval**

Configures the polling interval over which to count the total number of Packet Data Serving Node (PDSN) sessions in the system.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`threshold poll total-pdsn-sessions interval time`

`default` `threshold poll total-pdsn-sessions interval`

`default`

Restores the threshold poll interval value to its default value of 300 seconds.

`interval time`

Default: 300 seconds

Specifies the amount of time (in seconds) that comprises the polling interval.

`time` must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold model` and `threshold monitoring` commands for additional information on the system's support for thresholding.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPDSNSessions` command in this mode.

**Examples**

The following command configures the polling interval for the total number of PDSN sessions across all the PDSN sessions on a system, to 600 seconds (10 minutes):

```
threshold poll total-pdsn-sessions interval 600
```
threshold poll total-pgw-sessions interval

Configures the polling interval over which to count the total number of Packet Data Network Gateway (P-GW) sessions across all services in the system.

**Product**
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration
- configure

Entering the above command sequence results in the following prompt:

```
[local]\host_name\(config)#
```

**Syntax Description**

- `threshold poll total-pgw-sessions interval time`
- `default threshold poll total-pgw-sessions interval`

**Default**
Restores the threshold poll interval value to its default value of 300 seconds.

**interval time**
Default: 300 seconds
Specifies the amount of time (in seconds) that comprises the polling interval.

`time` must be an integer from 30 through 60000.

**Usage Guidelines**
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold model and threshold monitoring commands for additional information on the system's support for thresholding.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPGWSessions` command in this mode.

**Examples**

The following command configures the polling interval for the total number of P-GW sessions across all the P-GW sessions on a system, to 600 seconds (10 minutes):

```
threshold poll total-pgw-sessions interval 600
```
threshold poll total-saegw-sessions interval

Configures the polling interval over which to count the total number of System Architecture Evolution Gateway (SAEGW) sessions across all services in the system.

**Product**
SAEGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll total-saegw-sessions interval time
default threshold poll total-saegw-sessions interval
```

- **default**
  Restores the threshold poll interval value to its default value of 300 seconds.

- **interval time**
  Default: 300 seconds
  Specifies the amount of time (in seconds) that comprises the polling interval.
  `time` must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold model` and `threshold monitoring` commands for additional information on the system's support for thresholding.
Examples

The following command configures the polling interval for the total number of SAEGW sessions on a system, to 600 seconds (10 minutes):

```
threshold poll total-saegw-sessions interval 600
```
threshold poll total-sgsn-pdp-sessions interval

Configures the polling interval over which to count the total number of PDP contexts for all Serving GPRS Support Node (SGSN) sessions in the system.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
```
configure
```
Entering the above command sequence results in the following prompt:
```
[local]host_name(config)#
```

**Syntax Description**

```
threshold poll total-sgsn-pdp-sessions interval time
default threshold poll total-sgsn-pdp-sessions interval
```

- **default**
  Restores the threshold poll interval value to its default value of 300 seconds.

- **interval time**
  Default: 300 seconds
  Specifies the amount of time (in seconds) that comprises the polling interval.
  `time` must be an integer from 30 through 60000.

**Usage Guidelines**
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold model and threshold monitoring commands for additional information on the system's support for thresholding.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable
ThreshSGSNPDPSessions` command in this mode.

**Examples**

The following command configures the polling interval for the total number of PDP contexts across all the SGSN sessions on a system, to 600 seconds (10 minutes):

```
threshold poll total-sgsn-pdp-sessions interval 600
```
**threshold poll total-sgsn-sessions interval**

Configures the polling interval over which to count the total number of SGSN sessions in the system.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

- configure

Entering the above command sequence results in the following prompt:

[local]\host_name(config)#

**Syntax Description**

- `threshold poll total-sgsn-sessions interval time`
- `default threshold poll total-sgsn-sessions interval`

**Default**

Restores the threshold poll interval value to its default value of 300 seconds.

**interval time**

Default: 300 seconds

Specifies the amount of time (in seconds) that comprises the polling interval.

*time* must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold model** and **threshold monitoring** commands for additional information on the system's support for thresholding.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshSGSNSessions` command in this mode.

**Examples**

The following command configures the polling interval for the total number of SGSN sessions on a system, to 600 seconds (10 minutes):

```
threshold poll total-sgsn-sessions interval 600
```
threshold poll total-sgw-sessions interval

Configures the polling interval over which to count the total number of Serving Gateway (S-GW) sessions across all services in the system.

**Product**

- S-GW
- SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold poll total-sgw-sessions interval time

default threshold poll total-sgw-sessions interval
```

default

Restores the threshold poll interval value to its default value of 300 seconds.

`interval time`

Default: 300 seconds

Specifies the amount of time (in seconds) that comprises the polling interval.

`time` must be an integer from 30 through 60000.

**Usage Guidelines**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important**

All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold model` and `threshold monitoring` commands for additional information on the system's support for thresholding.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshSGWSessions` command in this mode.

Important

Examples

The following command configures the polling interval for the total number of S-GW sessions on a system, to 600 seconds (10 minutes):

```
threshold poll total-sgw-sessions interval 600
```
threshold poll total-subscriber interval

Configures the polling interval over which to count the total number of subscriber sessions across all services in the system.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax Description**
threshold poll total-subscriber interval time
default threshold poll total-subscriber interval

default
Restores the threshold poll interval value to its default value of 300 seconds.

interval time
Default: 300 seconds
Specifies the amount of time (in seconds) that comprises the polling interval.
time must be an integer from 30 through 60000.

**Usage Guidelines**
This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important**
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold model and threshold monitoring commands for additional information on the system's support for thresholding.
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshSubscriberTotal` command in this mode.

**Examples**

The following command configures the polling interval for the total number of subscribers on a system, to 600 seconds (10 minutes):

```
threshold poll total-subscriber interval 600
```
Global Configuration Mode Commands (threshold ppp - url-blacklisting)

The Global Configuration Mode is used to configure basic system-wide parameters.

This section includes the commands \texttt{threshold ppp-setup-fail-rate} through \texttt{url-blacklisting database}.

\textbf{Command Modes}

\texttt{Exec > Global Configuration}

\texttt{configure}

Entering the above command sequence results in the following prompt:

\[ \text{(local)} host\_name(config)\# \]

\textbf{Important}

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

- \texttt{threshold ppp-setup-fail-rate}, page 899
- \texttt{threshold route-service bgp-routes}, page 901
- \texttt{threshold route-service vrf-framed-routes}, page 903
- \texttt{threshold route-service vrf-total-routes}, page 905
- \texttt{threshold rp-setup-fail-rate}, page 907
- \texttt{threshold sess-flow-count}, page 909
- \texttt{threshold storage-utilization}, page 910
- \texttt{threshold subscriber active}, page 912
- \texttt{threshold subscriber total}, page 914
- \texttt{threshold system-capacity}, page 916
- \texttt{threshold total-asngw-sessions}, page 918
- \texttt{threshold total-ggsn-sessions}, page 920
- threshold total-gprs-pdp-sessions, page 922
- threshold total-gprs-sessions, page 924
- threshold total-ha-sessions, page 926
- threshold total-hnbgw-hnb-sessions, page 928
- threshold total-hnbgw-iu-sessions, page 930
- threshold total-hnbgw-ue-sessions, page 932
- threshold total-hsgw-sessions, page 934
- threshold total-lma-sessions, page 936
- threshold total-lns-sessions, page 938
- threshold total-mme-sessions, page 940
- threshold total-pdsn-sessions, page 942
- threshold total-pgw-sessions, page 944
- threshold total-saegw-sessions, page 946
- threshold total-sgsn-pdp-sessions, page 948
- threshold total-sgsn-sessions, page 950
- threshold total-sgw-sessions, page 952
- throttling-override-policy, page 954
- timestamps, page 955
- traffic shape, page 956
- unexpected-scenario session drop-call, page 958
- upgrade limit, page 960
- url-blacklisting database, page 962
- wsg-lookup, page 964
**threshold ppp-setup-fail-rate**

Configures alarm or alert thresholds for the percentage of point-to-point protocol (PPP) setup failures.

**Product**
- PDSN
- GGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration
- configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold ppp-setup-fail-rate high_thresh [ clear low_thresh ]
```

**high_thresh**
Default: 0

Specifies the high threshold rate percentage for PPP setup failures experienced by the system that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 100. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0

Specifies the low threshold rate percentage for PPP setup failures experienced by the system that maintains a previously generated alarm condition. If the number of setup failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 100. A value of 0 disables the threshold.

**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

PPP setup failure rate thresholds generate alerts or alarms based on the rate of call setup failures experienced by the system during the specified polling interval. The failure rate is the percentage of failures as determined by number of PPP setup failures divided by the total number of PPP sessions initiated.

Alerts or alarms are triggered for PPP setup failure rates based on the following rules:

- **Enter condition**: Actual number of call setup failures is greater than or equal to the high threshold.
- **Clear condition**: Actual number of call setup failures is less than the 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 to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Examples

The following command configures a PPP setup failure rate high percentage threshold of 50 percent and a clear threshold of 45 percent:

```
threshold ppp-setup-fail-rate 50 clear 45
```
threshold route-service bgp-routes

Configures alarm or alert thresholds for the percentage of BGP routes.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold route-service bgp-routes high_thresh [ clear low_thresh ]
```

**bgp-routes**

Specifies the threshold for percentage of maximum bgp routes per context. It is an integer from 0 through 100.

- **high_thresh**
  Specifies the high threshold rate percentage for maximum BGP routes per context that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thresh* is an integer from 0 through 100. A value of 0 disables the threshold. The default value is 0.

- **clear low_thresh**
  Specifies the low threshold rate percentage for BGP routes per context that maintains a previously generated alarm condition. If the number of BPG routes falls beneath the low threshold within the polling interval, a clear alarm will be generated. *low_thresh* is an integer from 0 through 100. A value of 0 disables the threshold. The default value is 0.

For more information on the maximum route value per context, refer to *Engineering Rules* in the *System Administration Guide*.

**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 configure a threshold in percentage of maximum BGP routes allowed. If the percentage of the number of BGP routes in a context reaches \textit{high\_thresh}, a notification is generated. Optionally, if the threshold subsystem is configured in 'alarm' mode, a \textbf{Threshold\_Clear} notification is generated when the percentage of the number of BGP routes in a context goes below \textit{low\_thresh}. The maximum number of BGP routes is also sent by BGP task when getting the statistics.

Alerts or alarms are triggered for BGP routes based on the following rules:

- **Enter condition**: Actual number of BGP routes is greater than the high threshold.
- **Clear condition**: Actual number BGP routes is less than the 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 \texttt{threshold poll} command to configure the polling interval and the \texttt{threshold monitoring} command to enable thresholding for this value.

Examples

The following command configures system for high threshold for \texttt{bgp-routes} of 50 percent and a clear threshold of 45 percent:

\texttt{threshold route-service bgp-routes 50 clear 45}
threshold route-service vrf-framed-routes

Configures alarm or alert thresholds for the percentage of VRF framed routes.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold route-service vrf-framed-routes high_thresh [ clear low_thresh ] [ context context_name vrf vrf_name ]
```

**vrf-framed-routes**

Specifies the threshold for percentage of VRF framed routes per VRF. It is an integer from 0 through 100.

- **high_thresh**
  
  Specifies the high threshold rate percentage for VRF framed routes per VRF that must be met or exceeded within the polling interval to generate an alert or alarm. `high_thresh` is an integer from 0 through 100. A value of 0 disables the threshold. The default value is 0.

- **clear low_thresh**
  
  Configures the alarm clear threshold. It is an integer from 0 through 100. The default value is 0.

- **context context_name**
  
  Configures the context to apply `vrf-framed-routes` threshold.

- **vrf vrf_name**
  
  Configures the VRF to apply `vrf-framed-routes` threshold.

For more information on the maximum route value per context, refer to *Engineering Rules* in the *System Administration Guide*. 
When the root level version of the `threshold route-service` command is issued without `context` and `vrf` information, the framed routes threshold value is configured for every VRF in the system. When the vrf-framed-routes command is issued for a specific context and VRF name, then the threshold value is configured only for that context and VRF. Any previously configured root level or VRF specific threshold value will be overwritten. The threshold values are set as a percentage of the `ip maximum routes` for the VRF. If `ip maximum routes` for a VRF is not configured, the default value is the maximum routes per context. If the threshold values in the above CLI command is set to 0, then the respective threshold configuration is removed.

Usage Guidelines

Use this command to configure a threshold in percentage of the maximum VRF framed routes. If the percentage of the number VRF framed routes reaches `high_thresh`, a notification is generated. Optionally, if the threshold subsystem is configured in 'alarm' mode, a `Threshold_Clear` notification is generated when the percentage of the number of VRF framed routes in a context goes below `low_thresh`.

Alerts or alarms are triggered for VRF framed routes based on the following rules:

- **Enter condition**: Actual number of VRF framed routes is greater than the high threshold.
- **Clear condition**: Actual number of VRF framed routes is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Examples

The following command configures system for high threshold for `vrf-framed-routes` of 70 percent with a clear threshold of 40 percent for all the VRFs in the system:

```
threshold route-service vrf-framed-routes 70 clear 40
```

The following command configures system for high threshold for `vrf-framed-routes` of 30 percent with a clear threshold of 20 percent for a context `egress1` and vrf `vrf1`:

```
threshold route-service vrf-framed-routes 30 clear 20 context egress1 vrf vrf1
```
threshold route-service vrf-total-routes

Configures alarm or alert thresholds for the count of VRF total routes.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description

threshold route-service vrf-total-routes high_thresh [ clear low_thresh ] [ context context_name vrf vrf_name ]

vrf-total-routes

Specifies the number of VRF total routes threshold value per VRF. It is an integer from 0 through 65536.

- **high_thresh**
  Specifies the high threshold count of total routes per VRF that must be met or exceeded within the polling interval to generate an alert or alarm. **high_thresh** is an integer from 0 through 65536. A value of 0 disables the threshold. The default value is 0.

- **clear low_thresh**
  Configures the alarms clear threshold. It is an integer from 0 through 65536. The default is 0.

- **context context_name**
  Configures the context to apply **vrf-total-routes** threshold.

- **vrf vrf_name**
  Configures the VRF to apply **vrf-total-routes** threshold.

For more information on the maximum route value per context, refer to **Engineering Rules** in the **System Administration Guide**.
Important

When the root level version of the **threshold-route-service** command is issued without **context** and **vrf** information, the total routes threshold value is configured for every VRF in the system. When the **vrf-total-routes** command is issued for a specific context and VRF name, the threshold value is configured only for that context and VRF. Any previously configured root level or VRF specific threshold value will be overwritten. The threshold values are set as the total count of the routes in the VRF which includes pool routes, interface routes, static routes, dynamic routes and framed routes. If the threshold values in the above CLI command is set to 0, then the respective threshold configuration is removed.

Usage Guidelines

Use this command to configure a threshold in number of the VRF total routes. If the count of VRF total routes in a context reaches **high_thresh**, a notification is generated. Optionally, if the threshold subsystem is configured in 'alarm' mode, a **Threshold_Clear** notification is generated when count of VRF total routes in a context goes below **low_thresh**.

Alerts or alarms are triggered VRF total routes based on the following rules:

- **Enter condition**: Actual number of VRF total routes is greater than the high threshold.
- **Clear condition**: Actual number of VRF total routes is less than the 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 to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Examples

The following command configures system for high threshold for **vrf-total-routes** of 3000 with a clear threshold of 2800 for all the VRFs in the system

```
threshold route-service vrf-total-routes 3000 clear 2800
```

The following command configures system for high threshold for **vrf-total-routes** of 1500 with a clear threshold of 800 for a context **egress1** and vrf **vrf1**:

```
threshold route-service vrf-total-routes 1500 clear 800 context egress1 vrf vrf1
```
threshold rp-setup-fail-rate

Configures alarm or alert thresholds for the percentage of RAN PDSN (RP) setup failures.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
`threshold rp-setup-fail-rate high_thresh [ clear low_thresh ]`

`high_thresh`
Default: 0
Specifies the high threshold rate percentage for RP setup failures experienced by the system that must be met or exceeded within the polling interval to generate an alert or alarm.
`high_thresh` is an integer from 0 through 100. A value of 0 disables the threshold.

`clear low_thresh`
Default: 0
Specifies the low threshold rate percentage for RP setup failures experienced by the system that maintains a previously generated alarm condition. If the number of setup failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.
`low_thresh` is an integer from 0 through 100. A value of 0 disables the threshold.

**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**
RP setup failure rate thresholds generate alerts or alarms based on the rate of call setup failures experienced by the system during the specified polling interval. The failure rate is the percentage of failures as determined
by number of Registration Request Messages rejected divided by the total number of Registration Request Messages received.

Alerts or alarms are triggered for RP setup failure rates based on the following rules:

- **Enter condition:** Actual number of call setup failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of call setup failures is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a RP setup failure rate high threshold of 50 percent and a clear threshold of 45 percent:

```
threshold rp-setup-fail-rate 50 clear 45
```
**threshold sess-flow-count**

Configures alarm or alert thresholds for the percentage of session manager flow count.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
`configure`
Entering the above command sequence results in the following prompt:
```
[local]\{host_name\}(config)#
```

**Syntax Description**
`threshold sess-flow-count flow_count_thresh [ clear clear_thresh ]`

*flow_count_percent*
Default: 90
Specifies the high threshold rate percentage for session manager flow count to generate an alert or alarm. `flow_count_thresh` is an integer from 1 through 100.

*clear clear_thresh*
Specifies the low threshold rate percentage for session manager flow count. If the number of session manager flow count falls beneath the low threshold, a clear alarm will be generated. `clear_thresh` is an integer from 1 through 100. The value chosen for the `clear_thresh` must always be lesser than the `flow_count_thresh`.

**Usage Guidelines**
Use this command to configure thresholds for monitoring the session flow count.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**
The following command configures a session flow count high threshold of 50 percent and a clear threshold of 45 percent:
`threshold sess-flow-count 50 clear 45`
**threshold storage-utilization**

Configures alarm or alert thresholds for the percentage of management card flash memory utilization.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`threshold storage-utilization high_thresh [clear low_thresh ]`

- `high_thresh`
  Default: 90
  Specifies the high threshold storage utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
  `high_thresh` is an integer from 0 through 100. A value of 0 disables the threshold.

- `clear low_thresh`
  Default: 90
  Specifies the low threshold storage utilization percentage that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  `low_thresh` is an integer from 0 through 100. A value of 0 disables the threshold.

**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**
Flash memory utilization thresholds generate alerts or alarms based on the utilization percentage of storage available to the system.
Alerts or alarms are triggered for storage utilization based on the following rules:

- **Enter condition:** Actual percentage storage utilization is greater than or equal to the high threshold.
- **Clear condition:** Actual percentage storage utilization is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

### Examples

The following command configures a high threshold for storage utilization percentage of 85 for a system using the Alert thresholding model:

```
threshold storage-utilization 85
```
threshold subscriber active

Configures alarm or alert thresholds for the number of active subscribers in the system.

<table>
<thead>
<tr>
<th>Product</th>
<th>PDSN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>GGSN</td>
</tr>
<tr>
<td></td>
<td>SGSN</td>
</tr>
<tr>
<td></td>
<td>HA</td>
</tr>
</tbody>
</table>

| Privilege | Security Administrator, Administrator |

| Command Modes | Exec > Global Configuration configure |

Entering the above command sequence results in the following prompt:

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

| Syntax Description | threshold subscriber active high_thresh [ clear low_thresh ] |

```markdown
high_thresh

Default: 0

Specifies the high threshold number of active subscriber sessions facilitated by the system that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.
```

```markdown
clear low_thresh

Default: 0

Specifies the low threshold number of active subscriber sessions facilitated by the system that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 and 4000000. A value of 0 disables the threshold.
```

---

**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**

Active subscriber thresholds generate alerts or alarms based on the total number of active subscriber sessions facilitated by the system during the specified polling interval.

Alerts or alarms are triggered for active subscriber totals based on the following rules:

- **Enter condition:** Actual total number of active subscriber sessions is greater than or equal to the high threshold.

- **Clear condition:** Actual total number of active subscriber sessions is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures an active subscriber high threshold count of 150000 and a low threshold of 100000 for a system using the Alarm thresholding model:

```
threshold subscriber active 150000 clear 100000
```
threshold subscriber total

Configures alarm or alert thresholds for the total number of active and inactive subscribers in the system.

**Product**
- PDSN
- GGSN
- HA

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold subscriber total high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 0

Specifies the high threshold number of subscriber sessions (active and dormant) facilitated by the system that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 4000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of subscriber sessions (active and dormant) facilitated by the system that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 and 4000000. A value of 0 disables the threshold.

**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**

Total subscriber thresholds generate alerts or alarms based on the total number of subscriber sessions (active and dormant) facilitated by the system during the specified polling interval.

Alerts or alarms are triggered for subscriber totals based on the following rules:

- **Enter condition:** Actual total number of subscriber sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of subscriber sessions is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures an active subscriber high threshold count of 450000 and a low threshold of 250000 for a system using the Alarm thresholding model:

```
threshold subscriber total 450000 clear 250000
```
threshold system-capacity

Configures alarm or alert thresholds based on the percentage of current system capacity.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`threshold system high_thresh [ clear low_thresh ]`

- **high_thresh**

  Default: 90
  
  Specifies the high threshold system capacity percentage that must be met or exceeded within the polling interval to generate an alert or alarm. `high_thresh` is an integer from 0 through 100. A value of 0 disables the threshold.

- **clear low_thresh**

  Default: 90
  
  Specifies the low threshold system capacity percentage that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated. `low_thresh` is an integer from 0 through 100. A value of 0 disables the threshold.

---

**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**

Flash memory utilization thresholds generate alerts or alarms based on the system utilization. Alerts or alarms are triggered for system capacity based on the following rules:
• **Enter condition:** Actual percentage of system capacity is greater than or equal to the high threshold.

• **Clear condition:** Actual percentage of system capacity is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a high threshold for system capacity percentage of 95 for a system using the Alert thresholding model:

`threshold system-capacity 95`
**threshold total-asngw-sessions**

Configures alarm or alert thresholds for the total number of ASN-GW sessions across all the services in the system.

**Product**

ANS-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`threshold total-asngw-sessions high_thresh | clear low_thresh`

**high_thresh**

Default: 0 (Disabled)

Specifies the high threshold number of total ASN-GW sessions across all the sessions in the system that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 4000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0 (Disabled)

Specifies the low threshold number of total ASN-GW sessions that maintains a previously generated alarm condition. If the number of ASN-GW sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 and 4000000. A value of 0 disables the threshold.

**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**

Monitor and set alarms or alerts when the total number of ASN-GW sessions across all the services in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for the total number of ASN-GW sessions based on the following rules:

- **Enter condition**: Actual total number of ASN-GW sessions is greater than or equal to the high threshold.
- **Clear condition**: Actual total number of ASN-GW sessions is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

### Examples

The following command configures a total ASN-GW session high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold total-asngw-sessions 10000
```
threshold total-ggsn-sessions

Configures alarm or alert thresholds for the total number of GGSN sessions across all the services in the system.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

**Syntax Description**

`threshold total-ggsn-sessions high_thresh | clear low_thresh`

**high_thresh**

Default: 0 (Disabled)

Specifies the high threshold number of total GGSN sessions across all the sessions in the system that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is an integer from 0 through 4000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0 (Disabled)

Specifies the low threshold number of total GGSN sessions that maintains a previously generated alarm condition. If the number of GGSN sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` is an integer from 0 and 4000000. A value of 0 disables the threshold.

**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**

Monitor and set alarms or alerts when the total number of GGSN sessions across all the services in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for the total number of GGSN sessions based on the following rules:

- **Enter condition:** Actual total number of GGSN sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of GGSN sessions is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a total GGSN session high threshold count of 10000 for a system using the Alert thresholding model:

```bash
threshold total-ggsn-sessions 10000
```
threshold total-gprs-pdp-sessions

Configures alarm or alert thresholds for the total number of PDP contexts per GPRS sessions in the system.

Product

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

Syntax Description

threshold total-gprs-pdp-sessions high_thresh [ clear low_thresh ]

high_thresh

Default: 0

Specifies the high threshold number of total PDP contexts per GPRS session for all GPRS services that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 1 through 2000000. A value of 0 disables the threshold.

clear low_thresh

Default: 0

Specifies the low threshold number of total PDP contexts per GPRS session for all GPRS services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 and 2000000. A value of 0 disables the threshold.

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

Monitor and set alarms or alerts when the total number of GPRS sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for GPRS sessions based on the following rules:

- **Enter condition**: Actual total number of PDP Contexts is greater than or equal to the high threshold.
- **Clear condition**: Actual total number of PDP contexts is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

### Examples

The following command configures a total number of PDP contexts per GPRS session high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold total-gprs-pdp-sessions 10000
```
threshold total-gprs-sessions

Configures alarm or alert thresholds for the total number of GPRS sessions in the system.

**Product**
SGSN

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
`threshold total-gprs-sessions high_thresh [ clear low_thresh ]`

**high_thresh**
Default: 0
Specifies the high threshold number of total GPRS sessions for all GPRS services that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is an integer from 1 through 2000000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0
Specifies the low threshold number of total GPRS sessions for all GPRS services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` is an integer from 0 and 2000000. A value of 0 disables the threshold.

**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**
Monitor and set alarms or alerts when the total number of GPRS sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for GPRS sessions based on the following rules:

- **Enter condition:** Actual total number of GPRS sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of GPRS sessions is less than the 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 command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a total number of GPRS sessions high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold total-gprs-sessions 10000
```
threshold total-ha-sessions

Configures alarm or alert thresholds for the total number of Home Agent (HA) sessions across all services in the system.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description

threshold total-ha-sessions high_thresh [ clear low_thresh ]

high_thresh

Default: 0

Specifies the high threshold number of HA sessions for all HA services that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

clear low_thresh

Default: 0

Specifies the low threshold number of HA sessions for all HA services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 and 4000000. A value of 0 disables the threshold.

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

Monitor and set alarms or alerts when the total number of HA sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for HA sessions based on the following rules:

- **Enter condition**: Actual total number of HA sessions is greater than or equal to the high threshold.
- **Clear condition**: Actual total number of HA sessions is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a total number of HA sessions high threshold count of **10000** for a system using the Alert thresholding model:

```
threshold total-ha-sessions 10000
```
threshold total-hnbgw-hnb-sessions

Configures alarm or alert thresholds for the total number of Home NodeB (HNB) sessions across all the HNB Gateway (HNB-GW) services in the system.

Product
HNBGW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]

Syntax Description
threshold total-hnbgw-hnb-sessions high_thresh [ clear low_thresh ]

high_thresh
Default: 0 (Disabled)
Specifies the high threshold for the total number of HNB-HNB-GW sessions on IuH interfaces across all HNB-GW services on a system that must be met or exceeded within the polling interval to generate an alert or alarm.

low_thresh is an integer from 0 through 1000000. A value of 0 disables the threshold.

clear low_thresh
Default: 0 (Disabled)
Specifies the low threshold for the total number of HNB-HNB-GW sessions on IuH interfaces across all services on a system that maintains a previously generated alarm condition. If the number of HNB-HNB-GW sessions in a system falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 1000000. A value of 0 disables the threshold.

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 monitor and set alarms or alerts when the total number of HNB-HNB-GW sessions on IuH interface across all HNB-GW services in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for the total number of HNB-HNB-GW sessions on IuH interface based on the following rules:

- **Enter condition:** Actual total number of HNB-HNB-GW sessions on IuH interface is greater than the high threshold.
- **Clear condition:** Actual total number of HNB-HNB-GW sessions on IuH interfaces is less than the 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 total-hnbgw-hnb-sessions` command to configure the polling interval and the `threshold monitoring hnbgw-service` command to enable thresholding for this value.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshTotalHNBGGWHnbSess` command in this mode.

---

Examples

The following command configures the total number of HNB-GW-HNB sessions on IuH interfaces to a high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold total-hnbgw-hnb-sessions 10000
```
threshold total-hnbgw-iu-sessions

Configures alarm or alert thresholds for the total number of subscriber sessions towards the Core Networks (CN) across all HNBGW services over Iu interfaces (Iu-CS/Iu-PS interface) on a system.

Product
HNBGW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description
threshold total-hnbgw-iu-sessions high_thresh | clear low_thresh |

high_thresh
Default: 0 (Disabled)
Specifies the high threshold for the total number of subscriber sessions towards CN across all HNB-GW services on a system that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 3000000. A value of 0 disables the threshold.

clear low_thresh
Default: 0 (Disabled)
Specifies the low threshold for the total number of subscriber sessions towards CN across all services on a system that maintains a previously generated alarm condition. If the number of subscriber sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 3000000. A value of 0 disables the threshold.

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 monitor and set alarms or alerts when the total number of subscriber sessions towards CN across all HNB-GW services in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for the total number of subscriber sessions towards CN across all HNB-GW service on a system based on the following rules:

- **Enter condition:** Actual total number of subscriber sessions across all HNB-GW service on a system is greater than the high threshold.

- **Clear condition:** Actual total number of subscriber sessions across all HNB-GW service on a system is less than the 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 total-hnbgw-iu-sessions` command to configure the polling interval and the `threshold monitoring hnbgw-service` command to enable thresholding for this value.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshTotalHNBGWlUSSess` command in this mode.

---

**Examples**

The following command configures the total number of subscriber sessions towards CN across all HNB-GW services to a high threshold count of 30000 for a system using the Alert thresholding model:

`threshold total-hnbgw-iu-sessions 30000`
threshold total-hnbgw-ue-sessions

Configures alarm or alert thresholds for the total number of UEs connected to an HNB-GW service across all the HNB-GW services in the system.

**Product**
HNBGW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
```
threshold total-hnbgw-ue-sessions high_thresh | clear low_thresh |
```

**high_thresh**
Default: 0 (Disabled)

Specifies the high threshold for the total number of UEs connected across all HNB-GW services on a system that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thesh* is an integer from 0 through 4000000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0 (Disabled)

Specifies the low threshold for the total number of UEs connected to HNB-GW service across all HNB-GW services that maintains a previously generated alarm condition. If the number of UE sessions across all the services in a system, falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thesh* is an integer from 0 and 4000000. A value of 0 disables the threshold.

---

**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 monitor and set alarms or alerts when the total number of UEs connected to HNB-GW service across all HNB-GW services in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for the total number of UEs connected across all HNB-GW service on a system based on the following rules:

- **Enter condition:** Actual total number of UEs connected to HNB-GW service across all HNB-GW services on a system is greater than the high threshold.

- **Clear condition:** Actual total number of UEs connected to HNB-GW service across all HNB-GW services on a system is less than the 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 total-hnbgw-ue-sessions` command to configure the polling interval and the `threshold monitoring hnbgw-service` command to enable thresholding for this value.

---

**Important**

To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshTotalHNBGWUeSess` command in this mode.

---

**Examples**

The following command configures the total number of UEs connected to HNB-GW service across all HNB-GW services to a high threshold count of `40000` for a system using the Alert thresholding model:

```
threshold total-hnbgw-ue-sessions 40000
```
threshold total-hsgw-sessions

Configures alarm or alert thresholds for the total number of HRPD Serving Gateway (HSGW) sessions across all services in the system.

**Product**

HSGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

`[local] host_name(config)#`

**Syntax Description**

`threshold total-hsgw-sessions high_thresh [ clear low_thresh ]`

`high_thresh`

Default: 0

Specifies the high threshold for the number of HSGW sessions for all HSGW services that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is an integer from 1 through 2500000. A value of 0 disables the threshold.

`clear low_thresh`

Default: 0

Specifies the low threshold for the number of HSGW sessions for all HSGW services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` is an integer from 0 and 2500000. A value of 0 disables the threshold.

**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**

Monitor and set alarms or alerts when the total number of HSGW sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for HSGW sessions based on the following rules:

- **Enter condition:** Actual total number of HSGW sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of HSGW sessions is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a total number of HSGW sessions high threshold count of `500000` for a system using the Alert thresholding model:

```
threshold total-hsgw-sessions 500000
```
threshold total-lma-sessions

Configures alarm or alert thresholds for the total number of Local Mobility Anchor (LMA) sessions across all services in the system.

**Product**
- P-GW
- SAEGW

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold total-lma-sessions high_thresh [ clear low_thresh ]
```

*high_thresh*

Default: 0

Specifies the high threshold number of LMA sessions for all LMA services that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 1 through 1500000. A value of 0 disables the threshold.

*clear low_thresh*

Default: 0

Specifies the low threshold number of LMA sessions for all LMA services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 1500000. A value of 0 disables the threshold.

---

**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

Monitor and set alarms or alerts when the total number of LMA sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for LMA sessions based on the following rules:

- **Enter condition:** Actual total number of LMA sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of LMA sessions is less than the 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 to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Examples

The following command configures a total number of LMA sessions high threshold count of 500000 for a system using the Alert thresholding model:

```
threshold total-lma-sessions 500000
```
threshold total-lns-sessions

Configures alarm or alert thresholds for the total number of L2TP Network Server (LNS) sessions in the system.

**Product**
- PDSN
- GGSN
- HA

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold total-lns-sessions high_thresh [ clear low_thresh ]
```

**high_thresh**
Default: 0
Specifies the high threshold number of total LNS sessions that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is an integer from 0 through 4000000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0
Specifies the low threshold number of total LNS sessions that maintains a previously generated alarm condition. If the number of LNS sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` is an integer from 0 and 4000000. A value of 0 disables the threshold.

---

**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
Monitor and set alarms or alerts when the total number of LNS sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for the total number of LNS sessions based on the following rules:

• **Enter condition**: Actual total number of LNS sessions is greater than or equal to the high threshold.

• **Clear condition**: Actual total number of LNS sessions is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Examples
The following command configures a total LNS session high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold total-lns-sessions 10000
```
threshold total-mme-sessions

Configures alarm or alert thresholds for the total number of Mobility Management Entity (MME) sessions across all the MME services in the system.

Product
MME

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description
threshold total-mme-sessions high_thresh [ clear low_thresh ]

high_thresh
Default: 0 (Disabled)
Specifies the high threshold number of total MME sessions that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 2500000. A value of 0 disables the threshold.

clear low_thresh
Default: 0 (Disabled)
Specifies the low threshold number of total MME sessions that maintains a previously generated alarm condition. If the number of MME sessions, across all the services in a system, falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 and 2500000. A value of 0 disables the threshold.

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 monitor and set alarms or alerts when the total number of MME sessions across all the MME services in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for the total number of MME sessions based on the following rules:

- **Enter condition**: Actual total number of MME sessions is greater than or equal to the high threshold.
- **Clear condition**: Actual total number of MME sessions is less than the 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 total-mme-sessions` command to configure the polling interval and the `threshold monitoring mme-service` command to enable thresholding for this value.

**Examples**

The following command configures a total MME session high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold total-mme-sessions 10000
```
**threshold total-pdsn-sessions**

Configures alarm or alert thresholds for the total number of Packet Data Serving Node (PDSN) sessions in the system.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold total-pdsn-sessions high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 0

Specifies the high threshold number of total PDSN sessions that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 2500000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of total PDSN sessions that maintains a previously generated alarm condition. If the number of PDSN sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 and 2500000. A value of 0 disables the threshold.

**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**

Monitor and set alarms or alerts when the total number of PDSN sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for the total number of PDSN sessions based on the following rules:

- **Enter condition:** Actual total number of PDSN sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of PDSN sessions is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a total PDSN session high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold total-pdsn-sessions 10000
```
threshold total-pgw-sessions

Configures alarm or alert thresholds for the total number of Packet Data Network Gateway (P-GW) sessions across all services in the system.

Product

- P-GW
- SAEGW

Privilege

Administrator

Command Modes

- Exec > Global Configuration
- configure

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
threshold total-pgw-sessions high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 0

Specifies the high threshold number of P-GW sessions for all P-GW services that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 1 through 3000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of P-GW sessions for all P-GW services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 3000000. A value of 0 disables the threshold.

**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
Monitor and set alarms or alerts when the total number of P-GW sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for P-GW sessions based on the following rules:

- **Enter condition:** Actual total number of P-GW sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of P-GW sessions is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Examples
The following command configurations a total number of P-GW sessions high threshold count of 500000 for a system using the Alert thresholding model:

```
threshold total-pgw-sessions 500000
```
threshold total-saegw-sessions

Configures alarm or alert thresholds for the total number of System Architecture Evolution Gateway (SAEGW) sessions across all services in the system.

**Product**
SAEGW

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration

```configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold total-saegw-sessions high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 0

Specifies the high threshold number of SAEGW sessions for all SAEGW services that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 1 through 3000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of SAEGW sessions for all SAEGW services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 3000000. A value of 0 disables the threshold.

**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**

Monitor and set alarms or alerts when the total number of SAEGW sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for SAEGW sessions based on the following rules:

- **Enter condition:** Actual total number of SAEGW sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of SAEGW sessions is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a total number of SAEGW sessions high threshold count of 500000 for a system using the Alert thresholding model:

```
threshold total-saegw-sessions 500000
```
threshold total-sgsn-pdp-sessions

Configures alarm or alert thresholds for the total number of PDP contexts for all Serving GPRS Support Node (SGSN) sessions in the system.

Product  SGSN

Privilege  Administrator

Command Modes  Exec > Global Configuration
                configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description  

threshold total-sgsn-pdp-sessions high_thresh [ clear low_thresh ]

high_thresh

Default: 0

Specifies the high threshold number of total PDP contexts per SGSN session for all SGSN services that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 1 through 4000000. A value of 0 disables the threshold.

clear low_thresh

Default: 0

Specifies the low threshold number of total PDP contexts per SGSN session for all SGSN services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

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  Monitor and set alarms or alerts when the total number of SGSN sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for SGSN sessions based on the following rules:

- **Enter condition:** Actual total number of PDP contexts is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of PDP contexts is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a total number of PDP contexts per SGSN session high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold total-sgsn-pdp-sessions 10000
```
threshold total-sgsn-sessions

Configures alarm or alert thresholds for the total number of SGSN sessions in the system.

Product          SGSN

Privilege        Administrator

Command Modes    Exec > Global Configuration
                  configure

Entering the above command sequence results in the following prompt:
[local]host_name(config)#

Syntax Description

threshold total-sgsn-sessions high_thresh [ clear low_thresh ]

high_thresh
Default: 0
Specifies the high threshold number of total SGSN sessions for all SGSN services that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 1 through 2000000. A value of 0 disables the threshold.

clear low_thresh
Default: 0
Specifies the low threshold number of total SGSN sessions for all SGSN services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 2000000. A value of 0 disables the threshold.

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
Monitor and set alarms or alerts when the total number of SGSN sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for SGSN sessions based on the following rules:

- **Enter condition:** Actual total number of SGSN sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of SGSN sessions is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a total number of SGSN sessions high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold total-sgsn-sessions 10000
```
### threshold total-sgw-sessions

Configures alarm or alert thresholds for the total number of Serving Gateway (S-GW) sessions across all services in the system.

**Product**  
S-GW

**Privilege**  
Administrator

**Command Modes**  
Exec > Global Configuration  
`configure`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold total-sgw-sessions high_thresh [ clear low_thresh ]
```

* **high_thresh**  
  Default: 0  
  Specifies the high threshold number of S-GW sessions for all S-GW services that must be met or exceeded within the polling interval to generate an alert or alarm.  
  `high_thresh` is an integer from 1 through 3000000. A value of 0 disables the threshold.

* **clear low_thresh**  
  Default: 0  
  Specifies the low threshold number of S-GW sessions for all S-GW services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.  
  `low_thresh` is an integer from 0 through 3000000. A value of 0 disables the threshold.

---

**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**  
Monitor and set alarms or alerts when the total number of S-GW sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for S-GW sessions based on the following rules:

- **Enter condition**: Actual total number of S-GW sessions is greater than or equal to the high threshold.
- **Clear condition**: Actual total number of S-GW sessions is less than the 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 to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a total number of S-GW sessions high threshold count of 500000 for a system using the Alert thresholding model:

```
threshold total-sgw-sessions 500000
```
throttling-override-policy

Creates a GTP-C Throttling Override Policy. Entering this command creates a Throttling Override Policy mode. Use this mode to configure the Throttling Override Policy that can be used at the GGSN/P-GW nodes to selectively bypass throttling for a configured message type or for the configured APN.

**Product**
- GGSN
- P-GW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration
  - configure
  
  Entering the above command sequence results in the following prompt:
  
  `[local] host_name(config)#`

**Syntax Description**

`throttling-override-policy throttling-override-policy_name`

- `throttling-override-policy`
  
  Creates a GTP-C throttling override policy.

  `throttling-override-policy_name` is a throttling override policy name for the policy that can be used at the GGSN/P-GW nodes.

**Usage Guidelines**

Enter this command mode to configure the Throttling Override Policy that can be used at the GGSN/P-GW nodes to selectively bypass throttling for a configured message type or for the configured APN.

**Examples**

Use the following command to enter throttling-override-policy mode:

`throttling-override-policy throttling-override-policy_name`
timestamps

Enables or disables the generation of a timestamp in response to each commands entered. The timestamp does not appear in any logs as it is a CLI output only. This command affects all future CLI sessions. Use the `timestamps` command in the Exec Mode to change the behavior for the current CLI session only.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

- `timestamps`
- `no timestamps`

- `no`

Disables generation of timestamps for each command entered. When omitted, the output of a timestamp for each entered command is enabled.

**Usage Guidelines**

Enable the timestamps when logging a CLI session on a remote terminal such that each command will have a line of text indicating the time when the command was entered.

**Examples**

The following commands enable and disable timestamps for each CLI command:

- `timestamps`
- `no timestamps`

- `no`
traffic shape

Configures the maximum buffer limit for sessmgr and subscribers for use during traffic shaping.

Product
- GGSN
- P-GW
- SAEGW

Important
Traffic Shaping is a license-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

Privilege
Administrator, Security Administrator

Command Modes
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax Description
- traffic shape max-buffer-size sessmgr MBs subscriber MBs
default

- traffic shape max-buffer-size

default
Returns sessmgr and subscriber settings to their default values.
Default setting for the sessmgr is 10MB. Default setting for the subscriber is 1MB.

- traffic
Allows configuration for data traffic.

- shape
Allows configuration for traffic shaping.

- max-buffer-size
Allows configuration of the maximum buffer size for the session manager and subscriber.
**sessmgr**

Specifies the maximum buffer limit for the session manager for use during traffic shaping.

Valid entries are from 1 to 100 MB.

The default is 10 MB.

The sessmgr value should be greater than the subscriber value.

---

**Caution**

Standard size buffers (500, 2k, and 10k bytes) are used for buffering packets to avoid memory fragmentation. As a result, there may be additional memory overhead in the memory used for buffering. The buffer limit in the above configuration refers to actual effective bytes used to store packets. Use caution to use appropriate buffer limits, so that the system does not significantly affect the overall Session Manager memory requirement for sessions.

---

**subscriber**

Specifies the maximum buffer limit for subscriber use during traffic shaping.

Valid entries are from 1 to 100 MB.

The default is 1 MB.

The subscriber value should be less than the sessmgr value.

---

**Usage Guidelines**

Use this command to set the maximum memory buffer limit for session manager and subscriber use during traffic shaping.

Traffic shaping and policing must first be configured in **APN Configuration Mode** using the apn-ambr command before the traffic shape command can be used.

---

**Examples**

The following example configures the maximum buffer size for the sessmgr at 20 MB, and configures the maximum buffer size for subscriber at 2 MB:

```
traffic shape max-buffer-size sessmgr 20 subscriber 2
```
unexpected-scenario session drop-call

Configures behavior when an unexpected call processing scenario is encountered. Enabling this command sets call clearing logic that replaces the automatic generation of asserts and core dumps for an initial assert.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
```
unexpected-scenario session drop-call | disable-core |
default unexpected-scenario session drop-call
```

- **default**
  Disables call clearing logic for a graceful assert. This results in automatic core dump generation for unexpected scenarios resulting in control and data outage for the task instance until the core is fully generated.

- **disable-core**
  This option disables the automatic generation of core dumps when a call is dropped for a specific session.

**Usage Guidelines**
Use this command to enable call clearing logic that will minimize the automatic generation of asserts and core dumps during a specific call processing session that may lead to data outage and session manager recovery. The call clearing logic is only applied to the first assert generated during a call processing session. When that assert occurs, a zero-second timer lets the current stack unwind to avoid reentrancy issues. The call is then dropped from all interfaces. This is considered to be a graceful assert.

A core dump is generated along with any application supplied debug info. The line number and file index of the ASSERT appears in the call-line; the current call-line is marked as being in "assert_hit" scenario.

With the **disable-core** option set, a core dump is **not** generated following a graceful assert.

An assert generated after a graceful assert for the same unexpected scenario will cause the call to be dropped and trigger an automatic core dump. Depending on the length of time required to generate the associated core dump, a session manager recovery may be initiated. This is a highly unlikely possibility.
The graceful assert call clearing logic can only be applied to call processing events, such as VoLTE. It cannot be used for ICSR-SRP scenarios.

The following command enables call clearing logic for graceful asserts of initial call processing failures:

```
unexpected-scenario session drop-call disable-core
```
upgrade limit

Configures upgrade session limits that trigger when the system may execute the software upgrade.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
upgrade limit [ time session_life ] [ usage session_num ]
```

**upgrade limit**

This command issued with no keywords sets all parameters to their defaults.

**time session_life**

Default: 120

Defines the maximum number of minutes that a session may exist on the system undergoing a software upgrade, before it is terminated by the system. As individual user sessions reach this lifetime limit, the system terminates the individual session(s). *session_life* must be an integer ranging from 1 through 1440.

**usage session_num**

Default: 100

This keyword defines a low threshold limit of sessions running either on a packet processing card or system-wide. When a software upgrade is invoked, this parameter applies to the entire system.

When the threshold is crossed (when the number of sessions on the packet processing card or system is less than this value), the remaining sessions on the card or system are terminated allowing the upgrade to begin. The remaining sessions on the packet processing card or system are terminated regardless of their session life. *session_num* must be an integer from 0 through 6000.

**Usage Guidelines**

Use this command to configure upgrade session limits that trigger the system to begin executing the software upgrade.
Important  This command is not supported on all platforms.

Important  Software Patch Upgrades are not supported in this release.

Examples  The following command sets the number of minutes a session can exist to 200, and the minimum number of sessions that may exist before terminating them to 50:

```
upgrade limit time 200 usage 50
```
url-blacklisting database

This command configures URL Blacklisting database directory parameters.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
url-blacklisting database { directory path path | max-versions max_versions | override file file_name }
default url-blacklisting database { directory path | max-versions | override file }

default
Configures this command with the default settings.

directory path path
Specifies the path to the directory to be used for storing URL Blacklisting databases.
path must be an alphanumeric string of 1 through 255 characters.
Default: /flash/bl

max-versions max_versions
Specifies the maximum number of URL Blacklisting database versions to be maintained in the URL Blacklisting database directory path with the base file name specified by the URL Blacklisting database override file.
max_versions must be an integer from 0 through 3.
Default: 0

override file file_name
Specifies the URL Blacklisting database override file name.
file_name must be in name.extension format. For example, abc.bin. And, must be an alphanumeric string of 1 through 10 characters.
Default: optblk.bin
Usage Guidelines

Use this command to configure URL Blacklisting database directory parameters.

Examples

The following command configures the maximum number of URL Blacklisting database versions to be maintained to 3:

```
url-blacklisting database max-versions 3
```
wsg-lookup

Enters the WSG lookup priority list configuration mode for site-to-site tunnels.

Product
WSG

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax Description
wsg-lookup

Usage Guidelines
Use this command to enter the WSG lookup priority list configuration mode for site-to-site tunnels.

Examples
The following command enters the SG lookup priority configuration mode:

wsg-lookup
Global Title Translation Address-Map Configuration Mode Commands

The Global Title Translation (GTT) Address Map Configuration is a sub-mode of Global Title Translation Mode. This mode is used to create and configure the GTT database.

This chapter describes the Global Title Translation Address-Map Configuration Mode.

Command Modes

Exec > Global Configuration > GTT Address-Map
configure > global-title-translation > address-map instance instance

Entering the above command sequence results in the following prompt:

[local] host_name(config-gtt-addrmap-instance)#

Important

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

- associate, page 966
- description, page 968
- do, page 969
- end, page 970
- exit, page 971
- gt-address, page 972
- mode, page 973
- out-address, page 974
**associate**

This command allows the user to configure the gtt-association.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Global Title Translation Address-Map Configuration

configure > global-title-translation address-map instance instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-gtt-addrmap-instance)#

**Syntax Description**

[no] associate gtt-association instance action id action_id

*no*

Removes the configured gtt-association.

*gtt-association*

This keyword is used to specify the gtt-association to be used.

*instance*

Specifies the gtt-association instance to be used. The instance is an integer value from 1 up to 16.

*action*

This keyword is used to specify the action for the rule. The actions are configured by the `action` command in the GTT Association Configuration Mode. For more information see the Global Title Translation Association Configuration Mode chapter.

*id*

This keyword is used to specify the action id. The action id's are associated with specific action types in the GTT Association Configuration Mode. For more information see the Global Title Translation Association Configuration Mode chapter.

*action_id*

The `action_id` is an integer value from 1 up to 15.
Usage Guidelines

This command allows the user to configure the gtt-association. The instance and the action can be configured using this command. The Action Id's are configured using the `action` command under the GTT Association Configuration Mode. For more information see *Global Title Translation Association Configuration Mode* chapter.

Examples

This command configures gtt-association for instance 12 and specifies the action id as 10:

```
associate gtt-association 12 action id 10
```
description

Allows the user to enter a descriptive text for this configuration.

Product  SGSN

Privilege  Security Administrator, Administrator

Command Modes  Exec > Global Configuration > Global Title Translation Address-Map Configuration

configure > global-title-translation address-map instance  instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-gtt-addrmap-instance)#

Syntax Description

description  text

no  description

no

Clears the description for this configuration.

text

Enter descriptive text as a string of 1 up to 127 characters.

Usage Guidelines

The description should provide useful information about this configuration.
do

Spawns an Exec mode command which displays information to the administrator.

**Product**

All

**Privilege**

Administrator

**Syntax Description**

`do show show_command_options`

`show show_command_options`

Executes an exec mode `show` command and immediately returns back to the current configuration mode.

`show_command_options` lists the various show commands available for the administrator.

**Usage Guidelines**

Use this command to display show command information to the administrator and immediately return back to the current configuration mode.
end

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

Product
All

Privilege
Security Administrator, Administrator

Syntax Description
end

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

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax Description**
exit

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

This command allows the user to configure the SCCP short address.

**Product**  
SGSN

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration > Global Title Translation Address-Map Configuration  
configure > global-title-translation address-map instance *instance*  

Entering the above command sequence results in the following prompt:  
[local]host_name(config-gtt-addrmap-instance)#

**Syntax Description**  
\[gt-address \texttt{gt\_address}\]  
\[no gt-address\]

no  
Removes the configured SCCP short address.

\[gt\_address\]

The gt-address is a numerical string of size 1 up to 15. The length of the address should be greater than or equal to the end-digit of the associated action-id.

**Examples**  
This command configures the gt-address of the SCCP entity as *101011*:  
\[gt-address 101011\]
mode

This command allows the user to configure the mode of operation of SCCP entities.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Global Title Translation Address-Map Configuration

configure > global-title-translation address-map instance instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-gtt-addrmap-instance)#

Syntax Description mode { dominant | loadshare }

dominant

This keyword configures the mode of operation of SCCP entities as dominant. In this mode even if multiple out-addresses are configured the first out-address will be used for handling all the signaling traffic. The next available out-address is chosen for handling all the signaling traffic if any out-address is not available. For example, if the first out-address is not available the second out-address is used for handling all the signaling traffic.

loadshare

This keyword configures the mode of operation of SCCP entities as loadshare. In this mode if multiple out-addresses are configured then the load of signaling traffic is shared among all the out-addresses configured. This is also the default mode.

Examples This command configures the mode of operation of SCCP entities as dominant:

mode dominant
out-address

This command allows the user to configure the outgoing address and outbound parameters of the SCCP entity.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Global Title Translation Address-Map Configuration

configure > global-title-translation address-map instance instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-gtt-addrmap-instance)#

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] out-address address_name</td>
<td>no</td>
</tr>
</tbody>
</table>

no

Removes the configured outgoing address and outbound parameters of the SCCP entity.

**address_name**
The address name is a string of size 1 up to 63.

**Usage Guidelines**
This command allows the user to configure the outgoing address of the SCCP entity, the user enters the Out-Address Configuration mode where the outbound parameters for the SCCP entities as part of the gtt-address-map configuration can be configured. For more information see Out-Address Configuration Mode Commands chapter in the Command Line Interface Reference, Commands I - Q document.

**Examples**

This command configures the outgoing address of the SCCP entity as sccp1:

out-address sccp1
Global Title Translation Association Configuration Mode Commands

The Global Title Translation (GTT) Association Configuration is a sub-mode of Global Title Translation Mode. This mode is used to create and configure the GTT association which defines the rules for handling global title translation.

This chapter describes the Global Title Translation Association Configuration Mode

**Command Modes**

Exec > Global Configuration > GTT Association

```
configure > global-title-translation > association instance instance
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-gtt-asso-instance)#
```

---

**Important**

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

- action, page 976
- description, page 978
- do, page 979
- end, page 980
- exit, page 981
- gt-format, page 982
- variant, page 983
**action**

This command allows the user to configure the action type for specific action id's.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Global Title Translation Association Configuration

```
configure > global-title-translation association instance instance
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-gtt-asso-instance)#
```

**Syntax Description**

```
[no] action action_id action_type start-digit start_digit_value end-digit end_digit_value
```

- **no**
  
  Removes the action type defined for the action id's.

- **action**
  
  Specifies the action for the rule.

- **id**
  
  This keyword is used to specify the action id.

  - **action_id**
    
    The `action_id` is an integer value from 1 up to 15.

- **type**
  
  This keyword is used to specify the action type.

  - **action_type**
    
    The supported action types are listed below:
    
    - **constant**: Translate incoming GT to a fixed address.
    - **fixed**: Fixed range of digits to perform GTT.
• **gt-to-pc**: Use digits in incoming GT digits as PC for routing.

• **insert-pc**: Insert DPC before incoming GTAI and change TT,ES and NAI.

• **selins**: Selective Insertion type to perform GTT.

• **strip-pc**: Strip first the "6" digits from GTAI if first "6" digits in SPC are in INT format.

• **var-asc**: Variable number of digits in ascending order to perform GTT.

• **var-des**: Variable number of digits in descending order to perform GTT.

### start-digit `start_digit_value`

Specifies the ending digit of the range. The `start_digit_value` is an integer value from 0 up to 255. The start digit value must be less than or equal to the end digit value.

### end-digit `end_digit_value`

Specifies the starting digit of the range. The `end_digit_value` is an integer value from 0 up to 255.

#### Usage Guidelines

The action id's can be configured for the GTT address-maps. Each action id is associated with a specific type of action. For more information see the `associate` command in the *Global Title Translation Address-Map Configuration Mode* chapter.

#### Examples

Listed below is an example where the action id "10" is defined with action type "fixed" along with start and end digits as "10" and "23" respectively:

```
action_id 10 type fixed start-digit 10 end-digit 23
```
**description**

Allows the user to enter a descriptive text for this configuration.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Global Title Translation Association Configuration

configure > global-title-translation association instance  instance

Entering the above command sequence results in the following prompt:

[local] host_name(config-gtt-asso-instance)#

**Syntax Description**

- **description**
- **text**
- **no description**

- **no**

  Clears the description for this configuration.

- **text**

  Enter descriptive text as a string of 1 up to 127 characters.

**Usage Guidelines**

The description should provide useful information about this configuration.
do

Spawns an Exec mode command which displays information to the administrator.

Product

All

Privilege

Administrator

Syntax Description

do show show_command_options

show show_command_options
Executes an exec mode show command and immediately returns back to the current configuration mode.
show_command_options lists the various show commands available for the administrator.

Usage Guidelines

Use this command to display show command information to the administrator and immediately return back to the current configuration mode.
end

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax Description**
end

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

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

exit

Usage Guidelines

Use this command to return to the parent configuration mode.
gt-format

This command configures Global Title Translation format in the GTT process.

Product
SGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Global Title Translation Association Configuration
configure > global-title-translation association instance  instance

Entering the above command sequence results in the following prompt:
[local]host_name(config-gtt-asso-instance)#

Syntax Description
[no] gt-format  format_number

no
Removes the configured format.

format_number
The format_number is an integer value from 1 up to 4. The format numbers correspond to the following formats:

- 1: Format 1
- 2: Format 2
- 3: Format 3
- 4: Format 4

Usage Guidelines
On configuring this command, the user enters the specified GT-Format mode. Each format has specific commands to define rules for GTT. For more information see GT-Format1/GT-Format2/GT-Format3/GT-Format4 Configuration Mode Commands chapters.

Examples
Listed below is an example where the GT-format is chosen as "1" which corresponds to GT-Format1 and enters the GT-Format1 Configuration Mode:

gt-format  1
**variant**

This command configures Global Title Translation (GTT) network variant.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Global Title Translation Association Configuration

```bash
configure > global-title-translation association instance instance
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-gtt-asso-instance) #
```

**Syntax Description**

```
variant variant
```

`variant`

The available options of network variant are listed below:

- `ansi`
- `china`
- `itu`
- `japan`

**Examples**

Listed below is an example where the network variant is selected as `ansi`:

```
variant ansi
```
GPRS Service Configuration Mode Commands

The GPRS Service Configuration Mode is used within the context configuration mode to define the criteria the SGSN needs to operate within a GPRS network. The GPRS Service works with other services, such as SGSN GPRS Tunneling Protocol (see SGTP Service Configuration Mode Commands) and Mobile Application Part (see MAP Service Configuration Mode Commands), to handle communication parameters required to work with other network entities such as the base station subsystem (BSS).

Command Modes

Exec > Global Configuration > Context Configuration > GPRS Service Configuration

configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

[(context_name) host_name] (config-gprs-service) #

Important

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

- accounting, page 987
- admin-disconnect-behavior, page 989
- associate, page 991
- associate-dscp-template, page 995
- associate-service, page 997
- cc profile, page 999
- check-imei, page 1001
- check-imei-timeout-action, page 1003
- ciphering-algorithm, page 1004
- dns mcc-mnc-encoding, page 1007
- dns israu-mcc-mnc-encoding, page 1009
- end, page 1011
• exit, page 1012
• gmm, page 1013
• llc, page 1019
• network-sharing, page 1023
• nri, page 1026
• paging-policy, page 1029
• peer-nsei, page 1031
• plmn, page 1033
• rai-skip-validation, page 1035
• reporting-action event-record, page 1036
• s4-overcharge-protection, page 1038
• setup-timeout, page 1040
• sgsn-context-request, page 1041
• sgsn-number, page 1042
• sm, page 1043
• sndcp, page 1046
accounting

Defines the accounting context name and enables/disables specific types of CDR generation for the accounting in the GPRS service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GPRS Service Configuration
`configure > context context_name > gprs-service service_name`

Entering the above command sequence results in the following prompt:
`{context_name}@host_name(config-gprs-service)#`

**Syntax Description**
`accounting { cdr-types { mcdr | scdr | sms { mo-cdr | mt-cdr } | lcs { mt-cdr | mo-cdr } | smbmscdr }+ | context cntx_name }`
`default accounting cdr-types`
`no accounting { cdr-types | context }`

**default**
Returns the system to default CDR generation which includes:
- M-CDR
- S-CDR
- SMS CDRs
- LCS CDRs
- SMBMS CDR

**no**
Disables all CDR types.

`cdr-types { mcdr | scdr | sms { mo-cdr | mt-cdr } | lcs { mt-cdr | mo-cdr } | smbmscdr }`
Default: all types enabled.

Defines the types of CDRs to be generated within the specified GPRS service for accounting:
- **mcdr**: Enables generation of M-CDRs.
• **scdr**: Enables generation of S-CDRs.

• **sms**: Enables generation of SMS-type CDRs based on one of the following:
  - **mo-cdr**: SMS CDRs originates from the mobile.
  - **mt-cdr**: SMS CDRs terminates at the mobile.

• **smbmscdr**: This CDR type is currently under development and should not be included in configuration for this release.

• **lcs**: Enables the generation of LCS CDRs, based on:
  - **mt-cdr**: Mobile terminated location request CDR
  - **mo-cdr**: Mobile originated location request CDR

+ This symbol indicates that more than one keyword can be used and repeated. This enables you to include more than one type of CDR selection in a single command.

**context cntx_name**

Specifies an accounting context to be associated with the GPRS service.

*cntx_name*: Define a string of 1 to 79 alphanumeric characters.

**Usage Guidelines**

Use this command to define the type of CDRs to generate for GPRS service. By default all types of CDRs are generated. Note that change of this configuration will be applied to new calls and/or to new PDP contexts only.

By default, the generation of all CDR types is enabled.

**Examples**

The following command configures the system to generate only M-CDRs for accounting in the current GPRS service:

```
accounting cdr-types mcdr
```
admin-disconnect-behavior

This command defines some of the actions the SGSN will take during an Admin-Disconnect procedure.

Product: SGSN

Privilege: Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > GPRS Service Configuration
configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:
[context_name]host_name(config-gprs-service)#

Syntax Description
admin-disconnect-behavior { clear-subscription | detach-type { reattach-not-required | reattach-required }
}

default admin-disconnect-behavior { clear-subscription | detach-type }

clear-subscription
Including this keyword in the configuration instructs the SGSN to clear subscriber contexts and the subscription data database whenever the clear subscribers all command is issued (from the Exec mode) for attached subscribers. As well, the SGSN will issue an appropriate Map-Purge-MS-Req to the HLR if needed.
Default: disabled

detach-type
Including this keyword defines which type of detach instruction to include in the Detach-Request message during an Admin-Disconnect procedure. One of the following options must be included when this command is entered:

- reattach-not-required
- reattach-required

Default: reattach-required

default
Including the default keyword in the command, instructs the SGSN to use the default value for the specified parameter.
no

Returns the SGSN to the default where this clear function is disabled

**Usage Guidelines**

Using the `clear subscribers all` command (in the Exec Mode) clears subscriber contexts and the subscription data database, and if needed, issues an appropriate Map-Purge-MS-Req to the HLR.

Include the `clear-subscription` keyword with this command configuration to ensure that more than attached MM-context and active PDP-contexts are cleared when the clear `subscribers all` command is issued for attached subscribers.

To clear subscription data for detached subscribers, refer to the `sgsn clear-detached-subscriptions` command described in the Exec mode chapter.

Including the `detach-type` keyword with this command instructs the SGSN to include either a 'reattach-required' or a 'reattach-no-required' instruction in the Detach-Request message.

**Examples**

Enable the clearing function so that subscription data is cleared from the HLR database:

```
admin-disconnect-behavior
clear-subscription
```
associate

Associates or disassociates supportive services and policies, such as an Evolved GPRS Tunnelling Protocol (eGTP) service or a DSCP marking template with this GPRS service configuration.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GPRS Service Configuration

configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gprs-service)#

Syntax Description

associate { { camel-service service_name | context context_name | dscp-template downlink
dscp_template_name | egtp-service egtp_svc_name | context context_name | gs-service gs_svc_name |
context context_name | hss-peer-service hss_svc_name | context context_name | location-service loc_name
| map-service map_svc_name | context context_name | network-global-mme-id-mgmt-db | sgtp-service
sgtp_svc_name | context context_name | tai-mgmt-db database_name }

no associate { camel-service | dscp-template downlink | egtp-service | gs-service | hss-peer-service |
location-service | map-service | network-global-mme-id-mgmt-db | sgtp-service | tai-mgmt-db }

no

Disassociates a previously associated service, DSCP marking template or management database with this GPRS service.

context ctx_name

Identifies an existing context name in which the named service is configured. If this keyword is omitted, the named service must exist in the same context as the GPRS service.

ctx_name- Enter an alphanumeric string of 1 through 63 characters.

camel-service camel_svc_name

Associates a CAMEL service with this GPRS service.

camel_svc_name specifies the name for a configured CAMEL service to associate with the GPRS service.
Enter an alphanumeric string of 1 to 63 characters.
**dscp-template downlink** `template_name`
Associates a DSCP template with the GPRS service.

`template_name` specifies a configured DSCP marking template to associate with this GPRS service. Enter an alphanumeric string of 1 to 64 characters.

**egtp-service** `egtp_svc_name`
Associates an eGTP service with GPRS service.

`egtp_svc_name` specifies the name for a configured eGTP service to associate with this GPRS service. Enter an alphanumeric string of 1 to 63 characters.

The eGTP service is created with the `egtp-service` command in the *Context Configuration Mode Commands* chapter. The eGTP service provides eGTP-C protocol interface support between the SGSN and EPS nodes. For more information on the eGTP service and the supported interface type(s), refer to the *eGTP Service Configuration Mode Commands* chapter.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only one eGTP service can be associated with a GPRS service. The eGTP service should be configured prior to issuing this command.</td>
</tr>
</tbody>
</table>

**gs-service** `gs_svc_name`
Associates a Gs service with this GPRS service.

`gs_svc_name` specifies the name for a configured Gs service to associate with the GPRS service. Enter an alphanumeric string of 1 to 63 characters.

The Gs service is created with the `gs-service` command in the *Context Configuration Mode Commands* chapter. The Gs service provides Gs interface support between the SGSN and MSC/VLR nodes. For more information on the Gs service and the supported interface type, refer to the *Gs Service Configuration Mode Commands* chapter.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only one Gs service can be associated with a GPRS service. The Gs service should be configured prior to issuing this command.</td>
</tr>
</tbody>
</table>

**hss-peer-service** `hss_svc_name`
Associates an HSS peer service with this GPRS service.

`hss_svc_name` specifies the name for a configured HSS peer service to associate with this GPRS service. Enter an alphanumeric string of 1 to 63 characters.

The HSS peer service provides S6d and S13-prime interface support via the Diameter protocol between the GPRS and an HSS (S6d) or EIR (S13-prime). For more information about the HSS peer service, refer to the `hss-peer-service` command in the *Context Configuration Mode Commands* chapter and the *HSS Peer Service Configuration Mode Commands* chapter.
Only one HSS peer service can be associated to a service in this release. The HSS peer service should be configured prior to issuing this command.

Important

**location-service** `loc_svc_name`

**map-service** `map_svc_name`

Associates a location service with this GPRS service.

`loc_svc_name` specifies the name for a pre-configured location service to associate with the GPRS service. Enter an alphanumeric string of 1 to 63 characters.

The location service is created with the **location-service** command in the *Context Configuration Mode Commands* chapter. For more information on the location services, refer to the *Location Services Configuration Mode* section.

Important

Only one MAP service can be associated with a GPRS service. The MAP service should be configured prior to issuing this command.

**network-global-mme-id-mgmt-db**

Associates the configured global MME ID management database with the GPRS service. This enables operators to associate a single custom list of MME Group IDs for use in GPRS to E-UTRAN handovers on the S4-SGSN. The global MME ID management database is configured in the *LTE Policy Configuration Mode* using the **network-global-mme-id-mgmt-db** command.

This command is available only if the *SGSN S4 Interface* license is enabled on the SGSN.

**sgtp-service** `sgtp_svc_name`

Associates an SGTP service with this GPRS service.

`sgtp_svc_name` specifies the name for a configured SGTP service to associate with the GPRS service. Enter an alphanumeric string of 1 to 63 characters.

The SGSN GPRS Tunneling Protocol (SGTP) service manages the configuration of the GTP-C and GTP-U related parameters. For more information on the SGTP service, refer to the **sgtp-service** command in the *Context Configuration Mode Commands* chapter and/or the *SGTP Service Configuration Mode Commands* chapter.

Important

Only one SGTP service can be associated with a GPRS service. The SGTP service should be configured prior to issuing this command. When co-locating an SGSN and MME, the GPRS Service cannot be associated with the same SGTP service that is used by the MME.

**tai-mgmt-db** `database_name`

Associates this GPRS service with a pre-configured TAI Management Database.
database_name specifies the name of a pre-configured TAI Management Database to associate with the SGSN service as alphanumeric string of 1 through 64 characters. For more information on subscriber maps, refer to the tai-mgmt-db command in the LTE Policy Configuration Mode Commands chapter and the LTE TAI Management Database Configuration Mode Commands chapter.

This command is available only if the SGSN S4 Interface license is enabled on the SGSN.

Usage Guidelines

Use this command to associate a pre-configured service and/or DSCP marking template and/or management database with this GPRS service. The command can be repeated as necessary to configure associations for all desired services/templates/databases.

Caution

This is a critical configuration. The GPRS service cannot be started without this configuration. Any change to this configuration would lead to restarting the GPRS service. Removing or disabling this configuration will stop the GPRS service.

Examples

The following command associates a previously-configured eGTP service called egtp1 in the dst_ctx context to this GPRS service:

```plaintext
associate egtp-service egtp1 context dst_ctx
```

The following command disassociates a MAP service called map1 that was previously associated with this GPRS service:

```plaintext
no associate map-service egtp1
```

The following command associates an HSS peer service called hss1, previously-configured in the same context as the GPRS service, to this GPRS service:

```plaintext
associate hss-peer-service hss1
```

The following command associates a previously-configured DSCP marking template called dscp-temp1 to this GPRS service:

```plaintext
associate dscp-template downlink dscp-temp1
```
associate-dscp-template

Identifies a DSCP template to be associated with the GPRS service.

Important

This command is used only in Releases 12.0 and 12.2. For Release 14.0 refer to the associate command.

Important

This command can be used before the associated DSCP template instance is created and configured but care should be used to match the template names.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GPRS Service Configuration

configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gprs-service)#

Syntax Description

associate-dscp-template downlink template_name
no associate-dscp-template downlink

no

Removes the template association definition from the configuration.

template_name

Specifies a unique DSCP template to associate with this GPRS service.

template_name must be a string of 1 to 64 alphanumeric characters with dots (.), dashes (-), and forward slashes (/) but with no spaces.

Usage Guidelines

Use this command to associate DSCP templates with this GPRS service. A single template can be associated with multiple GPRS services.

Related commands:
- The `dscp-template` command in the SGSN Global configuration mode creates / deletes an instance of a template. This command also provides access to the mode containing all the configuration commands used to define DSCP settings for the control packets for the Iu interface and the control and data packets for the Gb interface (see the DSCP Template Configuration Mode Commands chapter).

- To check the list of DSCP templates configured, use the `show sgsn-mode` command documented in the Exec Mode Commands chapters.

Examples

The following command associates the template with DSCP settings for traffic going through one of the SGSNs located in the `paris3` mobile network:

`associate-dscp-template dscp-template-paris3`
associate-service

Identifies services to be associated with the GPRS Service.

Important

This command is used only in Releases 12.0 and 12.2. For Release 14.0 refer to the associate command.

Important

This command can be used before the associated service instance is created and configured but care should be used to match the service names.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GPRS Service Configuration

configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gprs-service)#

Syntax Description

[ no ] associate-service { gs name | map name | sgtp name } [ context ctxt_name ]

no

Removes the service association definition from the configuration.

gs name

Specifies the Gs service configuration to associate with this GPRS service.

name must be a string of 1 to 63 alphanumeric characters with no spaces.

map name

Specifies the MAP service configuration to associate with this GPRS service.

name must be a string of 1 to 63 alphanumeric characters with no spaces.

sgtp name

Specifies the SGTP service configuration to associate with this GPRS service.
name must be a string of 1 to 63 alpha numeric characters with no spaces.

context ctxt_name
Defines the context in which the service was created.
ctxt_name must be a string of 1 to 63 alphanumeric characters with no spaces.

Usage Guidelines
Use this command to associate other services, that have been or will be configured, to this GPRS service.

Examples
The following command associates Gs service gs1 with this GPRS service.
associate-service gs gs1 context sgsn2
**cc profile**

Configures the charging characteristic (CC) profile index properties.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GPRS Service Configuration

    configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

    [context_name]host_name(config-gprs-service)#

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] cc profile index { buckets number</td>
</tr>
</tbody>
</table>

**no**

Removes the a specific charging characteristics configuration definition.

**default**

Resets the charging characteristics to system defaults.

**index**

Configures a profile index for the parameter to be specified. index can be configured to any integer from 0 to 15.

---

**Important**

3GPP standards suggest that profile index values of 1, 2, 4, and 8 be used for hot billing, flat rate billing, prepaid billing and normal billing, respectively. A single charging characteristics profile can contain multiple behavior settings.

**buckets number**

Default: 4

Specifies the number of statistics container changes due to QoS changes or tariff time that can occur before an accounting record should be closed.
number can be configured to any integer value from 1 through 4.

**interval time**

time is measured in seconds and can be configured to any integer from 60 to 40,000,000.

**tariff time1 mins hours time2 mins hours time3 mins hours time4 mins hours**

Specifies time-of-day time values to close the current statistics container (but not necessarily the accounting record). Six different tariff times may be specified. If less than six times are required, the same time can be specified multiple times.

---

**Important**
The system assumes that the billing system uses the day/date to determine if the statistics container represents an actual tariff period.

For each of the different tariff times, the following parameters must be configured:

- **mins**: The minutes of the hour, an integer from 0 to 59.
- **hours**: The hour of the day, an integer from 0 to 23.

**volume { downlink vol_down_octets uplink vol_up_octets | total total_octets }**

Specifies the downlink, uplink, and total volumes that must be met before closing a CDR.

- **vol_down_octets**: Measured in octets; can be configured to any integer from 100,000 to 4,000,000,000.
- **vol_up_octets**: Measured in octets; can be configured to any integer from 100,000 to 4,000,000,000.
- **total_octets**: The total traffic volume (up and downlink) measured in octets; can be configured to any integer from 100,000 to 4,000,000,000.

---

**Usage Guidelines**

Charging characteristics consist of a profile index and behavior settings. This command configures profile indexes for the SGSN's charging characteristics. The SGSN supports up to 16 profile indexes.

This command works in conjunction with the cc-sgsn command located in the APN configuration mode that dictates which CCs should be used for subscriber PDP contexts.

**Examples**

The following command configures a profile index of 10 for tariff times of 7:00 AM and 7:30 PM:

```
cc profile 10 tariff time1 0 7 time2 30 19
```
check-imei

Configures the action the SGSN will take if the route towards the Equipment Identity Register (EIR) is down.

**Product**  
SGSN

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration > Context Configuration > GPRS Service Configuration  
`configure > context context_name > gprs-service service_name`

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

**Syntax Description**

- `check-imei {gf-failure-action|gf-timeout-action} {continue | reject}`
- `default check-imei {gf-failure-action | gf-timeout-action}`

- `default`
  
  Resets the default function to reject the Attach.

- `gf-failure-action`
  
  Coupled with either `continue` or `reject`, this keyword instructs the SGSN to take action if a valid EIR configuration exists under the MAP service and if the EIR is temporarily unreachable due to associated DPC/SSN inaccessible/out-of-service.

- `gf-timeout-action`
  
  Coupled with either `continue` or `reject`, this keyword instructs the SGSN to take action if a valid EIR configuration exists under the MAP service and the route to the EIR is available, but no response is received from the EIR.

- `continue`
  
  Instructs the SGSN to continue the Attach process.

- `reject`
  
  Instructs the SGSN to reject the Attach process.
Usage Guidelines

Typically, the Attach process will be continued when there is an IMEI check timeout based on the configuration under the SGSN service configuration and/or the GPRS service configuration. But this works only if the route towards the EIR is UP and the IMEI request timer expires. This command configures the SGSN to allow the Attach process to continue in the case the route towards the EIR is down, that is the DPC/SSN is out-of-service.

Examples

Use the following command to reset the default and reject Attach:

default check-imei gf-failure-action
check-imei-timeout-action

This command has been deprecated.
ciphering-algorithm

Configures the priority, ordering, for the use of the GPRS encryption ciphering algorithms.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-gprs-service)#

**Syntax Description**

ciphering-algorithm { negotiation-failure-action { reject [ failure-code cause_code ] | use-geo0 } priority priority } default
default

Returns the system ciphering-algorithm priority to the default of GEA0 - which means that no ciphering will be done.

negotiation-failure-action { reject [ failure-code cause_code ] | use-geo0 }

This set of keywords configure the SGSN's action if there is not a match between the MS and SGSN ciphering algorithm configurations.

- **reject**: Instructs the SGSN to reject a call when the ciphering algorithms do not match.
- **failure-code cause_code**: Instructs the SGSN to include a GMM cause code in the Reject message. Enter an integer from 2 to 111; default code is 14 (GPRS services not allowed in this PLMN). Refer to the GMM failure cause codes listed below (information has been taken 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

• **use-geo0**: Instructs the SGSN to honor the Attach/RAU Request without ciphering (geo0). This is the default action for negotiation failure.

**priority priority algorithm**

Defines the priority, order of use, for the ciphering algorithm.

*priority*: Must be an integer from 1 to 4.

**algorithm**

Identifies the algorithm to be matched to the priority. Options include:

- gea0 - No ciphering
- gea1 - GPRS Encryption Algorithm - GEA1
- gea2 - GPRS Encryption Algorithm - GEA2
- gea3 - GPRS Encryption Algorithm - GEA3

**Usage Guidelines**

Use this command to specify the order (priority) of usage for the GPRS encryption algorithms. All of the GPRS encapsulation algorithms use a 64-bit key derived from a common mechanism: the mobile receives a random challenge, then the SIM calculates an authentication signature and an encryption key.

Also use this command to define the action to be taken if there is not a match between the MS and the SGSN ciphering algorithm configurations.

**Examples**

The following command sets no ciphering to be used after two encryption algorithms have been used:
```
ciphering-algorithm priority 3 gea0
```

The following command configures the SGSN to reject calls if the ciphering algorithm configurations don't match:
```
ciphering-algorithm negotiation-failure-action reject
```
**dns mcc-mnc-encoding**

Configures the encoding format for the MCC and MNC values in the DNS query.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GPRS Service Configuration
configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gprs-service)#
```

**Syntax Description**

```
dns mcc-mnc-encoding { apn-fqdn | mmec-fqdn | rai-fqdn| rnc-fqdn| tai-fqdn }* { a-query | snaptr-query }
                                             * { decimal | hexadecimal }

default dns mcc-mnc-encoding
```

**default**

Resets the SGSN to send the MCC and MNC values in decimal format for DNS queries.

**apn-fqdn**

This keyword is used for PGW/GGSN selection during PDP activation.

**mmec-fqdn**

Selects the Peer MME during MME to SGSN ATTACH/RAU procedure and Suspend procedure.

**rai-fqdn**

Selects the SGW and peer SGSN during RAU/Attach procedure, Suspend procedure and RIM procedure.

**rnc-fqdn**

Selects the Peer SGSN during SRNS re-location.

**tai-fqdn**

Selects the Peer MME during SGSN to MME SRNS re-location and RIM procedure.
a-query
Controls the DNS A/AAAA query MCC/MNC encoding format.

snaptr-query
Controls the DNS SNAPTR query MCC/MNC encoding format.

decimal
Default
Instructs the SGSN to send the MCC and MNC in decimal format in the DNS query.

hexadecimal
Instructs the SGSN to send the MCC and MNC in hexadecimal format in the DNS query.

Usage Guidelines
In order to provide effective control on DNS queries for particular type of procedures, existing CLI commands in GPRS and SGSN services have been deprecated and replaced with new enhanced commands. The command `dns israu-mcc-mnc-encoding [hexadecimal | decimal]` has been deprecated and this new CLI command is introduced. New keyword options `snaptr-query` and `a-Query` are provided to control different types of queries.

Examples
Use the following command to configure hexadecimal encoding in the DNS query:

dns mcc-mnc-encoding rai-fqdn apn-fqdn mmec-fqdn rnc-fqdn tai-fqdn a-query hexadecimal
dns israu-mcc-mnc-encoding

Configures either decimal or hexadecimal format for the MCC and MNC values in the DNS query.

**Important**
This command is deprecated from release 16.0 onwards, it is replaced by the `dns mcc-mnc-encoding` command. See the `dns mcc-mnc-encoding` command for more information.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

```bash
configure > context context_name > gprs-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gprs-service)#
```

**Syntax Description**

`dns israu-mcc-mnc-encoding { decimal | hexadecimal }`

- `default`
  - `default`
    - Resets the SGSN to send the MCC and MNC values in decimal format for DNS queries.
  - `decimal`
    - Default.
    - Instructs the SGSN to send the MCC and MNC in decimal format in the DNS query.
  - `hexadecimal`
    - Instructs the SGSN to send the MCC and MNC in hexadecimal format in the DNS query.

**Usage Guidelines**

Use this command to determine the type of encoding for the MCC and MNC to be included in the DNS query. For example:

- In decimal, the MNC/MCC in a DNS query would appear like:
  `rac0017.lac42e3.mnc310.mcc722.gprs`
In hexadecimal, the MNC/MCC in a DNS query would appear like:
\texttt{rac0017.lac42e3.mnc0136.mcc02d2.gprs}

\textbf{Examples}

Use hexadecimal values for the MCC/MNC in the DNS query.
\texttt{dns israu-mcc-mnc-encoding hexadecimal}
end

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

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax Description

end

Usage Guidelines

Return to the Exec mode.
exit

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

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax Description
exit

Usage Guidelines
Return to the context configuration mode.
gmm

**gmm** actually provides a set of commands used to define the GPRS mobility management (GMM) parameters for the SGSN service.

---

**Important**
The **gmm** commands can be repeated as needed to set each timer.

---

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

```bash
configure > context context_name > gprs-service service_name
```

Entering the above command sequence results in the following prompt:

```bash
[context_name]host_name(config-gprs-service)#
```

**Syntax Description**
```
gmm [Extended-T3312-timeout { value exT3312_minutes | when-subscribed } | low-priority-ind-ue | { accept-procedure | new-tlli | old-tlli | attach ptmsi-signature-mismatch send-reject failure-code cause_code | ciph-gmm-msg-from-unknown-ms { detach | ignore } | mobile-reachable-timeout mins implicit-detach-timeout secs | negotiate-t3314-timeout secs | paging-failure-action downlink-data-lockout-timer seconds | repeat number_repeats | | purge-timeout mins | T3302-timeout mins | T3312-timeout mins | T3313-timeout secs | t3346 min minimum max maximum | T3350-timeout secs | T3360-timeout secs | T3370-timeout secs | trau-timeout }

default gmm { attach ptmsi-signature-mismatch | ciph-gmm-msg-from-unknown-ms | mobile-reachable-timeout | implicit-detach-timeout secs | negotiate-t3314-timeout | purge-timeout | T3302-timeout | T3312-timeout | T3313-timeout | T3350-timeout | T3360-timeout | T3370-timeout | trau-timeout }

no gmm { Extended-T3312-timeout | negotiate-t3314-timeout | t3346 }  

default
```

Disables the specified function or resets the specified timer to system defaults.

```bash
no
```

Removes the specified GMM definition from the configuration.
Extended-T3312-timeout

This keyword enables the operator to determine how the SGSN handles Extended T3312 timer values in a 2G GPRS network environment.

- **value**: This keyword instructs the SGSN to send the defined Extended T3312 timer value in Attach or RAU Accept messages to the MS if the subscriber has a subscription for the Extended T3312 timer (Subscribed Periodic RAU/TAU Timer in ISD) and indicates support for the extended periodic timer via the MS Network Feature Support.

- **exT3312_minutes**: Enter an integer from 0 to 18600 to identify the number of minutes for the timeout; default is 186 minutes.

- **when-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 when the MS has indicated support in MS Network Feature Support.

- **low-priority-ind-ue**: This keyword instructs the SGSN to include the extended T3312 timer value only if the Attach/RAU Request messages include a LAPI (low access priority indicator) in the "MS Device Properties".

- **no**: This filter, when used with the command, instructs the SGSN to remove the extended T3312 configuration from the GPRS Service configuration.

**accept-procedure | new-tlli | old-tlli**

Default: new-tlli

This keyword enables the use of either a new TLLI (temporary logical link identifier) or an old TLLI for attach-accept or RAU-accept messages sent by the SGSN to the MS during related procedures.

**attach ptmsi-signature-mismatch send-reject failure-code cause_code**

Default: disabled

This keyword enables the SGSN to validate the P-TMSI signature, present in the Attach Request, against the PTMSI-SIGNATURE stored at the SGSN. The SGSN then sends an Attach Reject to the MS if the PTMSI-SIGNATURE does not match.

The P-TMSI signature validation functionality only works if the feature is enabled. But even if it is enabled, the feature does not validate in the following situations:

- when the PTMSI-SIGNATURE is absent from the 2G Attach Request.
- if the first subscriber being in DETACHED state or is purged with FREEZE-PTMSI. In both the scenarios PTMSI-SIGNATURE cannot be validated.
- when the 2G subscriber(MS2) attaches with the same P-TMSI and a different P-TMSI_Signature as previously attached 2G subscriber (MS1), both the subscriber profiles are cleared from the system. This is relevant where the old RAI for MS-2 is the same as the current RAI for MS-1.

Optionally, a GMM failure *cause_code* can be configured to include in the Attach Reject if one is sent. Refer to the GMM failure cause codes listed below (information has been taken 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

ciph-gmm-msg-from-unknown-ms { detach | ignore }

Configures how the SGSN will behave when it receives a ciphered GMM message from an unknown MS.

**detach** - Instructs the SGSN to send a Detach message to the MS.

**ignore** - Instructs the SGSN to send an Ignore (drop) message to the MS.

Default: **ignore**
**implicit-detach-timeout secs**

Specifies the implicit detach timer (IDT) value for the 2G ISR implicit detach procedure on the network side (see ISR -- Idle Mode Signaling Reduction on the S4-SGSN feature chapter in the SGSN Administration Guide for additional timer usage details).

The IDT is configurable from release 15.0 onwards and it is only applicable to 2G ISR activated calls. If ISR is not activated on a 2G call then the subscriber is detached soon after expiry of the mobile reachability timer (MNR) timer.

`secs` must be an integer from 240 to 86400 and the default value is 3600.

**mobile-reachable-timeout mins**

Default: 58 minutes

Specifies the timeout value for the mobile reachability timer (MNR). This timer is used with the IDT timer described above.

`mins` must be an integer from 4 to 1440.

**negotiate-T3314-timeout secs**

Set the number of seconds for the T3314-timeout ready timer value. Value sent out from SGSN so MS can negotiate ready timer.

`secs` must be an integer from 0 to 11160. Default is 44 seconds.

- If the MS does not send the ready timer in the Attach/RAU request, then the SGSN sends this T3314-timeout (ready timer) value.
- If the MS sends the requested value of the ready timer in the Attach/RAU Request, and if the requested value is less than or equal to the value of the negotiate-T3314-timeout timer, then the SGSN sends Att/RAU Accept with the requested T3314 value.
- If the MS sends the requested value of the ready timer in the Attach/RAU Request, and if the requested value is greater than the value of the negotiate-T3314-timeout timer, then the SGSN sends Att/RAU Accept with the negotiate-T3314-timeout value.

**Important**

This is the only GMM timer that can be disabled by entering `no` at the beginning of the command syntax: `no gmm negotiate-t3314-timeout` By disabling negotiation of the T3314-timeout value, if the MS sends the requested value of the ready timer in the Att/RAU Request, then the SGSN sends the T3314-timeout value in the Att/RAU Accept.

**paging-failure-action downlink-data-lockout-timer seconds [ repeat number_repeats ]**

Default: 1000 seconds.

Enables and configures the downlink data lockout timer, for the SGSN services, to reduce the frequency of mobile-initiated keep alive messages.

`seconds` set the number of seconds before timer expire, range of 0 to 10000.

`repeat number_repeats` optionally sets the number of times (1 to 10) that the timer restarts after paging failure.

**Note:** If repeat is not configured then paging proceeds endlessly until the MR timer expires.

| default | no | gmm paging-failure-action | disabling the downlink data lockout timer.
purge-timeout  
Default: 10080 minutes

The purge timer defines the MM-context lifetime, part of the MM-context procedure on the network side. The configured value sets the duration (number of minutes) the SGSN holds the detached subscriber's MM-context profile. If the subscriber does not reattach to the SGSN during this time, then the SGSN purges this detached subscriber's MM-context information from its database and sends a MAP purge request towards the HLR to indicate that the subscribers profile is gracefully purged from SGSN's database.

mins must be an integer from 1 to 20160.

T3302-timeout  
Default: 12 minutes

Defines the number of minutes for timer to send to MS.

mins is an integer from 1 to 186.

T3312-timeout  
Default: 54 minutes

Periodic RAU update timer to send to MS.

mins is an integer from 0 to 186.

T3313-timeout  
Default: 5 seconds

Initial page timeout timer for retransmission for Paging Requests.

secs is an integer from 1 to 60.

T3314-timeout  
Default: 44 seconds

Ready Timer for controlling Cell Update Procedure.

secs must be an integer from 0 to 11519.

t3346

This keyword enables the mobility management (MM) T3346 back-off timer for the 2G service. When the SGSN is confronted by a situation involving congestion, the SGSN can assign the back-off timer value to the UEs and requests the UEs not to access the network for a given period of time.

**min minimum:** Enter an integer from 1 to 15 to identify the minimum number of minutes that the timer will run; default is 15 minutes.

**max maximum:** Enter an integer from 1 to 30 to identify the maximum number of minutes the timer can run; default is 30 minutes.

- If an Attach Request or RAU Request or Service Request is rejected due to congestion, then the T3346 value will be included in the reject message with GMM cause code 22 (congestion). The MM back-off timer value sent will be chosen randomly from within the configured T3346 timer value range.

- The timer will be ignored if a Request message is received after congestion has cleared.
• If MM T3346 timer value is configured in a Call-Control Profile then that value will override the back-off timer values defined for this GPRS Service configurations.

T3350-timeout secs
Default: 6 seconds
Retransmission timer for Attach Accept/RAU Accept/P-TMSI Realloc Command.
secs must be an integer from 1 to 20.

T3360-timeout secs
Default: 6 seconds
Retransmission timer for Authentication Request.
secs must be an integer from 1 to 20.

T3370-timeout secs
Default: 6 seconds
Retransmission timer for Identity Request.
secs must be an integer from 1 to 20.

trau-timeout secs
Default: 30
Specifies the number of seconds the "old" 3G SGSN waits to purge the MS's data. This timer is started by the "old" SGSN after completion of the inter-SGSN RAU.
secs : Must be an integer from 5 to 60.

Usage Guidelines
Use this command to set GMM timers.

Examples
Set the t3370 timer expiration for 15 seconds:
gmm t3370-timeout 15
**Ilc**

Configures the timers that control the data flow for the logical link control (LLC) sub-layer.

**Important**
This command may be repeated as often as necessary to define the needed timers.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

`configure > context context_name > gprs-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-gprs-service)#
```

**Syntax Description**

```
Ilc { iov-ui-in-xid-reset | n201u-max { sapi11 pkt-size | sapi3 pkt-size | sapi5 pkt-size | sapi9 pkt-size } | nu-overflow-detection high-watermark high_num low-watermark low_num increment-oc pdu-lifetime secs | random-value-in iov-ui | negotiation-failure-action { fallback-to-default iovui | reject } | reset-vur | t200 sapi1 time | t200 sapi11 time | sapi3 time | sapi5 time | sapi7 time | sapi9 time | uplink-pdu-len-validation }

default Ilc { iov-ui-in-xid-reset | n201u-max { sapi11 | sapi3 | sapi5 | sapi9 } | nu-overflow-detection | pdu-lifetime | random-value-in iov-ui | reset-vur | T200 | sapi1 | sapi11 | sapi3 | sapi5 | sapi7 | sapi9 | uplink-pdu-len-validation }

no Ilc { iov-ui-in-xid-reset | nu-overflow-detection | random-value-in iov-ui | reset-vur | uplink-pdu-len-validation }

default

Resets the configuration parameter to the default values.

no

Disables a defined configuration parameter and returns to the SGSN default.

`iov-ui-in-xid-reset`

This keyword makes it possible for the operator to configure whether or not to send IOV-UI in an XID-RESET. This is useful when the MS is not setup to accept IOV-UI (for example, MS sends Attach/RAU Requests with cksn=7) and including IOV-UI in the XID-Reset would result in Attach/RAU failure.
Default: Enabled

**n201u-max sapi n pkt_size**

This keyword sets the maximum number of octets, per service access point identifier (SAPI), for the downlink data packets. This is the upper limit that the SGSN will negotiate with the subscriber for packets sent from the SGSN to the BSC.

**sapi n**: Command must identify one of the following SAPI: sapi11, sapi3, sapi5, or sapi9.

**pkt_size**: Must be an integer from 140 to 1520. Default size is 1520 octets.

**nu-overflow-detection high-watermark high_num low-watermark low_num increment-oc**

Enables/disables overflow detection for the N(u) counter and setting overflow high/low thresholds facilitates ciphering synchronization between the MS and SGSN.

**high_num**: Enter an integer between 1 and 511.

**low_num**: Enter an integer between 0 and 510.

If the expected value of nu(Vur) is greater than or equal to the configured high-watermark, and the received nu(LFN) is less than or equal to the configured low-watermark, the SGSN increments the overflow counter (VurOC).

The recommended overflow settings are as follows: **llc nu-overflow-detection high-watermark 496 low-watermark 15 increment-oc**

While expecting a packet with 496 < nu < 511 and a packet with 0 < nu < 15 is received, overflow is detected and VurOC is incremented.

**pdu-lifetime secs**

Defines LLC layer PDU lifetime at the BSC.

**secs** must be an integer from 0 to 90.

Default: 6

**random-value-in iov-ui [ negotiation-failure-action { fallback-to-default-iovui | reject } ]**

Including this keyword enables the SGSN to negotiate the sending of a random value for the IOV-UI in the XID Request sent to the MS. If this keyword is not included, then by default the SGSN sends a zero (0) as the value of the IOV-UI in the XID message.

Including **default** in a command with the **negotiation-failure-action** keyword resets the SGSN configuration so that all calls are rejected whenever the deciphering fails due to failure of the XID negotiation for random IOV-UI.

If the **negotiation-failure-action fallback-to-default-iovui** option is included in the configuration, then the SGSN will fall back to unencrypted mode whenever the XID negotiation for random IOV-UI negotiation fails.

If the **negotiation-failure-action reject** option is included in the configuration to return the SGSN to the default functionality and reject all calls when random IOV-UI negotiation fails. This option is typically used only if the **negotiation-failure-action fallback-to-default-iovui** option has previously been part of the configuration.

The **reject** option conditionally causes the SGSN to reject calls, for example, when XID for random IOV-UI negotiation failure occurs during intra-RAU or standalone authentication for SMS, the SGSN moves the subscriber to STANDBY and marks the XID negotiation as a failure.
Despitethe reject configuration, the SGSN may respond to XID negotiation failure in one of the following manners according to associated circumstances:

- Initiates XID for new random IOV-UI negotiation:
  - with the MS is in STANDBY state, any uplink packet (in either ciphered or unciphered mode, except Attach / Intra-RAU) from the MS which results in CELL-UPDATE, READY TIMER START and RADIO STATUS READY causes an event indication to the application.

- Initiates Detach:
  - with the MS is in STANDBY state, any uplink activity causes the SGSN to initiate a new XID exchange, which if it fails or aborts due to the reception of SUSPEND, RADIO-STATUS and READY-TIMER expiry, results in the SGSN initiating Detach.
  - when PAGING is ongoing, any Page response from the MS results in the SGSN initiating Detach.
  - during OLD_SGSN ISRAU, when any uplink data comes before T3 tunnel timer expiry then the SGSN initiates Detach.

- Handles Messages:
  - Attach and intra-RAU (from both local and non-local TLLI or from both the same and different RA) will be processed in any state.

- Moves to STANDBY state:
  - MS is moved to STAND-BY state if the XID exchange failed due to any of the following cases suspend, radio status, BVC block, BVC reset, ready timer expiry, no response received for XID exchange during INTRA-RAU/Standalone Authentication for SMS.
  - XID is ongoing in READY state and if the MS moves to either 3G or to the peer-SGSN then the subscriber is moved to STANDBY state.

reset-vur
Enables/disables the mechanism to reset the Vur value maintained at LLC if the intra RAU request is received with N(U) = 0
Default: Disabled

**T200 sapi1 time**
Sets the retransmission timer (in seconds) for sapi1.

*time* must be an integer of 1 to 10.

Default: 5

**T200 sapi11 time**
Sets the retransmission timer (in seconds) for sapi11.

*time* must be an integer of 1 to 50.

Default: 40
T200 sapi3 time
Sets the retransmission timer (in seconds) for sapi3.
time must be an integer of 1 to 10.
Default: 5

T200 sapi5 time
Sets the retransmission timer (in seconds) for sapi5.
time must be an integer of 1 to 20.
Default: 10

T200 sapi7 time
Sets the retransmission timer (in seconds) for sapi7.
time must be an integer of 1 to 40.
Default: 20

T200 sapi9 time
Sets the retransmission timer (in seconds) for sapi9.
time must be an integer of 1 to 40.
Default: 20

uplink-pdu-len-validation
This feature enables validation of the size of the uplink LLC packets. With validation enabled, the SGSN will drop any uplinked packets that are larger than the negotiated limit.
If the no form of the command is used, then this feature is disabled. The SGSN will be more flexible with uplink packet sizes. So if the SGSN and MS have a mismatch and the MS sends packets that are larger than expected, then the SGSN will not drop the packets.
Default: Enabled.

Usage Guidelines
Use the command repeatedly to configure additional timers and features for the LLC sub-layer.

Examples
Set the T200 retransmission timer to timeout at 12 seconds for SAPI5:
llc t200 sapi5 12

Use the following command to instruct the SGSN to ignore the N201_U packet size limits for uplink packets from an MS:
no uplink-pdu-len-validation
network-sharing

Enables or disables CS-PS coordination checking for homers (UEs in their home network) or roamers (UEs from outside the home network). The command also sets the failure code that will be sent for GPRS MOCN.

**Product**  
SGSN

**Privilege**  
Administrator

**Command Modes**  
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

```
configure > context context_name > gprs-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name (config-gprs-service) #
```

**Syntax Description**

```
network-sharing { cs-ps-coordination { failure-code <gmm-cause> | homer | roamer } | failure-code <gmm-cause> }
no network-sharing cs-ps-coordination { homer | roamer }
default network-sharing cs-ps-coordination

no
```

Disables CS-PS coordination check for either homers or roamers.

```
default
```

Set the CS-PS coordination parameters to default values.

```
failure-code <gmm-cause>
```

This keyword has two optional functions:

- When used with the `cs-ps-coordination` keyword, it sets the GMM cause code that is to be included in the message when the SGSN requests the BSC to provide CS-PS coordination. Default value is 14.
- When used as an independent keyword with the `network-sharing` command, it sets the failure cause that is used by GPRS MOCN if no failure cause is available when the SGSN sends a Reject message. Default value is 7.

```
<gmm-cause>
```

is an integer from 2-111. Valid options include:

- 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

**homer**
Enables checking for CS-PS coordination for UEs from inside the home network (homers) only.

**roamers**
Enables checking for CS-PS coordination for UEs from another network (roamers) only.

**Usage Guidelines**
The operator can use this command to configure CS-PS coordination checking explicitly for homer or roamers subscribers and for the failure-code to be sent when the SGSN asks the BSC to perform CS-PS coordination.
Examples

Use a command similar to the following to have the SGSN perform CS-PS coordination checking only for all UEs from outside of the home network:

```
network-sharing cs-ps-coordination homer
```
nri

Configures the network resource identifier (NRI) to identify a specific SGSN. The NRI information is stored in the P-TMSI. The SGSN uses a portion of this NRI to set the parameters for Gb flex (SGSN pooling) functionality.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GPRS Service Configuration

configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-gprs-service)#
```

**Syntax Description**

```
nri length nri_length  { nri-value nri_value | null-nri-value null_nri_value non-broadcast-lac lac_id rac rac_id | nri-value value || non-pooled-nri-value value | }

default nri

no nri
```

default

A default configuration was made available beginning in Release 14.0.

Using this keyword now resets the nri configuration to nri length 6 and nri value 0.

---

**Important**

Behavior change in Release 14.0 -- it is no longer necessary to configure NRI as default values have been enabled.

---

**Important**

no nri command form is deprecated in Release 14.0. To ensure backward compatibility with configuration files created with pre-Release 14.0 builds, the no nri configuration will be automatically converted to the Release 14.0 default values of nri 6 and 0.

This command removes the configured NRI value and location information in the P-TMSI that would be retrieved by this SGSN.
**length nri_length**

Specifies the number of bits to be used in the P-TMSI, bits 23 to 18 are used to define the network resource identifier (NRI). The NRI length configuration also sets the maximum size of the pool. If not configured, the NRI length will be of zero length.

*nri_length* : Must be an integer from 1 to 6 to identify the number of bits.

**null-nri-value null_nri_value**

Configures the null NRI value which must be unique across the pool areas. This keyword is used for the offloading procedure for SGSN pooling (enabled with the *sgsn offloading* command, see the Exec Mode chapter).

*null_nri_value* is an integer from 0 (zero) to 63 used to identify the SGSN to be used for the offloading procedure for SGSN pooling. There is no default value for this parameter.

**non-broadcast lac lac_id rac rac_id**

Defines the non-broadcast LAC/RAC to be used in combination with the null-NRI for the offloading procedure.

*lac_id* defines a location area code associated with a BSS. Must be an integer between 1 and 65535.

*rac_id* defines the remote area code to be associated with a BSS. Must be an integer between 1 and 255.

**nri-value nri_value**

Specifies the MS-assigned value of the NRI to retrieve from the P-TMSI. This value must not exceed the maximum possible value specified by the NRI length. The NRI value must be unique across the pool or across all overlapping pools.

*nri_value* must be an integer from 1 to 63 to identify a specific SGSN in a pool. Use of 0 (zero) value is not recommended.

Multiple NRI values can be identified by providing multiple *nri-value* separated by a blank space for example:

```
nri length 6 nri-value 29 43 61
```

The NRIs configured using this keyword will be used only in pooled area if the keyword *non-pooled-nri-value* is configured, else the NRIs configured using the *nri-value* keyword will be used for both pooled and non-pooled areas.

**non-pooled-nri-value value**

If pooling is supported (the *null-nri-value* keyword is configured) use this keyword to configure values of NRIs to be used for non-pooled area. If the NRI CLI is configured as *nri length length_value nri-value values non-pooled-nri-value values* (null-nri-value is not configured, that is pooling not supported at SGSN) , NRIs will be used from "non-pooled-nri-value" irrespective of RNC/BSC being pooled or non-pooled.

---

**Note**

The same NRI can be configured using both the keywords *nri-value* and *non-pooled-nri-value*, this implies the NRI can be used either in pooled area or non-pooled area. If an NRI is configured for both pooled and non-pooled areas, then the SGSN re-uses the same NRI when moving from pooled to non-pooled areas and vice versa.
Usage Guidelines

Use this command to add or remove the Gb flex pool configuration for this GPRS service. The command can be repeated to specify different values for any of the keyword parameters. If more than one NRI is configured, the GPRS service will round-robin between the available NRIs when new subscribers (re)connect.

Use this command to retrieve the NRI (identity of an SGSN) stored in in bits 23 to 18 of the packet-temporary mobile subscriber identity (P-TMSI). If more than one NRI value is configured, the GPRS service will round-robin between the available NRIs when new subscribers (re)connect.

Examples

The following command specifies the NRI length as 5 bits, identifies SGSN 23 with LAC 222 and RAC 12 for offloading procedure with NRIs 6 and 41:

```
nri length 5 null-nri-value 34 non-broadcast lac 222 rac 12 nri-value 6 41
```
paging-policy

Configures the paging parameters for the GPRS service.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GPRS Service Configuration

configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gprs-service)#

Syntax Description

paging-policy { last-known-area { all | bsc | cell | location-area | routing-area } + | max-retransmissions retran_num }

no paging-policy last-known-area { bsc | cell | location-area | routing-area }

default paging-policy { last-known-area | max-retransmissions }

no

Disables the paging-policy definition for this GPRS service configuration.

default

 Resets the defaults for parameters managed by this paging policy.

last-known-area

Select one or more paging areas and enter them in preferred paging order:

• all : Pages in the last known BSC.
• bsc : Pages in last known BSC.
• cell : Pages in last known cell.
• location-area : Pages in last known location area.
• routing-area : Pages in last known routing area.

By default, paging occurs in the following order:
cell, BSC, routing area, location area.
max-retransmission \textit{retran\_num}

Configures the maximum number of retries for a page request per paging area.

\textit{retran\_num}: Enter an integer from 0 to 5.

- 2: default.
- 0: disables retransmission for paging request so that the SGSN only sends a single 2G PS-paging request to the BSC with no retransmissions.

+ Keywords can be repeated or combined as needed to complete the paging policy configuration.

**Usage Guidelines**

Use this command to configure the order of preference for retransmitting into specified paging-areas.

**Examples**

Use the following command to instruct the SGSN to page the cell and BSC as the last-known areas:

\texttt{paging-policy last-known-area cell bsc}
peer-nsei

This command associates a peer (remote) network service entity (NSEI) for a BSS with this GPRS service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

[context_name] host_name(config-gprs-service) #

**Syntax Description**

peer-nsei nse_id { associate dscp-template downlink template_name | lac lac_id rac rac_id | name peer_nsei_name | pooled }

no peer-nsei nse_id { associate dscp-template downlink | lac lac_id rac rac_id | name | pooled }

no

Removes the specified configuration from this peer-nsei configuration.

---

**Important**
Deleting the LAC/RAC portion of the configuration will probably result in the loss of subscriber connections.

**nse_id**
Defines a specific peer NSEI configuration for this GPRS service.

nse_id - enter an integer from 0 to 65535.

**associate dscp-template downlink template_name**

Identifies a specific DSCP marking template to associate with the peer-NSE. The DSCP template must first be created with SGSN Global configuration mode and then defined with the commands in the DSCP Template configuration mode. The template provides a mechanism for differentiated services code point (DSCP) marking of control packets and LLC signaling messages on Gb interfaces. This DSCP marking feature enables the SGSN to perform classifying and managing of network traffic and to determine quality of service (QoS) for the interfaces to an IP network.

template_name- enter an alphanumeric string of 1 to 64 characters.
lac *lac_id*
Defines a location area code associated with the NSE BSS.
*lac_id* must be an integer between 1 and 65535.

rac *rac_id*
Defines the remote area code to be associated with the NSE BSS
*rac_id* must be an integer between 1 and 255.

name *peer_nsei_name*
Enables identifying a BSC by a name which is stored in SCT.
*peer_nsei_name* - enter an alphanumeric string of 1 to 64 characters.

pooled
Enables pooling with non-pooled BSCs within the pool area.

Usage Guidelines
Use this command repeatedly to associate one or more LAC/RAC combinations and/or pooling with this peer-GPRS service configuration. Also repeat the command as needed to create an association with a DSCP marking template, to define a name for a BSC, and to enable pooling with non-pooled BSCs.

The Network Service Entity (NSE) at the BSS and the SGSN provides the network management functionality required for the operation of the Gb interface. Each NSE is identified by means of NSE identifier (NSEI).

Examples
The following command configures the NSE with identifier as 4114 having location area code 234 and routing area code as 22:
peer-nsei 4114 lac 234 rac 22

The following command enables Gb flex (pooling) functionality for NSEI 4414 for this GPRS service:
peer-nsei 4114 pooled
plmn

This command identifies the Public Land Mobile Network (PLMN) for the GPRS service. It also configures the common PLMN-Id and an optional list of dedicated PLMN-Ids in support of Multi-Operator Core Network (MOCN) operation.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

```
configure > context context_name > gprs-service service_name
```

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-gprs-service)#
```

**Syntax Description**

```
plmn id mcc mcc_num mnc mnc_num [ network-sharing common-plmn mcc mcc_num mnc mnc_num [ plmn-list mcc mnc_num mcc_num mnc_num [ mcc mcc_num mnc mnc_num | + | ] ]
no plmn id

no
```

Removes the PLMN information from the configuration for the current SGSN service.

```
mcc mcc_num
```

Defines the mobile country code (MCC) portion of the PLMN Id.

```
mnc_num
```

must be a 3-digit integer from 100 to 999. MCC values of 000-099 are Reserved codes.

```
mnc mnc_num
```

Defines the mobile network code (MNC) portion of the PLMN Id.

```
mnc_num
```

must be a 2- or 3-digit integer from 00 to 999. MNC value of 000 is reserved.

```
network-sharing common-plmn
```

Configures the common PLMN-Id broadcast by a radio network. An MS that does not support network sharing will only see this PLMN-Id. An MS that supports network sharing (MOCN) will see this PLMN-Id and the list of PLMN-Ids configured using the `plmn-id` keyword.
plmn-list

Configures a list of PLMN-Ids that an MS will see when network sharing is enabled.

+

The plus symbol indicates that more than one set of the keywords, for PLMN-Id, can be entered within a single command.

Usage Guidelines

Use this command to set PLMN parameters for the current SGSN service. This command also sets the common PLMN-Id and a list of PLMN-Ids employed in network sharing (MOCN) deployments. There is no limit to the number of PLMN-Ids that can be included in the list.

Examples

The following command identifies the PLMN MCC as 200 and the MNC as 10:
plmn id mcc 200 mnc 10
rai-skip-validation

Enable or disable if validation checks are done to verify the MCC and MNC fields received in the old RAI IE in Attach/RAU Requests.

Product
SGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > GPRS Service Configuration
configure > context context_name > gprs-service service_name
Entering the above command sequence results in the following prompt:
{context_name}@host_name(config-gprs-service)#

Syntax Description
[ no ] rai-skip-validation

no
Disables skipping the validation of the old RAI MCC/MNC fields and enables the default behavior to validate.

Usage Guidelines
This command configures the SGSN to enable or disable rejection of RAU requests with invalid MCC/MNC values in the old RAI field. By default, this configuration is disabled allowing the default behavior to validate the old RAI MCC/MNC fields.

This command also impacts the PTMSI attache where the old RAI field is invalid. If the OLD RAI field is invalid and if the validation is enabled, the identity of the MS is requested directly from the MS instead of the peer SGSN.

Validation checks are done per 3GPP TS 24.008 for the MCC/MNC fields of the old RAI IE in Attach/RAU Requests. RAU requests with invalid MCC/MNC values in the old RAI field are rejected. For Attach requests with invalid MCC/MNC values in the old RAI field, the identity of the MS is retrieved directly from the MS instead of sending an identity request to the peer Node where the MS identity is derived from the valid old-RAI.

Examples
Use this command to configure rejection of RAU requests with invalid MCC/MNC values in the old RAI field:

no rai-skip-validation
**reporting-action event-record**

This command enables the SGSN to log GMM/SM events in EDR files for 2G services.

**Product**
- SGSN

**Privilege**
- Security Administrator, Administrator

**Command Modes**

```
Exec > Global Configuration > Context Configuration > GPRS Service Configuration
configure > context context_name > gprs-service service_name
```

Entering the above command sequence results in the following prompt:

```
<context_name>@host_name>(config-gprs-service)#
```

**Syntax Description**

```
reporting-action event-record
[ default | no ] reporting-action event-record
```

- **default**
  - Disables the logging function.

- **no**
  - Removes the logging function from the configuration file.

**Usage Guidelines**

This command is one of the steps needed to enable the SGSN to create a log for events such as Attach, RAU, and Activations. The log is an EDR (event data record) in CSV format. For details about how this feature works, refer to the *GMM-SM Event Logging* chapter in the *SGSN Administration Guide*.

**Related Commands:**

- To enable GMM/SM event logging for 2G services, the `reporting-action event-record` command must be configured in the SGSN service configuration.

- To enable a log to be generated in an EDR file, the `edr-module active-charging-service` command must be enabled in the Context configuration mode.

- To configure parameters for the logging file characteristics and for file transfer, use the commands in the EDR Module Configuration Mode.
Examples

Enable GMM/SM event logging for 3G services:

`reporting-action event-record`
s4-overcharge-protection

Enables or disables Subscriber Overcharging Protection functionality for the S4-SGSN in the 2G network and associates a BSSGP (base station subsystem GPRS protocol) cause code group with the GPRS Service configuration.

Important

We recommend that you enable Release Access Bearer, with the release-access-bearer command in the Call-Control Profile Configuration mode, before this s4-overcharge-protection command is used to enable Subscriber Overcharging Protection.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GPRS Service Configuration

configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

{context_name} host_name (config-gprs-service) #

Syntax Description

s4-overcharge-protection bssgp-cause-code-group group_name

no s4-overcharge-protection

no

Disables Subscriber Overcharging Protection functionality for 2G. Disabled is the default.

bssgp-cause-code-group group_name

Associates a BSSGP cause code group with the GPRS Service configuration. You can enter a group's name before the cause code group is actually created but the names must match.

group_name: Enter an alphanumeric string up to 16 characters long to identify the cause code group.

Usage Guidelines

The cause code group is created with the cause-code-group command in the LTE Policy Configuration mode. To see the name of the defined cause code group(s) or the configuration of the BSSGP cause code groups, use the show lte-policy cause-code-group [ name | summary ] command in Exec mode.
To see the status of the Subscriber Overcharging Functionality and the associated BSSGP cause code group, use Exec command `show gprs-service name service_name`.

**Important**

If Release Access Bearer is enabled and going out of the S4-SGSN, the ARRL (abnormal release of radio link) bit will be included if this CLI is enabled and if LORC (loss of radio coverage) is detected.

### Examples

Enable Subscriber Overcharging Protection and associated cause code group `ccgp1` with a command similar to the following:

```
s4-overcharge-protection bssgp-cause-code-group ccgp1
```

Disable Subscriber Overcharging Protection and automatically disassociate the cause code group with the GPRS Service configuration by using a command similar to the following:

```
no s4-overcharge-protection
```
**setup-timeout**

Configures the maximum number of seconds allowed for session setup.

**Product**  
SGSN

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration > Context Configuration > GPRS Service Configuration  
*configure > context context_name > gprs-service service_name*

Entering the above command sequence results in the following prompt:

```
<context_name>host_name>(config-gprs-service)#
```

**Syntax Description**

- `setup-timeout seconds`
- `default setup-timeout`

**Syntax Description**

- `default`
  
  Returns the configuration to the default, 60 seconds.

- `seconds`
  
  An integer from 1 to 100000.

**Usage Guidelines**  
Use this command to set the time allowed for session setup.

**Examples**

The following command sets the maximum session setup time to 300 seconds:

```
setup-timeout 300
```
sgsn-context-request

Specifies whether or not the PTMSI signature check should be skipped if the PTMSI signature is not included in the SGSN context request.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GPRS Service Configuration
configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-gprs-service)#
```

**Syntax Description**

sgsn-context-request ptmsi-signature-absence allowed
default sgsn-context-request ptmsi-signature-absence
no sgsn-context-request ptmsi-signature-absence allowed

default

Returns the configuration to the default action to perform the PTMSI signature check.

no

Removes this definition from the system configuration.

**Usage Guidelines**

Use this command to skip the PTMSI signature check.

**Examples**

The following command instructs the system to perform the PTMSI signature check.

default sgsn-context-request ptmsi-signature-absence
sgsn-number

Define the SGSN E.164 number to be used when interacting via MAP protocol for this GPRS service.

Product
SGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > GPRS Service Configuration
configure > context context_name > gprs-service service_name

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

Syntax Description
sgsn-number sgsn_number
no sgsn-number

no
Disables the use of this definition in the system configuration.

sgsn-number
Enter a string of 1 to 16 digits to identify the SGSN's E.164 identification (Country Code+National Destination Code+Subscriber Number).

Usage Guidelines
Use this command to identify the ISDN number for the SGSN associated with this GPRS service.
The SGSN supports multiple SGSN numbers – different numbers in the 2G GPRS service configuration and the 3G SGSN service configuration. If an HLR-initiated dialog is received, the SGSN will perform a lookup based on the IMSI and find the correct SGSN number with which the MS is associated. Subsequent messaging will use this address.

Examples
Disable the E.164 number for this GPRS service.
no sgsn-number
**sm**

Configures the session management (SM) parameters associated with this particular GPRS service context.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

```plaintext
configure > context context_name > gprs-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gprs-service)#
```

**Syntax Description**

```plaintext
sm { activate-max-retransmissions num_retries | deactivate-max-retransmissions num_retries | guard-timer guard_seconds | ignore-pco-decode-error | modify-max-retransmissions num_retries | partial-apn-match | radio-priority from-arp arp-rp_prof_name | requested-apn-from-first-subrec | t3385-timeout secs | t3386-timeout secs | t3395-timeout secs | t3396 min minimum max maximum cause cause_code | trim-trailing-spaces-in-apn }

default sm { activate-max-retransmissions | deactivate-max-retransmissions | ignore-pco-decode-error | modify-max-retransmissions | t3385-timeout | t3386-timeout | t3395-timeout | trim-trailing-spaces-in-apn }

no sm { ignore-pco-decode-error | radio-priority from-arp | partial-apn-match | radio-priority | requested-apn-from-first-subrec | t3396 | trim-trailing-spaces-in-apn }

default

Resets the SM parameters to their defaults.

no

Removes the identified parameter configuration from the GPRS Service configuration.

**activate-max-retransmissions num_retries**

Defines the maximum number of retries to transmit 'activate PDP context request'.

* num_retries : Must be an integer from 1 to 10.

Default: 4

**deactivate-max-retransmissions num_retries**

Defines the maximum number of retries to transmit 'deactivate PDP context request'.
**num_retries**: Must be an integer from 1 to 10.

Default: 4

**guard-timer guard_seconds**

Sets the number of seconds before the session manager resources are cleared.

*guard_seconds* is an integer from 30 to 150.

Default: 80 seconds

**ignore-pco-decode-error**

Enables the SGSN to ignore received decode errors that are due to incorrectly encoded PCO IE length in SM Requests.

Default: disabled

**modify-max-retransmissions num_retries**

Defines the maximum number of retries to transmit 'modify PDP context request'.

*num_retries*: integer from 1 to 10.

Default: 4

**partial-apn-match**

Enables partial matching of requested APN during APN selection.

Partial APN or APN with trailing spaces may be present in an Activate Request because incorrect information was keyed in by the user. Though it is valid to reject such Activation Requests, it increases the signaling between the MS and the SGSN. This has an impact on the radio resources.

**radio-priority from-arp**

Associates an ARP-RP Mapping Profile with the GPRS service. The profile is created and configured via the ARP-RP Mapping Profile configuration mode under the SGSN-Global configuration mode.

*arp-rp_prof_name* - Enter a string of 1 to 64 alphanumeric characters to identify the mapping profile and moves into the ARP-RP mapping profile configuration mode.

Use the **show configuration** command to display the association.

**requested-apn-from-first-subrec**

Enables use of a 'requested APN' from the first subscription record. When this feature is enabled, the PDP Activation is not rejected during APN Selection; instead, the APN from the first subscription record is used as the requested APN and the SGSN continues with the rest of the APN Selection process.

A requested APN is an optional IE in an Activate PDP Request. To get the requested PDP type, if multiple PDP subscription records exist for the subscriber, then the MS has to include the APN information to choose the PDP subscription record during APN selection. Otherwise, such activations will be rejected during APN selection (per TS 23.060 Appendix A). Though it is valid to reject such activation requests, it increases the signaling between the MS and the SGSN, which impacts the radio resources.
t3385-timeout secs
Defines the maximum amount of time for retransmission of 'activate request' messages.
secs : Must be an integer from 1 to 60.
Default: 8

t3386-timeout secs
Defines the maximum amount of time for retransmission of 'modify request' messages.
secs : Must be an integer from 1 to 60.
Default: 8 seconds.

t3395-timeout secs
Defines the maximum amount of time for retransmission of 'deactivate request' messages.
secs : Must be an integer from 1 to 60.
Default: 8

t3396
Enables the session management (SM) T3396 back-off timer for the 2G service. When the SGSN is confronted by a situation involving congestion, the SGSN can assign the back-off timer value to the UEs and request the UEs not to access the network for a given period of time.

min minimum: Enter an integer from 1 to 15 to identify the minimum number of minutes that the timer will run; default is 15 minutes.

max maximum: Enter an integer from 1 to 30 to identify the maximum number of minutes the timer can run; default is 30 minutes.

cause cause_code: Enter an integer from 1 to 255 to identify the appropriate rejection cause code. The default is 26. During congestion, the configured value is ignored and 26 is sent.
  • During congestion, the SGSN randomly chooses a T3396 value from the configured range and sends that timer value to the UE in the Reject message with the cause code #26.
  • The command can be repeated to define a maximum of 16 cause codes.

trim-trailing-spaces-in-apn
Enables SGSN to strip off any trailing space(s) in requested APN.

If a requested APN in an Activate PDP Context Request has any trailing spaces, then those trailing spaces will be removed and the length field will be updated.

Usage Guidelines
Repeat this command with different keywords (parameters) to configure the SM (session management) as needed for this GPRS service. Keywords can be used to optimize signaling between the MS and the SGSN to reduce the impact on the radio resources.

Examples
Reset the number of retransmission messages for deactivate PDP context request to 5.
sm deactivate-max-retransmissions 5
**sndcp**

Defines the sub-network dependent convergence protocol (SNDCP) network packet data unit (N-PDU) reassembly timeout interval associated with this GPRS service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

`configure > context context_name > gprs-service service_name`

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-gprs-service)#
```

**Syntax Description**

- `sndcp reassembly-timeout seconds`
- `default sndcp reassembly-timeout`

- `default`
  Reset the timer configuration to the default value of 30 seconds.

- `seconds`
  Defines the number of seconds the SGSN waits for all the SNDCP segments to arrive before dropping all the disassembled segments.

  - `seconds`: Must be an integer from 1 to 300.

**Usage Guidelines**

Use this command to modify the SNDCP reassembly timer. This timer starts as soon as the first N-PDU segment is received (either in-order or out-of-order). If all the segments belong to the N-PDU arrive before the timer expires then the segments are reassembled. If all the segments do not arrive before the timer expires, then the stored segments are discarded.

**Examples**

Reset the default for the timer.

```
default sndcp reassembly-timeout
```
**GRE Tunnel Interface Configuration Mode Commands**

The Generic Routing Encapsulation (GRE) Tunnel Interface Configuration Mode is used to create and manage the GRE tunneling interfaces for addresses, address resolution options, etc.

**Command Modes**

Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > GRE Tunnel Interface Configuration

configure > context context_name > interface interface_name tunnel > tunnel-mode gre

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-tunnel-mode)#
```

**Important**

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

- destination, page 1048
- end, page 1049
- exit, page 1050
- keepalive, page 1051
- source, page 1053
- tos, page 1055
- ttl, page 1057
destination

This command configures the destination IP address of the tunnel by specifying the destination end address. This is a mandatory configuration for a GRE tunnel interface.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > GRE Tunnel Interface Configuration

c\>configure \>context context_name \>interface interface_name tunnel > tunnel-mode gre

Entering the above command sequence results in the following prompt:

{context_name}\host_name\(config-if-tunnel-mode)#

Syntax Description

[ no ] destination address ip_address

no

Removes or disassociates the configured destination IP address from a specific GRE tunnel interface configuration.

address ip_address

Configures the IP address for the interface.

ip_address must be specified using the IPv4 dotted-decimal notation.

Usage Guidelines

Use this command to configure the destination IP address of the tunnel by specifying the IP address of destination tunnel end for GRE tunnel interface.

Important

State of source address will affect the operational state of the tunnel.

Examples

The following command sets the 10.2.3.4 as destination IP address of the GRE tunnel interface:

destination address 10.2.3.4
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.
keepalive

This command configures various parameters for sending Keepalive messages to the remote end-point in GRE tunnel interface configuration. By default sending keepalives is disabled.

Product
All

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > GRE Tunnel Interface Configuration

configure > context context_name > interface interface_name tunnel > tunnel-mode gre

Entering the above command sequence results in the following prompt:

[(context_name)host_name](config-if-tunnel-mode)#

Syntax Description
keepalive [ interval time_interval num-retry retry ]
| default | no | keepalive

default
Sets the sending of Keepalives with default parameters.
interval: 10 seconds
num-retry: 3 retries

no
Disables the keepalive and turns off the sending of Keepalives messages.

interval time_interval
Default: 10
Specifies the time interval (in seconds) between two Keepalives sent to remote ends of GRE tunnel interface configuration.
time_interval must be an integer from 5 through 3600.

num-retry retry
Default: 3
Specifies number of retransmission of keepalives to remote node without getting any response before the remote node is marked as dead/down.

retry must be an integer between 0 through 10.

Usage Guidelines

Use this command to configure the parameters for sending Keepalives to the remote end-point of GRE tunnel. It also configures the interval at which GRE Keepalives are sent on the interface and number of retries without getting a response from the remote end-point before the tunnel is shutdown. By default, Keepalives will not be sent.

Examples

The following command enables the keepalive and sets the other parameters to defaults:

default keepalive
source

This command configures the source IP address of the tunnel either by specifying the IP address (host address) or by specifying another configured non-tunnel IP interface. This is a mandatory configuration for GRE tunnel interface.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > GRE Tunnel Interface Configuration

configure > context context_name > interface interface_name tunnel > tunnel-mode gre

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-if-tunnel-mode)#

Syntax Description

{ no | source { address ip_address | interface interface_name } }

no

Removes/disassociates the configured source IP address or host interface from a specific GRE tunnel interface configuration.

address ip_address

Configures the IP address for the interface specifying the IP address. ip_address must be specified using IPv4 dotted-decimal notation.

interface interface_name

Specifies the name of the preconfigured non-tunnel IP interface, whose address is used as the source address of the GRE tunnel.

Usage Guidelines

Use this command to configure the source IP address of the tunnel either by specifying the IP address (host address) or by specifying another configured non-tunnel IP interface for GRE tunnel interface.

Important

State of source address will affect the operational state of the tunnel.
Examples

The following command sets the 10.2.3.4 as source IP address of the GRE tunnel interface:

source address 10.2.3.4
tos

This command configures the parameters/action for the type of Service (ToS) parameter in the IP tunnel transport protocol header.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > GRE Tunnel Interface Configuration

```
configure > context context_name > interface interface_name tunnel > tunnel-mode gre
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-if-tunnel-mode)#
```

Syntax Description

```
tos { value | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef | lower-bits
tos_value } | copy }
| default | no | tos
```

default

Sets the IP TOS to lower bits value of 0.

value | tos_value |

Default: af11

Specifies the IP QoS DSCP per-hop behavior to be marked on the outer header of signalling packets originating from the Access Gateway. This is a standards-based feature (RFC 2597). The following forwarding types are supported:

- af11: Assured Forwarding 11 per-hop behavior
- af12: Assured Forwarding 12 per-hop behavior
- af13: Assured Forwarding 13 per-hop behavior
- af21: Assured Forwarding 21 per-hop behavior
- af22: Assured Forwarding 22 per-hop behavior
- af23: Assured Forwarding 23 per-hop behavior
- af31: Assured Forwarding 31 per-hop behavior
• af32: Assured Forwarding 32 per-hop behavior
• af33: Assured Forwarding 33 per-hop behavior
• af41: Assured Forwarding 41 per-hop behavior
• af42: Assured Forwarding 42 per-hop behavior
• af43: Assured Forwarding 43 per-hop behavior
• be: Best Effort forwarding per-hop behavior
• ef: Expedited Forwarding per-hop behavior typically dedicated to low-loss, low-latency traffic.

The assured forwarding behavior groups are listed in the table below.

<table>
<thead>
<tr>
<th></th>
<th>Class 1</th>
<th>Class 2</th>
<th>Class 3</th>
<th>Class 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low Drop</td>
<td>AF11</td>
<td>AF21</td>
<td>AF31</td>
<td>AF41</td>
</tr>
<tr>
<td>Medium Drop</td>
<td>AF12</td>
<td>AF22</td>
<td>AF32</td>
<td>AF42</td>
</tr>
<tr>
<td>High Drop</td>
<td>AF13</td>
<td>AF23</td>
<td>AF33</td>
<td>AF43</td>
</tr>
</tbody>
</table>

Traffic marked with a higher class is given priority during congestion periods. If congestion occurs to traffic with the same class, the packets with the higher AF value are dropped first.

**lower-bits tos_value**

Default: 0

Sets the least-significant 6 bits in the ToS byte with the specified numeric value.

tos_value must be an integer from 0 through 255.

**copy**

This keyword instructs the system to copy the ToS value from the passenger IPv4 packet or Traffic class value from the passenger IPv6 packet to the ToS value of the IPv4 tunnel transport protocol header.

**Usage Guidelines**

Use this command either to set the ToS parameter in the IPv4 tunnel transport protocol header to the specified value or instructs to copy the ToS value from the passenger IPv4 packet or Traffic class value from the passenger IPv6 packet to the ToS value of the IPv4 tunnel transport protocol header. If one of the enumerated values is set, the DSCP bits which are the six most-significant bits in the ToS byte are marked. If the integer value is set, it will be written into the six least-significant bits of the ToS byte.

**Examples**

The following command instructs the system to copy the ToS value from the passenger IPv4 packet or Traffic class value from the passenger IPv6 packet to the ToS value of the IPv4 tunnel transport protocol header:

tos copy
ttl

This command configures the Time to live (TTL) parameter to be used in the tunnel transport protocol header for the current GRE tunnel interface.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > GRE Tunnel Interface Configuration

```
configure > context context_name > interface interface_name tunnel > tunnel-mode gre
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-tunnel-mode)#
```

**Syntax Description**

```
ttl ttl_value
default ttl
```

**default**

Sets the TTL value to system default value.

**ttl_value**

Default: 15

Specifies the maximum time to live to be used in the tunnel transport protocol header

The time to live (TTL) is not a measure of time but the number of hops through the network.

*ttl_value* must be an integer between 1 through 255.

**Usage Guidelines**

Use this command to set the TTL parameter to be used in the tunnel transport protocol header for the GRE tunnel configuration.

**Examples**

The following configures the TTL to a value of 10:

```
ttl 10
```
GRE Tunnel Interface Configuration Mode Commands

ttl
Gs Service Configuration Mode Commands

The Gs Service configuration mode configures the parameters used to setup and maintain a Gs interface for a connection between the SGSN and an MSC/VLR.

**Command Modes**

Exec > Global Configuration > Context Configuration > Gs Service Configuration

configure > context *context_name* > gs-service *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name] host_name (config-gs-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 1060
- bssap+, page 1062
- end, page 1064
- exit, page 1065
- max-retransmission, page 1066
- non-pool-area, page 1068
- pool-area, page 1070
- sgsn-number, page 1072
- timeout, page 1073
- vlr, page 1075
associate-sccp-network

This command associates a previously defined Signaling Connection Control Part (SCCP) network instance with the Gs service. This association is required to access Visitor Location Register(s) (VLRs).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > Gs Service Configuration

`configure > context context_name > gs-service service_name`

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-gs-service)#
```

**Syntax Description**

- `associate-sccp-network sccp_net_id`
- `no associate-sccp-network`

**Usage Guidelines**
Use this command to associate the SCCP network configuration instance with the Gs interface in this service.

**Important**
A single SCCP network configuration instance can not be shared with multiple Gs services.

**Important**
To enable a Gs service, the user needs to configure `ssn` with the `bssap+` command.
Examples

Following command associates SCCP network 2 with this Gs service.

`associate-sccp-network 2`
bssap+

This command defines the Base Station System Application Part Plus configuration parameters for the Gs service to enable the SGSN to access a Visitor Location Register(s) (VLRs).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > Gs Service Configuration

configure > context context_name > gs-service service_name

Entering the above command sequence results in the following prompt:

```
{context_name} host_name (config-gs-service)#
```

**Syntax Description**

```
bssap+ ssn ss_num

no bssap+ ssn ss_num

no
```

- **no**
  - Removes the configured BSSAP+ subsystem number from this Gs service.

- **ssn ss_num**
  - Specifies the subsystem number to configure in this Gs interface to use BSSAP+.
    - `ss_num` must be an integer from 1 through 255.

**Usage Guidelines**

- Use this command to configure the BSSAP+ subsystem with Gs interface in this service to communicate with VLR(s).

---

**Important**

- A single SCCP network configuration instance can not be shared with multiple Gs services.

---

**Important**

- To start a Gs service, the user needs to configure the command parameter.
Examples

Following command configures subsystem 101 with BSSAP+ in this Gs service.

`bssap+ ssn 101`
end

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

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax Description
end

Usage Guidelines
Return to the Exec mode.
exit

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

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax Description**
exit

**Usage Guidelines**
Return to the previous configuration mode.
max-retransmission

This command configures the retransmission values for different procedure counters in Gs service as described in TS 29.018.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Gs Service Configuration

configure > context context_name > gs-service service_name

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-gs-service)#
```

**Syntax Description**

```
max-retransmissions { n8 | n9 | n10 | n12 } retrans_num
default max-retransmissions { n8 | n9 | n10 | n12 }

no
```

no

Removes the configured Gs procedures from this Gs service.

```
{ n8 | n9 | n10 | n12 }
```

Specifies the various Gs service procedures that are available to be used to communicate with VLR(s).

- **n8**: Defines the maximum number of retries for explicit IMSI detach from a non-GPRS service. Default is 2.
- **n9**: Defines the maximum number of retries for explicit IMSI detach from a non-GPRS service. Default is 2.
- **n10**: Defines the maximum number of retries for implicit IMSI detach from the GPRS service. Default is 2.
- **n12**: Defines the maximum number of retries for BSSAP+ to send Reset Indication messages. Default is 2.

**retrans_num**

Default: 2

Specifies the number of re-transmission of message for specified procedures.
retrans_num: Must be an integer from 0 through 10.

**Usage Guidelines**
Use this command to configure the retransmission values for specific procedure counters in Gs service. counters are based on TS 29.018.
This command can be entered for each procedure counter separately.

**Examples**
Following command configure retransmission value as 3 for counter for procedure to send BSSAP+ Reset Indication messages in this Gs service.

```
max-retransmissions n12 3
```
non-pool-area

This command creates a non-pool area for a set of subscriber location area code (LAC) values that can be used with a specific VLR for the Gs service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > Gs Service Configuration

configure > context context_name > gs-service service_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-gs-service)#

**Syntax Description**

non-pool-area non_pool_name { use-vlr vlr_name lac lac_num } +

no non-pool-area non_pool_name | lac lac_num

**no**
Removes the configured non-pool area from this Gs service.

**non_pool_name**
Specifies the name of the non-pool area to configure with this command.

*non_pool_name* must be an alpha and/or numeric string of 1 to 63 characters.

**use-vlr vlr_name**
Specifies the name of the VLR to be associated with this non-pool area.

*vlr_name* is the name of VLR and must be an alpha and/or numeric string of 1 to 63 characters.

**lac lac_num**
Specifies the subscribers’ location area code to be attached with this non-pool area and specific VLR. This LAC of subscriber is obtained from the radio area indicator (RAI).

Including this keyword with the **no** form of the command enables the operator to remove a specific LAC from the non-pool area configuration.

*lac_num* is the LAC value and must be an integer value from 1 through 65535.
More than one `lac_num`, separated by a space, can be entered within a single command.

**Usage Guidelines**

This command can be repeated as necessary to define a total of 32 configured LACs for the combined **non-pool-area** and **pool-area** configurations per Gs service.

**Examples**

Following command configure a non-pool area `starpool1` to use VLR named `starvlr1` for LAC 101 in a Gs service.

```
non-pool-area starpool1 use-vlr starvlr1 lac 101
```
pool-area

This command creates a pool area configuration instance. This command also enters the Pool Area configuration mode to define the set of VLRs to use for a pool area for a set of subscriber location area code (LAC) values in the Gs service.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Gs Service Configuration

configure > context context_name > gs-service service_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-gs-service)#

Syntax Description

pool-area pool_name [-noconfirm]

no pool-area non_pool_name

no

Removes the configured pool area from this Gs service.

pool_name

Specifies the name of the pool area to configure with this command for VLR pooling and association of a LAC.

pool_name: Must be an alpha and/or numeric string of 1 to 63 characters.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to create/enter the pool area configuration mode. This mode is used configure the set of VLRs to be used for a set of subscriber LAC.

This command can be used multiple times, subject to a limit of 128 LAC values (the total number of non-pool-area and pool-area configurations) per Gs service.
**Examples**

The following command configures a pool area named `starpool1` in a Gs service without any confirmation prompt.

`pool-area starpool1 -noconfirm`
sgsn-number

Define the SGSN's E164 number to associate an SGSN with this Gs Service.

Product: SGSN

Privilege: Security Administrator, Administrator

Command Modes: Exec > Global Configuration > Context Configuration > Gs Service Configuration

configure > context context_name > gs-service service_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-gs-service)#

Syntax Description: sgsn-number E.164_number

E.164_number

Defines the SGSN's 'telephone' number, the ISDN number for per ITU-T E.164 numbering plan. The number must be a numerical string of 1 to 15 digits.

Usage Guidelines: For releases 8.1 or higher, use this command to define the SGSN's E.164 ISDN number. This value should match the sgsn-number defined for SGSN Service or GPRS Service.

Important: Note: the Gs Service will not start unless the SGSN's E.164 number is configured.

Examples: sgsn-number 12345678901234
timeout

This command configures various timers defining the wait before retransmitting a specific message for Gs service procedures.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > Gs Service Configuration

```plaintext
configure > context context_name > gs-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gs-service)#
```

**Syntax Description**

```
timeout { t6-1-timer t6_1_dur | t8-timer t8_dur | t9-timer t9_dur | t10-timer t10_dur | t12-1-timer minute t12_1_dur | t12-2-timer t12_2_dur }
| default | timeout { t6-1-timer | t8-timer | t9-timer | t10-timer | t12-1-timer | t12-2-timer }
```

**default**

Sets the timer value to wait in seconds/minutes to default values. Default values for timers are:

- **t6-1-timer**: 10 seconds
- **t8-timer**: 4 seconds
- **t9-timer**: 4 seconds
- **t10-timer**: 4
- **t12-1-timer**: 54 mins (+8 seconds)
- **t12-2-timer**: 4 seconds

**t6-1-timer t6_1_dur**

Default: 10

Specifies the retransmission timer value to guard the location update.

*t6_1_dur* is the waiting duration in seconds before retransmitting the specific message and must be an integer from 10 through 90.
t8-timer \textit{t8\_dur}

Default: 4

Specifies the retransmission timer value to guard the explicit IMSI detach from the GPRS service procedure. \textit{t8\_dur} is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 30.

\textbf{t9-timer \textit{t9\_dur}}

Default: 4

Specifies the retransmission timer value to guard the explicit IMSI detach from the non-GPRS service procedure. \textit{t9\_dur} is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 30.

\textbf{t10-timer \textit{t10\_dur}}

Default: 4

Specifies the retransmission timer value to guard the implicit IMSI detach from the GPRS service procedure. \textit{t10\_dur} is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 30.

\textbf{t12-1-timer minute \textit{t12\_1\_dur}}

Default: 54 minutes (plus 8 seconds for transmission delay)

Specifies the retransmission timer value to control the resetting of SGSN-Reset variable procedure. \textit{t12\_1\_dur} is the waiting duration in minutes before retransmitting reset message for the SGSN Reset variable and must be an integer from 0 through 384.

\textbf{t12-2-timer \textit{t12\_2\_dur}}

Default: 4

Specifies the retransmission timer value to guard the SGSN reset procedure. \textit{t12\_2\_dur} is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 120.

\textbf{Usage Guidelines}

Use this command to configure the time, for different procedure timers, to wait before retransmitting a procedure message.

This command can be repeated for each timer to configure multiple timers.

\textbf{Examples}

Following command sets the timeout duration of 4 seconds for t8 timer to wait before retransmitting the procedure message to explicitly do the IMSI detach from GPRS service:

\texttt{default timeout t8-timer}
This command defines a VLR configuration for use with this Gs service.

Product
SGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > Gs Service Configuration
configure > context context_name > gs-service service_name

Entering the above command sequence results in the following prompt:

\[(context_name)host_name\](config-gs-service)#

Syntax Description
vlr vlr_name isdn-number E164_num [point-code pt_code]
| bssap+ ssn ssn [point-code pt_code]
no vlr vlr_name

no
Removes the configured VLR from the Gs service.

vlr_name
Specifies the name of the VLR to configure in this Gs mode with ISDN number.
vlr_name must be an alpha and/or numeric string of 1 to 63 characters.

isdn-number E164_num
Specifies the VLR number to configure with this command.
E164_num: The ISDN number for the target VLR. Value must be defined according to the E.164 numbering plan and must be a numeric string of 1 to 15 digits.

bssap+ ssn ssn
Specifies the subsystem number to configure with this VLR to use BSSAP+.
ssn: Must be an integer from 1 through 255. Default value is 252.

point-code pt_code
Specifies SS7 address of VLR in point code value to this configured VLR name.
**pt_code:** Must be in SS7 point code dotted-decimal ###.###.### format or decimal ####### format.

**Usage Guidelines**
Use this command to define VLR configuration instances to be associated with the Gs service.
A maximum of 32 VLRs can be configured per Gs service.

**Examples**
Following command configures the VLR named *starvlr1* with an ISDN number 12344567, a subsystem number of 252, and a point code value of 123.345.567:

```plaintext
vlr starvlr1 isdn-number 12344567 point-code 123.345.567
```
GT-Format1 Configuration Mode Commands

The GT-Format1 configuration mode is a sub-mode for either the Global Title Translation Association configuration mode or the Global Title Translation Address-Map configuration mode. This sub-mode configures a set of rules used in the global title translation (GTT) process.

Command Modes

Exec > Global Configuration > GTT Association Configuration > GT-Format1 Configuration

configure > global title translation association instance instance_number > gt-format format_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-gtt-instance-format1)#

Important

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

- end, page 1078
- exit, page 1079
- nature-of-address, page 1080
- odd-even-indicator, page 1081
end

Exits the configuration mode and returns to the Exec mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax Description
end

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

Exits the configuration mode and returns to the Global configuration mode.

Product  SGSN

Privilege  Security Administrator, Administrator

Syntax Description  exit

Usage Guidelines  Return to the Global configuration mode.
nature-of-address

Configures the indicator to identify the nature of the address.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > GTT Association Configuration > GT-Format1 Configuration
configure > global title translation association instance instance_number > gt-format format_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-gtt-instance-format1)#

Syntax Description

nature-of-address { international | national | subscriber }

international
Identifies the numbers as international.

national
Identifies the numbers as matching the national configuration.

subscriber
Identifies the numbers as subscriber numbers.

Usage Guidelines

Configure the identify of the GT format as national.

Examples

nature-or-address national
**odd-even-indicator**

Configures the bits for matching the global title translation.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > GTT Association Configuration > GT-Format1 Configuration

```
configure > global title translation association instance instance_number > gt-format format_number
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-gtt-instance-format1)#
```

**Syntax Description**

```
odd-even-indicator type
```

*type*

- **odd**: Sets the odd bit for matching the GTT.
- **even**: Sets the even bit for matching the GTT.
GT-Format2 Configuration Mode Commands

The GT-Format2 configuration mode is a sub-mode for either the Global Title Translation Association configuration mode or the Global Title Translation Address-Map configuration mode. This sub-mode configures a set of rules used in the global title translation (GTT) process.

**Command Modes**

Exec > Global Configuration > GTT Association Configuration > GT-Format2 Configuration

```
configure > global title translation association instance instance_number > gt-format format_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-gtt-instance-format2)#
```

**Important**

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

- end, page 1084
- exit, page 1085
- translation-type, page 1086
end

Exits the configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax Description

der

Usage Guidelines

Change the mode back to the Exec mode.
exit

Exits the configuration mode and returns to the Global configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax Description**
exit

**Usage Guidelines**
Return to the Global configuration mode.
**translation-type**

Configures the translation type to be applied during the translation process.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > GTT Association Configuration > GT-Format2 Configuration

configure > global title translation association instance instance_number > gt-format format_number

Entering the above command sequence results in the following prompt:

[local] *host_name*(config-gtt-instance-format2)#

**Syntax Description**

`translation-type number`

- `number`
  - Must be an integer between 0 and 255.
  - Default is 0

**Usage Guidelines**

Use this command to configure the GTT translation type to be applied during global title translation process.

**Examples**

`translation-type 232`
GT-Format3 Configuration Mode Commands

The GT-Format3 configuration mode is a sub-mode for either the Global Title Translation Association configuration mode or the Global Title Translation Address-Map configuration mode. This sub-mode configures a set of rules used in the global title translation (GTT) process.

**Command Modes**

Exec > Global Configuration > GTT Association Configuration > GT-Format3 Configuration

```markdown
configure > global title translation association instance instance_number > gt-format format_number
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-gtt-instance-format3)#
```

---

**Important**

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

- encoding-scheme, page 1088
- end, page 1089
- exit, page 1090
- numbering-plan, page 1091
- translation-type, page 1092
encoding-scheme

Configures the encoding-scheme to use during global title translation (GTT).

Product
SGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > GTT Association Configuration > GT-Format3 Configuration
configure > global title translation association instance instance_number > gt-format format_number

Entering the above command sequence results in the following prompt:
[local]host_name(config-gtt-instance-format3)#

Syntax Description
encoding scheme scheme_type

scheme_type
Select one of the following encoding scheme types to determine the encoding type to be used during GTT:

- **bcd-even**: BCD even encoding scheme
- **bcd-odd**: BCD odd encoding scheme
- **nw-specific**: Network specific encoding scheme
- **unknown**: Unknown encoding scheme

Usage Guidelines
Select BCD even encoding for GTT

Examples
encoding scheme bcd-even
**end**

Exits the configuration mode and returns to the Exec mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax Description**
end

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

Exits the configuration mode and returns to the Global configuration mode.

Product  SGSN

Privilege  Security Administrator, Administrator

Syntax Description  exit

Usage Guidelines  Return to the Global configuration mode.
numbering-plan

Configures the GTT process to apply one of the numbering-plans during the GT translation process.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

 Exec > Global Configuration > GTT Association Configuration > GT-Format3 Configuration
 configure > global title translation association instance instance_number > gt-format format_number

Entering the above command sequence results in the following prompt:

[local] host_name (config-gtt-instance-format3)#

Syntax Description

numbering-plan plan_type

plan_type

Select one of the following numbering plans be employed during GTT:

- data: Data numbering plan
- generic: Generic number plan
- isdn: ISDN tel numbering plan
- isdn-mobile: ISDN mobile numbering plan
- land-mobile: Land mobile numbering plan
- maritime-mobile: Maritime mobile numbering plan
- nw-specific: Private network / network-specific numbering plan
- telex: Telex numbering plan
- unknown: Unknown numbering plan

Usage Guidelines

Select ISN telephone number plan for GTT process.

Examples

The following command sets the numbering plan to use during GTT processing to isdn
numbering-plan isdn
translation-type

Configures the global title translation (GTT) process to apply a specific number for translation during the GTT process.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > GTT Association Configuration > GT-Format3 Configuration

```
configure > global title translation association instance instance_number > gt-format format_number
```

Entering the above command sequence results in the following prompt:
```
[local] host_name (config-gtt-instance-format3)#
```

**Syntax Description**

```
translation-type number
```

- **number**
  
  Must be an integer between 0 and 255.
  
  Default is 0

**Usage Guidelines**

Use this command to define the translation-type to be used during the global title translation process.

**Examples**

```
translation-type 233
```
GT-Format4 Configuration Mode Commands

The GT-Format4 configuration mode is a sub-mode for either the Global Title Translation Association configuration mode or the Global Title Translation Address-Map configuration mode. This sub-mode configures a set of rules used in the global title translation (GTT) process.

**Command Modes**

Exec > Global Configuration > GTT Association Configuration > GT-Format4 Configuration

```
configure> global title translation association instance instance_number > gt-format format_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-gtt-instance-format4)#
```

**Important**

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

- encoding-scheme, page 1094
- end, page 1095
- exit, page 1096
- nature-of-address, page 1097
- numbering-plan, page 1098
- translation-type, page 1099
encoding-scheme

Configures the encoding-scheme to use during GTT.

Product
SGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > GTT Association Configuration > GT-Format4 Configuration
```
configure > global title translation association instance instance_number > gt-format format_number
```

Entering the above command sequence results in the following prompt:
```
[local] host_name(config-gtt-instance-format4)#
```

Syntax Description
```
encoding scheme scheme_type
```

scheme_type
Select one of the following encoding scheme types to determine the encoding type to be used during GTT:

- **bcd-even**: BCD even encoding scheme
- **bcd-odd**: BCD odd encoding scheme
- **nw-specific**: Network-specific encoding scheme
- **unknown**: Unknown encoding scheme

Usage Guidelines
Select BCD even encoding for GTT

Examples
```
encoding scheme bcd-even
```
end

Exits the configuration mode and returns to the Exec mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax Description

end

Usage Guidelines

Change the mode back to the Exec mode.
exit

Exits the configuration mode and returns to the Global configuration mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax Description
exit

Usage Guidelines
Return to the Global configuration mode.
nature-of-address

Configures the indicator to identify the nature of the address.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > GTT Association Configuration > GT-Format4 Configuration

```
configure > global title translation association instance instance_number > gt-format format_number
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-gtt-instance-format4)#
```

**Syntax Description**
```
nature-of-address { international | national | subscriber }
```

- **international**
  Identifies the numbers as international.

- **national**
  Identifies the numbers as matching the national configuration.

- **subscriber**
  Identifies the numbers as subscriber numbers.

**Usage Guidelines**
Configure the identify of the GT format as national.

**Examples**
```
nature-or-address national
```
numbering-plan

Configures the GTT process to apply one of the numbering-plans during the GT translation process.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > GTT Association Configuration > GT-Format4 Configuration

configure > global title translation association instance instance_number > gt-format format_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-gtt-instance-format4)#

Syntax Description

numbering-plan plan_type

plan_type

Select one of the following numbering plans be employed during GTT:

- data: Data numbering plan
- generic: Generic number plan
- isdn: ISDN tel numbering plan
- isdn-mobile: ISDN mobile numbering plan
- land-mobile: Land mobile numbering plan
- maritime-mobile: Maritime mobile numbering plan
- nw-specific: Private network/ network-specific numbering plan
- telex: Telex numbering plan
- unknown: Unknown numbering plan

Usage Guidelines

Select ISN telephone number plan for GTT process.

Examples

numbering-plan isdn
translation-type

Configures the GTT process to apply a specific number for translation during the GTT process.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > GTT Association Configuration > GT-Format4 Configuration

```
configure > global title translation association instance instance_number > gt-format format_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-gtt-instance-format4)#
```

**Syntax Description**
`translation-type number`

- `number`
  - Must be an integer between 0 and 255.
  - Default is 0.

**Usage Guidelines**
Use this command to configure the translation-type to be implemented during the global title translation process.

**Examples**
`translation-type 231`
GTPC Load Control Profile Configuration Mode Commands

Load control enables a GTP-C entity (for example, an S-GW/P-GW) to send its load information to a GTP-C peer (e.g. an MME/SGSN, ePDG, TWAN) to adaptively balance the session load across entities supporting the same function (for example, an S-GW cluster) according to their effective load. The load information reflects the operating status of the resources of the GTP-C entity.

This chapter describes the GTPC Load Control Profile Configuration Mode commands.

**Command Modes**

Exec > Global Configuration > GTPC Load Control Profile Configuration

```
configure > gtpc-load-control-profile profile_name
```

Entering the above command results in the following prompt:

```
[local] host_name(config-gtpc-load-control-profile)#
```

---

**Important**

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

- end, page 1102
- exit, page 1103
- inclusion-frequency, page 1104
- load-control-handling, page 1106
- load-control-publishing, page 1108
- threshold, page 1110
- weightage, page 1112
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.
inclusion-frequency

Configures parameters to determine the inclusion frequency of the Load Control Information IE for a GTP-C Load Control Profile configuration.

Important

GTP-C Load Control Profile is a license-controlled feature. For more information, contact your Cisco account or support representative.

Product

P-GW
SAEGW
S-GW

Privilege

Administrator, Security Administrator

Command Modes

Exec > Global Configuration > GTPC Load Control Profile Configuration

configure > gtpc-load-control-profile profile_name

Entering the above command results in the following prompt:

[local] host_name (config-gtpc-load-control-profile)#

Syntax Description

inclusion-frequency { advertisement-interval interval_in_seconds | change-factor change_factor } 
default inclusion-frequency { advertisement-interval | change-factor }

inclusion-frequency

Specifies that parameters to determine the inclusion frequency of the Load Control Information IE for a GTP-C Load Control Profile configuration will be configured. The Load Control Information IE is a 3GPP-specific IE that is sent to peers when a configured threshold is reached. This parameter specifies how often the operator wants to send this information to the peers.

advertisement-interval interval_in_seconds

Configures the advertisement-interval for Load Control in seconds. Specifies how often load control information should be sent to the peers. If configured to 0, the node will send load control information in each and every outgoing message to the peers.

interval_in_seconds must be an integer from 0 to 3600.

Default: 300
change-factor change_factor

Configures the change factor for Load Control. If the load control factor changes by the configured factor, whether it is an increase or decrease, the load control information should be sent to the peers. This information is only sent to the peers when the load factor changes by the factor configured.

change_factor must be an integer from 1 to 20.

Default: 5%

default

Returns configured parameters to their default value.

Usage Guidelines

Use this command to specify parameters to determine the inclusion frequency of the Load control information IE for a GTP-C Load Control Profile configuration. This IE reflects the current operating status of the network element based on the configured weightage parameters. The network element ensures that new/updated load control information is propagated to the target receivers within an acceptable delay, so that the purpose of the information (i.e., effective load balancing) is achieved.

The weightage command in GTP-C Load Control Profile Configuration Mode should also be configured along with the inclusion-frequency setting.

If this setting is not configured, the node will use the default setting.

The Load Control profile must be associated with a P-GW, S-GW, or SAEGW service using one of the following commands:

- P-GW: associate command in P-GW Service Configuration Mode
- S-GW: associate command in S-GW Service Configuration Mode
- SAEGW: associate commands in both P-GW and S-GW Service Configuration modes

Examples

This example configures the inclusion-frequency advertisement-interval to 120 seconds.

inclusion-frequency advertisement-interval 120
**load-control-handling**

Enables or disables the handling of GTP-C load control information provided to the MME and S-GW.

---

**Important**

GTP-C Load Control Profile is a licensed-controlled feature. For more information, contact your Cisco account or support representative.

---

**Product**

- P-GW
- S-GW
- SAEGW

**Privilege**

Administrator, Security Administrator

**Command Modes**

Exec > Global Configuration > GTP Load Control Profile Configuration

```
configure > gtpc-load-control-profile profile_name
```

Entering the above command results in the following prompt:

```
[local] host_name(config-gtpc-load-control-profile)#
```

**Syntax Description**

```
| no | load-control-handling { home | visited }
| default | load-control-handling
```

- **no**
  
  Disables load-control-handling for the specified option (home or visited).

- **default**

  Returns the load-control-handling feature to its default behavior (enabled).

- **load-control-handling**

  Enables load control handling for the specified option.

- **home**

  Enables load control handling information for the home PLMN.
**visited**
Enables/disables load control handling information for the visited PLMN.

**Examples**
Use this command to enable/disable the handling of load control information handling for the home or visited PLMN.
If no parameters are specified, the system will use the default settings.
The Load Control Profile must be associated with a P-GW, S-GW, or SAEGW service using one of the following commands:
- P-GW: `associate` command in P-GW Service Configuration Mode
- S-GW: `associate` command in S-GW Service Configuration Mode
- SAEGW: `associate` commands in both P-GW and S-GW Service Configuration modes

**Examples**
This command enables load control handling for the home PLMN.
`load-control-handling home`
load-control-publishing

Enables/disables the publishing of GTP-C load control information.

Important

GTP-C Load Control Profile is a license-controlled feature. For more information, contact your Cisco account or support representative.

Product

P-GW
S-GW
SAEGW

Privilege

Administrator, Security Administrator

Command Modes

Exec > Global Configuration > GTPC Load Control Profile Configuration

configure > gtpc-load-control-profile profile_name

Entering the above command results in the following prompt:

[local] host_name(config-gtpc-load-control-profile)#

Syntax Description

| no | load-control-publishing { home | visited }

default load-control-publishing

no

Disables load control publishing for the specified option.

default

Returns load control publishing to its default behavior (enabled).

load-control-publishing

Enables the publishing of load control information towards the home or visited PLMN.

home

Enables load control publishing information for the home PLMN.
visited

Enables load control publishing information for the visited PLMN.

Usage Guidelines

Use this command to enable/disable load control information publishing for the home or visited PLMN. The Load Control Profile must be associated with a P-GW, S-GW, or SAEGW service using one of the following commands:

- P-GW: `associate` command in P-GW Service Configuration Mode
- S-GW: `associate` command in S-GW Service Configuration Mode
- SAEGW: `associate` commands in both P-GW and S-GW Service Configuration modes

Examples

This command enables the publishing of load control information towards the visited peers.

`load-control-publishing visited`
threshold

Configures the minimum threshold value above which PGW-provided GTP-C load control information should be utilized for calculating the PGW effective weight during initial node selection.

Important

GTP-C Load Control Profile is a license-controlled feature. For more information, contact your Cisco account or support representative.

Product

P-GW
S-GW
SAEGW

Privilege

Administrator, Security Administrator

Command Modes

Exec > Global Configuration > GTPC Load Control Profile Configuration

configure > gtpc-load-control-profile profile_name

Entering the above command results in the following prompt:

[local] host_name(config-gtpc-load-control-profile) #

Syntax Description

| no | threshold

threshold

Enables the configuration of the minimum threshold value above which PGW-provided load control information should be utilized for calculating the P-GW effective weight during initial node selection.

percentage

Enter the threshold setting as a percentage of 100%. The entry must be an integer from 1 to 100. The default setting is 50%.

no

Disables the configured threshold setting.
Usage Guidelines

Use this command to configure the minimum threshold value above which PGW-provided load control information should be utilized for calculating the P-GW effective weight during initial node selection. The Load Control Profile must be associated with a P-GW, S-GW, or SAEGW service using one of the following commands:

- P-GW: `associate` command in P-GW Service Configuration Mode
- S-GW: `associate` command in S-GW Service Configuration Mode
- SAEGW: `associate` commands in both P-GW and S-GW Service Configuration modes

Examples

This command sets the threshold to 60%.

`threshold 60`
weightage

Configures weightage for various GTP-C load control profile parameters.

---

**Important**

GTP-C Load Control Profile is a license-controlled feature. For more information, contact your Cisco account or support representative.

---

**Product**

- P-GW
- SAEGW
- S-GW

**Privilege**

Administrator, Security Administrator

---

**Command Modes**

Exec > Global Configuration > GTP Load Control Profile Configuration

**Syntax Description**

```
weightage system-cpu-utilization percentage
weightage system-memory-utilization percentage
weightage license-session-utilization percentage
weightage default weightage
```

```
weightage

Specifications that system memory, system CPU, and license session utilization parameters will be configured.
```

---

**Important**

All parameters must be specified. The total of all three parameter settings should total, but not exceed, 100%.

---

**system-cpu-utilization percentage**

Specifies system CPU utilization weightage as a percentage of 100.

**percentage** must be an integer from 0 to 100.

Default: 40%
**Usage Guidelines**

Use this command to set weightage percentages for system CPU, memory, and license session utilization as part of a GTP-C Load Control Profile configuration. These settings constitute the basic Load Control Profile for this network element. These parameters allow the P-GW/S-GW/SAEGW to send its load information to a peer GTP control plane node which the receiving GTP control plane peer node uses to augment existing GW selection procedure for the P-GW and S-GW. Load Information reflects the operating status of the resources of the originating GTP control plane node.

If no parameters are specified, the system will use the default settings.

Operators should also configure the **inclusion-frequency** command in GTP-C Load Control Profile Configuration mode to specify parameters to determine the inclusion frequency of the Load Control Information IE sent to peers for the GTP-C Load Control Profile configuration.

The Load Control Profile must be associated with a P-GW, S-GW, or SAEGW service using one of the following commands:

- **P-GW**: `associate` command in P-GW Service Configuration Mode
- **S-GW**: `associate` command in S-GW Service Configuration Mode
- **SAEGW**: `associate` commands in both P-GW and S-GW Service Configuration modes

**Examples**

The following example configures system-cpu-utilization at 30%, system-memory utilization at 40%, and license-utilization at 30%.

```
weightage system-cpu-utilization 30 system-memory-utilization 40 license-session-utilization 30
```
GTPC Overload Control Profile Configuration Mode Commands

Overload control enables a GTP-C entity becoming or being overloaded to gracefully reduce its incoming signalling load by instructing its GTP-C peers to reduce sending traffic according to its available signalling capacity to successfully process the traffic. A GTP-C entity is in overload when it operates over its signalling capacity, which results in diminished performance (including impacts to handling of incoming and outgoing traffic).

This chapter describes the GTPC Overload Profile Configuration Mode Commands

**Command Modes**

Exec > Global Configuration > GTPC Overload Control Profile Configuration

```
configure > gtpc-overload-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-gtpc-overload-control-profile)#
```

---

**Important**

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

- end, page 1117
- exit, page 1118
- inclusion-frequency, page 1119
- message-prioritization, page 1121
- overload-control-handling, page 1123
- overload-control-publishing, page 1125
- self-protection-behavior, page 1127
- tolerance, page 1129
- throttling-behavior, page 1131
- validity-period, page 1133
- weightage, page 1135
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.
inclusion-frequency

Configure parameters to determine the inclusion frequency of the Overload Control Information IE.

Important

GTP-C Overload Control Profile is a license-controlled feature. For more information, contact your Cisco account or support representative.

Product

P-GW
SAEGW
S-GW

Privilege

Administrator, Security Administrator

Command Modes

Exec > Global Configuration > GTPC Overload Control Profile Configuration

configure > gtpc-overload-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-gtpc-overload-control-profile)#

Syntax Description

inclusion-frequency { advertisement-interval \( interval\_{in\_seconds} \mid change-factor\ \( change\_{factor} \) }

default inclusion-frequency { advertisement-interval | change-factor }

inclusion-frequency

Specifies that parameters to determine the inclusion frequency of the Overload Control Information IE for a GTP-C Overload Control Profile configuration will be configured. The Overload Control Information IE is a 3GPP-specific IE that is sent to peers when a configured threshold is reached. This parameter specifies how often the operator wants to send overload information to the peers.

advertisement-interval \( interval\_{in\_seconds} \)

Configures the advertisement-interval for overload control in seconds. Specifies how often overload control information should be sent to the peers. If configured to 0, the node will send overload control information in each and every outgoing message to the peers.

\( interval\_{in\_seconds} \) must be an integer from 0 to 3600.

Default: 300
**change-factor change_factor**

P-GW only. Configures the change factor for overload control. If the overload control factor changes by a configured factor, whether by an increase or decrease, the overload control information should be sent to the peers. This information is only sent to the peers when the overload factor changes by the factor configured. 

*change_factor* must be an integer from 1 to 20.

Default: 5%

**Usage Guidelines**

Use this command to configure parameters to decide inclusion frequency of Overload Control Information IE. How often the sender includes the overload control information is implementation specific. The network element ensures that new/updated overload control information is propagated to the target receivers within an acceptable delay so that the purpose of the information, effective load balancing, is achieved.

If no parameters are specified, the system will use the default settings.

The Overload Control Profile must be associated with a P-GW, S-GW, or SAEGW service using one of the following commands:

- P-GW: `associate` command in P-GW Service Configuration Mode
- S-GW: `associate` command in S-GW Service Configuration Mode
- SAEGW: `associate` commands in both P-GW and S-GW Service Configuration modes

**Examples**

The following example configures the inclusion-frequency change factor to 10.

`inclusion-frequency change-factor 10`
message-prioritization

Configures the priority percentage to be given to the two specific message groups for the GTP-C Overload Control Profile feature.

Important  GTP-C Overload Control Profile is a license-controlled feature. For more information, contact your Cisco account or support representative.

Product  ePDG
P-GW
SAEGW
S-GW

Privilege  Administrator, Security Administrator

Command Modes  Exec > Global Configuration > GTPC Overload Control Profile Configuration
configure > gtpc-overload-control-profile profile_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-gtpc-overload-control-profile)#

Syntax Description  
message-prioritization group1 percentage group2 percentage
| no | default | message-prioritization

no
Disables message-prioritization for this node.

default
Returns the message-prioritization settings to their default value. The defaults are 50% for each message group.

message-prioritization
Configures the priority percentage to be given to the two message groups.
In the overload control it is possible to apply message throttling (when peer indicated it is overloaded) based on message priority. To apply message prioritization using the loss algorithm the node must know how many messages each node (PGW or ePDG) is expected to generate. This keyword allows the operator to define the expected number of messages in, as a percentage in each message group. **group1** messages are:

- Update Bearer Request message for default bearer generated from PGW ingress
- Update Bearer Request message for dedicated bearer generated from PGW ingress
- Handoff Create Session Request message generated from ePDG egress.

The entry must be an integer from 0 to 100.
The default setting is 50%.

**group2** messages are:

- Create Bearer Request message for default bearer generated from PGW ingress
- PDN connection requested Create Session Request message from ePDG egress.

The entry must be an integer from 0 to 100.
The default setting is 50%.

**Usage Guidelines**

Use this command to configure priority the message prioritization percentage to be given to the two specific message groups.

The Overload Control Profile must be associated with a P-GW, S-GW, or SAEGW service using one of the following commands:

- P-GW: **associate** command in P-GW Service Configuration Mode
- S-GW: **associate** command in S-GW Service Configuration Mode
- SAEGW: **associate** commands in both P-GW and S-GW Service Configuration modes

**Examples**

This command sets the message-prioritization for both message groups to 40%.

```
message prioritization group1 40 group2 60
```
overload-control-handling

Enables/disables the handling of GTP-C overload control information for the node.

Important
---
GTP-C Overload Control Profile is a license-controlled feature. For more information, contact your Cisco account or support representative.

Product
---
P-GW
SAEGW
S-GW

Privilege
---
Administrator, Security Administrator

Command Modes
---
Exec > Global Configuration > GTPC Overload Control Profile Configuration

configure > gtpc-overload-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-gtpc-overload-control-profile)#

Syntax Description
---
[ no ] overload-control-handling { home | visited }

no
Disables overload control information handling for this node.

overload-control-handling
Enables the handling of overload control information.

home
Specifies that the handling of overload control information will be enabled for the home PLMN.

visited
Specifies that the handling of overload control information will be enabled for the visited PLMN.

Usage Guidelines
---
Use this command to enable/disable the handling of overload control information for this node.
The Load Control Profile must be associated with a P-GW, S-GW, or SAEGW service using one of the following commands:

- P-GW: `associate` command in P-GW Service Configuration Mode
- S-GW: `associate` command in S-GW Service Configuration Mode
- SAEGW: `associate` commands in both P-GW and S-GW Service Configuration modes

**Examples**

This command enables the handling of overload control information for the home PLMN.

`overload-control-handling home`
overload-control-publishing

Enables/disables the publishing of overload control information towards the home or visited PLMN.

**Important**

GTP-C Overload Control Profile is a license-controlled feature. For more information, contact your Cisco account or support representative.

### Product

- P-GW
- SAEGW
- S-GW

### Privilege

Administrator, Security Administrator

### Command Modes

Exec > Global Configuration > GTPC Overload Control Profile Configuration

**configure > gtpc-overload-control-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-gtpc-overload-control-profile)#
```

### Syntax Description

- **no** overload-control-publishing { home | visited }
- default overload-control-publishing

**no**

Disables overload control information publishing towards the home or visited PLMN.

**default**

Returns overload control publishing to the default setting.

**overload-control-publishing**

Enables the publishing of overload control information.

**home**

Enables the publishing of overload control information towards the home PLMN.
**visited**

Enables the publishing of overload control information towards the visited PLMN.

**Usage Guidelines**

Use this command to enable/disable the publishing of overload control information towards the home or visited PLMN.

The Load Control Profile must be associated with a P-GW, S-GW, or SAEGW service using one of the following commands:

- **P-GW**: `associate` command in P-GW Service Configuration Mode
- **S-GW**: `associate` command in S-GW Service Configuration Mode
- **SAEGW**: `associate` commands in both P-GW and S-GW Service Configuration modes

**Examples**

This command enables overload control publishing towards the visited PLMN.

`overload-control-publishing visited`
**self-protection-behavior**

Configures self protection behavior for up to three APN names or EARP values for the GTP-C Overload Control Profile feature.

---

**Important**

GTP-C Overload Control Profile is a license-controlled feature. For more information, contact your Cisco account or support representative.

---

**Product**

- P-GW
- SAEGW
- S-GW

**Privilege**

Administrator, Security Administrator

**Command Modes**

Execute > Global Configuration > GTPC Overload Control Profile Configuration

```bash
configure > gtpc-overload-control-profile
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-gtpc-overload-control-profile)#
```

**Syntax Description**

```
| no | self-protection-behavior { apn apn_name * exclude | earp { 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 * } exclude } }
```

- **no**
  
  Disables self-protection-behavior for this node.

- **self-protection-behavior**
  
  Enables self protection behavior for this node

- **apn apn_name** *
  
  Specify up to three APN names to be allowed under self-protection behavior.

- **earp { 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 * }**
  
  Configures up to three EARP priority level values so that incoming request messages for the configured EARP priority values are not rejected even if the system is under self-protection mode.
exclude

Specifies that configured emergency pdn connections and/or EARP priority values are not rejected.

Usage Guidelines

Use this command to configure GTP-C overload control self-protection behavior. This functionality enables the operator to configure up to three APN names and up to three EARP priority level values for self-protection mode so that incoming request messages for emergency packet data node (PDN) connections and/or configured EARP priority values are not rejected even if the system is under self-protection mode.

The Load Control Profile must be associated with a P-GW, S-GW, or SAEGW service using one of the following commands:

• P-GW: associate command in P-GW Service Configuration Mode
• S-GW: associate command in S-GW Service Configuration Mode
• SAEGW: associate commands in both P-GW and S-GW Service Configuration modes

Examples

The following command configures self protection behavior for the APN named APN1.

```
self-protection-behavior apn APN1
```
tolerance

Configures GTP-C Overload Control Profile tolerance limits.

Important GTP-C Overload Control Profile is a license-controlled feature. For more information, contact your Cisco account or support representative.

Product
- P-GW
- SAEGW
- S-GW

Privilege
Administrator, Security Administrator

Command Modes
- Exec > Global Configuration > GTPC Overload Control Profile Configuration
- configure > gtpc-overload-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-gtpc-overload-control-profile)#

Syntax Description

tolerance { initial-reduction-metric percentage | threshold report-reduction-metric percentage self-protection-limit percentage } 
default tolerance { initial-reduction-metric | threshold }

tolerance
Specifies that GTP-C overload profile configuration tolerance parameters will be configured.

initial-reduction-metric percentage
Configures initial overload reduction metric value to be advertised upon reaching minimum overload tolerance limit. When reaching the configured minimum threshold, this parameter specifies how much the node wants the peers to reduce incoming traffic.

percentage must be an integer from 1 to 100.
Default: 10%
threshold report-reduction-metric percentage

Configures the minimum overload tolerance threshold for advertising overload reduction metric to the peer. When the minimum threshold is reached, the node will report this information to peers. When the maximum limit is reached, the node will go into self-protection mode.

Important

The threshold report-reduction-metric should always be lower than the self-protection-limit.

percentage must be an integer from 1 to 100.
Default: 80%

self-protection-limit percentage

Configures the maximum overload tolerance threshold after which node will move to self protection mode. When the maximum limit is reached, the node will start rejecting all incoming messages, except for delete messages. The node will not initiate any new messages to the peers. This is to mitigate the overload condition.

percentage must be an integer from 1 to 100.
Default: 95%

Usage Guidelines

Use this command to configure GTP-C Overload Control Profile tolerance limits.
Default parameters are used if any parameters are not configured.
The Overload Control Profile must be associated with a P-GW, S-GW or SAEGW service using one of the following commands:

- P-GW: associate command in P-GW Service Configuration Mode
- S-GW: associate command in S-GW Service Configuration Mode
- SAEGW: associate commands in both P-GW and S-GW Service Configuration modes

Examples

The following example configures the initial-reduction-metric to 20%.
tolerance initial-reduction-metric 20
throttling-behavior

Configures throttling behavior based on peer's overload reduction-metric by excluding some or all emergency events and/or EARP messages for the GTP-C Overload Control Profile feature.

Important
GTP-C Overload Control Profile is a license-controlled feature. For more information, contact your Cisco account or support representative.

Product
P-GW
SAEGW
S-GW

Privilege
Administrator, Security Administrator

Command Modes
Exec > Global Configuration > GTPC Overload Control Profile Configuration

configure > gtpc-overload-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-gtpc-overload-control-profile)#

Syntax Description

throttling-behavior { earp [1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 *] exclude } |
emergency-events exclude }

no throttling-behavior { earp [1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 *] exclude } |
emergency-events exclude }

throttling-behavior

Configures throttling behavior based on peer's overload reduction-metric.

earp [1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 *] exclude

Excludes the specified messages with configured earp from throttling due to peer's overload-reduction metric. If a bearer with configured EARP is created or updated, it will be excluded from throttling.

*: More than one of the previous keywords can be entered within a single command.
emergency events exclude

P-GW Only. Excludes all emergency events from throttling due to the peer's overload reduction-metric. While reducing messages towards the peer based on the overload information received from the peer, the P-GW will exclude events sent for emergency sessions.

Usage Guidelines

Use this command to configure throttling behavior based on peer's overload reduction-metric by excluding some or all emergency events and/or messages with configured EARL. Message throttling applies only to initial messages. Triggered request or response messages should not be throttled since that would result in the retransmission of the corresponding request message by the sender.

If throttling behavior is configured, the profile can be associated with an S-GW or P-GW service. If a P-GW specific keyword is configured, and the profile is associated with an S-GW service, the S-GW will ignore the P-GW specific configuration. Only the parameters specific to S-GW or P-GW will be utilized.

The Overload Control Profile must be associated with a P-GW, S-GW, or SAEGW service using one of the following commands:

- P-GW: `associate` command in P-GW Service Configuration Mode
- S-GW: `associate` command in S-GW Service Configuration Mode
- SAEGW: `associate` commands in both P-GW and S-GW Service Configuration modes

Examples

The following example excludes emergency events.

`throttling-behavior emergency-events exclude`
validity-period

Configures the time, in seconds, that specifies how long the overload control information is valid.

**Important** GTP-C Overload Control Profile is a license-controlled feature. For more information, contact your Cisco account or support representative.

**Product**
- P-GW
- SAEGW
- S-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > GTPC Overload Control Profile Configuration
`configure > gtpc-overload-control-profile profile_name`

Entering the above command sequence results in the following prompt:
`[local] host_name(config-gtpc-overload-control-profile)#`

**Syntax Description**
`validity-period seconds`
`default validity-period`

`validity-period seconds`
Specifies the length of time during which the overload condition specified by the OCI IE is to be considered as valid, unless overridden by subsequent new overload control information.

seconds must be an integer from 1 to 3600.
Default: 600

**Usage Guidelines**
Use this command to configure how long the overload control profile information is valid.
If no validity-period is configured, the system will use the default setting.
The Overload Control profile must be associated with a P-GW, S-GW, or SAEGW service using one of the following commands:
- P-GW: `associate` command in P-GW Service Configuration Mode
- S-GW: `associate` command in S-GW Service Configuration Mode
• SAEGW: **associate** commands in both P-GW and S-GW Service Configuration modes

**Examples**
The following example configures the validity-period to 700 seconds:

`validity-period 700`
weightage

Configures weightage for various GTP-C Overload Control Profile parameters.

---

**Important**
GTP-C Overload Control Profile is a license-controlled feature. For more information, contact your Cisco account or support representative.

---

**Product**

- P-GW
- SAEGW
- S-GW

**Privilege**

Administrator, Security Administrator

**Command Modes**

Exec > Global Configuration > GTPC Overload Control Profile Configuration

configure > gtpc-overload-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-gtpc-overload-control-profile)#

**Syntax Description**

weightage system-cpu-utilization percentage
system-memory-utilization percentage
license-session-utilization percentage
default weightage

weightage

Specifies that system memory, CPU, and license session utilization parameters are to be configured.

---

**Important**

All parameters must be specified. The total weightage for all parameters should be 100%. The total of all three parameters cannot exceed 100%.

---

**system-cpu-utilization percentage**

Specify the desired system CPU utilization weightage as a percentage of 100.

*percentage* must be an integer from 0 to 100.

Default: 40%
system-memory-utilization percentage
Specify the system memory utilization weightage as a percentage of 100.
percentage must be an integer from 0 to 100.
Default: 30%

license-session-utilization percentage
Specify the license session utilization weightage as a percentage of 100.
percentage must be an integer from 0 to 100.
Default: 30%

default weightage
Returns all settings to their default value.

Usage Guidelines
Use this command to specify weightage for various GTP-C Overload Control Profile parameters. These parameters constitute the basic settings for this GTP-C Overload Control Profile. Communication of these parameters indicates to peers when this network element is becoming or being overloaded. When this occurs, the NE will be able to instruct its peers to gracefully reduce its incoming signalling load by instructing the peers to reduce sending traffic according to its available signalling capacity to successfully process the traffic. A GTP-C entity is in overload when it operates over its signalling capacity, which results in diminished performance (including impacts to handling of incoming and outgoing traffic).

Use the inclusion-frequency command in GTP-C Overload Profile Configuration mode to determine the inclusion frequency of the Overload-Load control information IE that is sent to the peers to keep them up to date on the overload condition on this network element.

If no parameters are specified, the system will use the default settings.

The Overload Control profile must be associated with a P-GW, S-GW, or SAEGW service using one of the following commands:

- P-GW: associate command in P-GW Service Configuration Mode
- S-GW: associate command in S-GW Service Configuration Mode
- SAEGW: associate commands in both P-GW and S-GW Service Configuration modes

Examples
This example configures system-cpu-utilization to 30%, system-memory-utilization to 30%, and license-session-utilization to 40%.
weightage system-cpu-utilization 30 system-memory-utilization 30 license-session-utilization 40
GTPP Server Group Configuration Mode

Commands

GTPP server group commands facilitate the setup of the hard disk for CDR storage. They also support accounting and charging functionality within a context, and configuration of a group (list) of charging gateway function (CGF) servers on a per subscriber or per GGSN/P-GW APN level.

The GTPP Server Group Configuration Mode is used to create and manage the GTPP server groups within the context or system.

**Command Modes**

Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

```
configure > context context_name > gtpp group group_name
```

Entering the above command sequence results in the following prompt:

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

**Important**

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

- end, page 1139
- exit, page 1140
- gtpp attribute, page 1141
- gtpp charging-agent, page 1152
- gtpp data-record-format-version, page 1154
- gtpp data-request sequence-numbers, page 1156
- gtpp deadtime, page 1158
- gtpp dead-server suppress-cdrs, page 1160
- gtpp detect-dead-server, page 1162
- gtpp dictionary, page 1164
• gtpp duplicate-hold-time, page 1167
• gtpp echo-interval, page 1169
• gtpp egcdr, page 1171
• gtpp error-response, page 1175
• gtpp max-cdrs, page 1176
• gtpp max-pdu-size, page 1178
• gtpp max-retries, page 1180
• gtpp mbms bucket, page 1182
• gtpp mbms interval, page 1183
• gtpp mbms tariff, page 1184
• gtpp mbms volume, page 1186
• gtpp redirection-allowed, page 1187
• gtpp redirection-disallowed, page 1189
• gtpp server, page 1190
• gtpp source-port-validation, page 1193
• gtpp storage-server, page 1194
• gtpp storage-server local file, page 1195
• gtpp storage-server max-retries, page 1200
• gtpp storage-server mode, page 1201
• gtpp storage-server timeout, page 1203
• gtpp suppress-cdrs zero-volume, page 1205
• gtpp suppress-cdrs zero-volume-and-duration, page 1207
• gtpp timeout, page 1209
• gtpp transport-layer, page 1210
• gtpp trigger, page 1212
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.
gtpp attribute

Enables the specification of some of the optional fields in the CDRs that the GSN (GGSN or SGSN) generates and/or how the information is to be presented. Many keywords are also applicable to S-GW and P-GW CDRs.

**Product**
- GGSN
- P-GW
- SAEGW
- SaMOG
- SGSN
- S-GW

**Privilege**
Security Administrator, Administrator

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

`configure > context context_name > gtpp group group_name`

Entering the above command sequence results in the following prompt:

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

**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 | sgsnpdprecord | sgwrecord | served-mnai | served-pdp-pdn-address-extension | served-pdp-pdn-address-prefix-length | sgsn-change | sms { destination-number | recording-entity | service-centre } | sgw-ipv6-addr | sna-ipv6-addr | sponsor-id | start-time | stop-time | twanuli | uli | user-csg-information } +

default gtpp attribute { apn-ambr [ include-for-all-bearers | include-for-default-bearer | include-for-non-gbr-bearers ] | apn-ni | apn-selection-mode | charging-characteristic-selection-mode | 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 | 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 }
```

---

**gtpp attribute**

Enables the specification of some of the optional fields in the CDRs that the GSN (GGSN or SGSN) generates and/or how the information is to be presented. Many keywords are also applicable to S-GW and P-GW CDRs.

**Product**
- GGSN
- P-GW
- SAEGW
- SaMOG
- SGSN
- S-GW

**Privilege**
Security Administrator, Administrator

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

`configure > context context_name > gtpp group group_name`

Entering the above command sequence results in the following prompt:

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

**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 | sgsnpdprecord | sgwrecord | served-mnai | served-pdp-pdn-address-extension | served-pdp-pdn-address-prefix-length | sgsn-change | sms { destination-number | recording-entity | service-centre } | sgw-ipv6-addr | sna-ipv6-addr | sponsor-id | start-time | stop-time | twanuli | uli | user-csg-information } +

default gtpp attribute { apn-ambr [ include-for-all-bearers | include-for-default-bearer | include-for-non-gbr-bearers ] | apn-ni | apn-selection-mode | charging-characteristic-selection-mode | 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 | 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 }
```
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 | insi-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 | record-extension | 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
Resets the default attribute values for this GTPP group configuration.

no
Disables the specified optional field so that the information will not be present in generated 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 custom 24 GTPP dictionary.

Important
This keyword option will be available only if a valid license is installed. For more information, contact your Cisco account representative.

The APN Aggregate Maximum Bit Rate (AMBR) is a subscription parameter stored per APN. It limits the aggregate bit rate that can be expected to be provided across all non-GBR bearers and across all PDN connections of the same APN. Each of these non-GBR bearers potentially utilize the entire APN AMBR, e.g. when the other non-GBR bearers do not carry any traffic. The APN AMBR is present as part of QoS information.

In 15.0 and later releases, this CLI command should be configured along with the following additional options to support APN-AMBR reporting in SGW-CDRs in all GTPP dictionaries.

- **include-for-all-bearers**: Includes the APN-AMBR information in SGW-CDRs for all bearers (GBR and NON-GBR)
- **include-for-default-bearer**: Includes APN-AMBR information in SGW-CDRs only for default bearer.
- **include-for-non-gbr-bearers**: Includes APN-AMBR information for non-gbr-bearers.

This feature is required to enable post-processing of CDRs to verify MVNO subscribers actual QoS against invoicing systems.

Important
This CLI command and the associated options are not available for products other than S-GW and P-GW. The option "**non-gbr-bearers-only**" is available in S-GW and P-GW but the other options are available in S-GW only.

In the P-GW implementation, if the CLI command "**gtpp attribute apn-ambr**" is configured, it will be treated as "**gtpp attribute apn-ambr non-gbr-bearers-only**". In case of S-GW/P-GW combo if any of the options is configured, it will be considered that the attribute is available.
**apn-ni**
Default: Enabled
This keyword controls the inclusion of the optional field "APN" in the x-CDRs.

**apn-selection-mode**
Default: Enabled
This keyword controls the inclusion of the optional field "APN Selection Mode" in the x-CDRs.

**camel-info**
SGSN only
Enter this keyword to include CAMEL-specific fields in SGSN CDRs. Default: Disabled

**cell-plmn-id**
SGSN only
Enter this keyword to enable the system to include the Cell PLMN ID field in the M-CDR. Default: Disabled

**charging-characteristic-selection-mode**
Default: Enabled
This keyword controls the inclusion of the optional field "Charging Characteristic Selection Mode" in the x-CDRs.

**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, GTPP group name is used. For default GTPP groups, GTPP context-name is used. If the gtpp single-source centralized-lrsn is not configured, then node-id format for CDRs generated by Sessmgr is as follows: <1-byte Sessmgr 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>.

**Important**

If the gtpp single-source centralized-lrsn is not configured, the GGSN uses the GTPP context name as the Node-id-suffix (truncated to 16 characters) and the SGSN uses the GTPP group name as the node-id-suffix.

---

**losdv**
Default: Enabled
This keyword controls the inclusion of the optional field "List of Service Data" in the x-CDRs.

**ms-timezone**
Default: Enabled
This keyword controls the inclusion of the optional field "MS-Timezone" in the x-CDRs.

**msisdn**
Default: Enabled
This keyword controls the inclusion of the optional field "MSISDN" in the x-CDRs.

**node-id**
Default: Enabled
This keyword controls the inclusion of the optional field "Node ID" in the x-CDRs.

**node-id-suffix STRING**
Default: Disabled
Specifies the configured Node-ID-Suffix to use in the NodeID field of GTPP CDRs as an alphanumeric string of 1 through 16 characters. Each Session Manager task generates a unique NodeID string per GTPP context.

---

**Important**
The NodeID field is a printable string of the ndddSTRING format; n: The first digit is the Sessmgr restart counter having a value between 0 and 7. ddd: The number of sessmgr instances. Uses the specified NodeID-suffix in all CDRs. The "Node-ID" field consists of sessMgr Recovery counter (1 digit) n + AAA Manager identifier (3 digits) ddd + the configured Node-Id-suffix (1 to 16 characters) STRING. If the centralized LRSN feature is enabled, the "Node-ID" field will consist of only the specified NodeID-suffix (NodeID-prefix is not included). If this option is not configured, then GTPP group name will be used instead (For default GTPP groups, context-name will be used).

---

**Important**
If this node-id-suffix is not configured, the GGSN uses the GTPP context name as the Node-id-suffix (truncated to 16 characters) and the SGSN uses the GTPP group named as the node-id-suffix.
pdn-connection-id
Default: Enabled
This keyword controls the inclusion of the optional field "PDN Connection ID" in the x-CDRs.

pdp-address
Default: Enabled
This keyword controls the inclusion of the optional field "PDP Address" in the x-CDRs.

pdp-type
Default: Enabled
This keyword controls the inclusion of the optional field "PDP Type" in the x-CDRs.

pgw-ipv6-addr
Default: Disabled
Specifying this option allows to configure the P-GW IPv6 address.

Important
This attribute can be controllably configured in custom24 and custom35 SGW-CDR dictionaries.

pgw-plmn-id
Default: Enabled
This keyword controls the inclusion of the optional field "PGW PLMN-ID" in the x-CDRs.

plmn-id [ unknown-use ]
Default: Enabled
For SGSN, reports the SGSN PLMN Identifier value (the RAI) in the S-CDR provided if the dictionary supports it.
For GGSN, reports the SGSN PLMN Identifier value (the RAI) in the G-CDR if it was originally provided by the SGSN in the GTP create PDP context request. It is omitted if the SGSN does not supply one.
Normally when SGSN PLMN-id information is not available, the attribute sgsnPLMNIdentifier is not included in the CDR. This keyword enables the inclusion of the sgsnPLMNIdentifier with a specific value when the SGSN PLMN-id is not available.
unknown-use hex_num: is 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.

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

This command dictates some of the optional information fields that should be reported in CDRs generated by the GGSN. 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).

Examples

The following command disables the inclusion of the field "SGSN Change" in the S-CDR:

no gtpp attribute sgsn-change

Examples

The following command dictates that 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 CGF or the GSS.

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

**Privilege**
Security Administrator, Administrator

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

configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

- `gtpp charging-agent address ip_address [port port]`
- `no gtpp charging-agent`
- `address ip_address`
- `port port`

**no gtpp charging-agent**

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 G-CDR records to the CGF or the GSS.

*ip_address* is expressed in IPv4 dotted-decimal notation.

**port port**

Specifies the Charging Agent UDP port as an integer from 1 through 65535. If the port is not defined, the default port number 49999 will be used.
Important
Configuring GTPP charging-agent on port 3386 may interfere with ggsn-service configured with the same ip address.

Usage Guidelines
This command can be used to establish a UDP interface to connect to the GSS or this command can establish a Ga interface to connect to the CFG. 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 GGSN/SGSN is known to the CGF or the GSS. Therefore, the IP address used for the Ga or UDP interface could be identical to one bound to a GGSN/SGSN service (a Gn interface).

If no GGSN/SGSN services are configured in the same context as the Ga/UDP 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
```
```
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.

Product
- GGSN
- P-GW
- SGSN
- S-GW

Privilege
Administrator

Command Modes
- Exec > Global Configuration > Context Configuration
- configure > context context_name

Entering the above command sequence results in the following prompt:

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

Syntax Description

| no | gtpp data-record-format-version string |

no
Specifies that the default data record format will be encoded based on the GTPP dictionary being used.

\text{gtpp data-record-format-version string}

Specifies the 3GPP release version to be encoded. \text{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 \textit{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
- P-GW
- SAEGW
- SGSN
- S-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration
configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
gtp data-request sequence-numbers start { 0 | 1 }
default gtpp data-request sequence-numbers start
```

**default**
Default is 0 (zero).

**start { 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/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 number 0 in the echo request packets.
Examples

The following command sets the sequence to start at 1.

```
gtp data-request sequence-numbers start 1
```
gtpp deadtime

Configures the amount of time the GGSN/SGSN waits before attempting to communicate with a CGF that was previously marked as unreachable (non-responsive).

Product

- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

{context_name}host_name{config-gtpp-group}#

Syntax Description

gtpp deadtime time
default gtpp deadtime

default

Resets the deadtime to the default of 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 to 65535. Default: 120

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.
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 dead-server suppress-cdrs**

Configures the action the GGSN or the SGSN will take on CDRs generated during a communication failure between the GGSN or the SGSN and the GTPP servers.

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

**Privilege**
- Security Administrator
- Administrator

**Command Modes**

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

`configure > context context_name > gtpp group group_name`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

| no | default | gtpp dead-server suppress-cdrs |

- no
  
  Removes the suppression instruction from the configuration and sets the CDR suppression mode as disabled.

- default
  
  Resets to the default mode: disable suppression of CDRs when GTPP server detected as "dead" or unreachable.

**Usage Guidelines**

For the GGSN/P-GW: This command works in conjunction with the `gtpp detect-dead-server` to set an action when a communication failure is detected between the GGSN and a configured GTPP server. It disables the archiving of CDRs on the system when the GTPP server is unreachable or dead.

For the GGSN, P-GW, and SGSN: During a communication or server failure, the GGSN, P-GW, or SGSN typically retains the GTPP requests until the system buffer runs out of resources. This command enables suppression of the CDRs, so with this command the GGSN, P-GW, or the SGSN will start purging all CDRs associated with this GTPP group as soon as the GGSN/P-GW/SGSN detects that the GTPP server is down or that a communication failure has occurred. The CDRs generated, for the period while the server is down/unreachable, will also be purged.
Examples

The following command configures the system to start purging CDRs when a communication failure with a server is detected:

```
gtpp dead-server suppress-cdrs
```
gtpp detect-dead-server

Configures the number of consecutive communication failures that could occur before the system marks a CGF as "dead" (unreachable).

**Product**

GGSN
P-GW
SAEGW
SGSN
S-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

`configure > context context_name > gtpp group group_name`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`gtpp detect-dead-server consecutive-failures max_number`

`default gtpp detect-dead-server consecutive-failures`

`default`

Resets the system to the default number of consecutive failures.

`consecutive-failures max_number`

Default: 5

Specifies the number of failures that could occur before marking a CGF as down as an integer from 0 through 1000. If 0 (zero) is the value entered, the system will mark the CGF as dead after a single instance of `max-retries` has been attempted with no success, regardless of configured `deadtime`.

**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.

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 gtp 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:

```
gtp detect-dead-server consecutive-failures 8
```
**gtpp dictionary**

Designates specific dictionary used by GTPP for specific context.

**Product**

GGSN
P-GW
SAEGW
SGSN
S-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

```
configure > context context_name > gtpp group group_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
gtpp dictionary { custom1 | custom10 | custom11 | custom12 | custom13 | custom14 | custom15 | custom16 | custom17 | custom18 | custom19 | custom2 | custom20 | custom21 | custom22 | custom23 | custom24 | custom25 | custom26 | custom27 | custom28 | custom29 | custom3 | custom30 | custom31 | custom32 | custom33 | custom34 | custom35 | custom36 | custom37 | custom38 | custom39 | custom4 | custom40 | custom41 | custom42 | custom43 | custom44 | custom45 | custom46 | custom47 | custom48 | custom49 | custom5 | custom50 | custom51 | custom52 | custom53 | custom54 | custom55 | custom56 | custom57 | custom58 | custom59 | custom6 | custom60 | custom7 | custom8 | custom9 | standard }
default gtpp dictionary
```

default

Configures the default dictionary.

**custom1**

Custom-defined dictionary. It 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.
Custom-defined dictionary. It conforms to TS 32.015 v 3.6.0 for R99 but it does support the encoding of IP addresses in binary format for CDRs.

Custom-defined dictionary. It conforms to TS 32.015 v 3.6.0 for R99 except that:

- the Data Record Format Version information element contains 0x1307 instead of 0x1308
- "QoSRequested" is not present in the LoTV containers
- "QoSnegotiated" is added only for the first container and the container after a QoS change

Custom-defined dictionaries for GGSN only.

Custom-defined dictionary for customization of G-CDR records for GGSN only. This is compliant to 3GPP TS 32.298 (R6 v 6.5.0) for proprietary fields and encoding.

Custom-defined dictionary for customization of S-CDR records for SGSN only. This is compliant to 3GPP TS 32.298 (R6 v 6.6.0) for proprietary fields and encoding.

Custom-defined dictionaries for GGSN only.

Custom-defined dictionaries based on 3GPP 32.298 v6.4.1 for SGSN only.

- **custom31**: Custom-defined dictionary for S-CDR encoding. Includes a field appended for PLMN-ID.
- **custom33**: Custom-defined dictionary for S-CDR encoding. Includes a field appended for PLMN-ID and does not support diagnostic or SGSN-change fields.

Default: Enabled

A dictionary conforming 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 onto CDRs that are possibly duplicates while waiting for the primary CGF to come back up.

**Product**

GGSN
P-GW
SAEGW
SGSN
S-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

```
configure > context context_name > gtpp group group_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
gtpp duplicate-hold-time minutes
default gtpp duplicate-hold-time
```

**default**

Resets the configuration to the default value of 60 minutes for the duplicate hold time.

**minutes**

When the primary CGF is down, the number of minutes to hold onto CDRs that may be duplicates. *minutes* must be an integer from 1 to 10080. Default is 60.

**Usage Guidelines**

Use this command to configure how long to hold onto CDRs, that are possibly duplicates, while waiting for the primary CGF to come back up. If the GGSN determines that the primary CGF is down, CDRs that were sent to the primary CGF, but not acknowledged, are sent by the GGSN to the secondary CGF as "possibly duplicates". When the primary CGF comes back up, the GGSN 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 onto CDRs to 2 hours (120 minutes):

gtpp duplicate-hold-time minutes 120
gtpp echo-interval

Configures the frequency at which the system sends GTPP echo packets to configured CGFs.

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

**Privilege**
Security Administrator, Administrator

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

```
configure > context context_name > gtpp group group_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
```
gtpp echo-interval time

{ default | no } gtpp echo-interval

default

Resets the configuration to the default echo-interval of 60 seconds.

no

Disables the use of the echo protocol except for the scenarios described in the Usage section for this command.

**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
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 > GTPP Server Group Configuration

```
configure > context context_name > gtpp group group_name
```

Entering the above command sequence results in the following prompt:

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

**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 dll-path | rulebase-max-length rulebase_name_max_length | service-data-flow-threshold { interval interval | volume { downlink bytes | uplink bytes | total bytes | uplink bytes | downlink bytes } } | service-idle-timeout { 0 | service_idle_timeout } }

default gtpp egcdr { closure-reason admin-disconnect | dynamic-path | final-record include-content-ids only-with-traffic closing-cause same-in-all-partials | losdv-max-containers | lotdv-max-containers | service-idle-timeout 0 }

no gtpp egcdr { dynamic-path | rulebase-max-length | service-data-flow-threshold { interval | volume { downlink | uplink | total | uplink | downlink } } }
```

**closing-reason**
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.

```plaintext
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.

• **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`

Specifies 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`

Specifies 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 ddds. The DDL file will be parsed to populate metadata required to generate eGCDR/PGW-CDR.

---

**Important**

It is not recommended to enable `gtpp_egcdr dynamic-path` when there are active calls.

---

In this release, both current and new framework are functional to enable field defined (customer created) eGCDR/PGW-CDR generation. By default, the new framework is disabled.

**rulebase-max-length rulebase_name_max_length**

Specifies the maximum character length of charging rulebase name in LOSDVs of eG-CDR/P-GW-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-GW-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-CDP/P-CDR.

- `interval interval`: Specifies the time interval (in seconds) to close the eG-CDP/P-CDR if the minimum time duration thresholds for service data flow containers satisfied in flow-based charging. The interval is 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 eG-CDR/P-CDRs to the 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 40000000.

A service data flow container has statistics for an individual content ID. When the threshold is reached, the service data flow container is closed.

In 12.3 and earlier releases, when the CLI command `gtpp_egcdr service-data-flow threshold interval` was configured to 'n' seconds, the difference between "timeOfFirstUsage" and "timeOfReport" of LOSDV was always 'n' seconds for the LOSDVs closed due to "service-data-flow" threshold. Here, changeTime of LOSDV was reported incorrectly. It was always timeOfFirstUsage + 'n'. This does not hold true when the traffic for a particular content ID was not continuous.
In StarOS release 14.0 and later, when the command `gtppegcdr service-data-flow threshold interval` is configured to 'n' seconds, the difference between "timeOfFirstUsage" and "timeOfReport" of LOSDV can be any value between 1 and 'n' seconds depending on the continuity of traffic. If the traffic is not continuous, the difference is less than 'n' seconds. And if the traffic is continuous the difference will be 'n' seconds. When this CLI command is configured in the GTPP Server Group Configuration mode, each LOSDV will be closed at configured regular interval after the arrival of first packet.

```

service-idle-timeout { 0 | service_idle_timeout }
```

Specifies a time period during which 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.

0: Specifies there is no service-idle-timeout trigger.

`service_idle_timeout` is an integer from 10 through 86,400. Default: 0

**Usage Guidelines**

Use this command to configure individual triggers for eG-CDR/P-CDR generation.

**Examples**

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

`gtppegcdr losdv-max-containers 7`
gtpp error-response

Configures the response when the system receives an error response after transmitting a DRT (data record transfer) request.

Product

- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

context_name host_name(config-gtpp-group)#

Syntax Description

gtpp error-response { discard-cdr | retry-request }

default gtpp error-response

default

Resets the system's configuration to the default value for error-response. Default is retry-request.

discard-cdr

Purges the request upon receipt of an error response and not to retry.

retry-request

Retries 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 max-cdrs

Configures the maximum number of charging data records (CDRs) to be included in a packet.

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

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration
- configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

```
{context_name}\host_name{config-gtpp-group}#
```

**Syntax Description**

```
gtpp max-cdrs max_cdrs \[wait-time wait_time] \ndefault gtp max-cdrs
```

- **default**
  Sets the default configuration.

- **max_cdrs**
  Specifies the maximum number of CDRs to insert in a single packet as an integer from 1 through 255. Default: 1

- **wait-time wait_time**
  Specifies the number of seconds the GSN waits to send the packet while accumulating CDRs as defined by max-cdrs. If the wait-time interval expires before max-cdrs is reached, this keyword over-rides and the packet is sent. Default: Disabled
  wait_time is an integer from 1 through 300.

---

**Important**
The wait-time interval can only be enabled if the value for max-cdrs is greater than 1.
Usage Guidelines

The system places CDRs into a packet until either max-cdrs is met, wait-time times out, or the maximum PDU size, configured by the gtp max-pdu-size command, is met.

The gtp max-pdu-size and the wait-time parameters take priority over max-cdrs.

Important

This command's configuration is ignored if CDRs are stored on an SMC hard disk.

Examples

The following command configures the system to place a maximum of 10 CDRs in a single GTPP packet with a wait-time of 30 seconds:

gtp max-cdrs 10 wait-time 30
gtpp 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
- S-GW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration
  - configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

- `gtpp max-pdu-size pdu_size`  
  - `default gtpp max-pdu-size`

  **default**
  - Resets the default `max-pdu-size` of 65400.

  **pdu_size**
  - Specifies the maximum payload size (in bytes) of the GTPP packet as an integer from 1024 to 65400. The payload includes the CDR and the GTPP header. Default: 65400

**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).
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 CGF.

**Product**

GGSN
P-GW
SAEGW
SGSN
S-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

```
configure > context context_name > gtpp group group_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`gtpp max-retries max_attempts`

`default gtpp max-retries`

- `default`
  
  Resets the maximum number of to the default of 4.

- `max_attempts`
  
  Specifies the number of times the system attempts to communicate with a CGF that is not responding as an integer from 1 to 15. Default: 4

**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 \texttt{gtpd detect-dead-server} and \texttt{gtpd timeout} commands for additional information.

\textbf{Examples} 

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

\texttt{gtpd max-retries 8}
gtpp mbms bucket

Configures the traffic data volume (bucket) limit of charging buckets due to QoS changes of tariff time that can occur before a G-GBMS-CDR should be closed.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTTP Server Group Configuration

configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp mbms buckets number
| no | gtpp mbms buckets

number

Specifies the number of statistics container changes due to QoS changes or tariff time that can occur before a G-GBMS-CDR should be closed as an integer from 1 through 4. Default: 4

Usage Guidelines

Use this command to configure the traffic data volume (bucket) based G-GBMS-CDR generation triggers for MBMS user data service.

Examples

The following command configures the bucket-based trigger to generate G-GBMS-CDRs after changes in 2 container:

gtpp mbms buckets 2
gtp mbms interval

Configures the interval duration for interval-based triggers for GTPP MBMS Charging Data Record (G-MBMS-CDR) generation.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration
c

configure > context context_name > gtp group group_name
c

Entering the above command sequence results in the following prompt:
c

{context_name}host_name(config-gtpp-group)#
c

Syntax Description

gtp mbms interval duration_sec
c

no gtp mbms interval
c

c

no

c
c

Disables the interval-based trigger for G-MBMS-CDR generation for MBMs user service data.

duration_sec

c
c

Specifies the normal time duration (in seconds) that must elapse before closing an accounting record provided that any or all of the following conditions occur:

c

• Downlink traffic volume is reached within the time interval
• Tariff time based trigger occurred within the time interval
• Data volume (up and downlink) bucket trigger occurred within the time interval

duration_sec is an integer from 60 through 40,000,000. Default: Disabled

Usage Guidelines

Use this command to configure the G-MBMS-CDR generation triggers for MBMS user data service.

Examples

The following command configures the interval-based trigger to generate G-MBMS-CDRs in every 60 seconds:

gtp mbms interval 60
gtpp mbms tariff

Configures the tariff slots for tariff-based triggers for GTPP MBMS Charging Data Record (G-MBMS-CDR) generation.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration
configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp mbms tariff time1 mins hours | time2 mins hours | time3 mins hours | time4 mins hours |

no gtpp mbms tariff

no

Disables the tariff-based triggers for GTPP MBMS Charging Data Record (G-MBMS-CDR) generation.

tariff time1 mins hours | time2 mins hours | time3 mins hours | time4 mins hours |

Specifies time-of-day time values to close the current statistics container (but not necessarily the accounting record). Default: Disabled

Important

The system assumes that the billing system uses the day/date to determine if the statistics container represents an actual tariff period.

For each of the different tariff times, the following parameters must be configured:

- mins: Minute of the hour, an integer from 0 through 59.
- hours: Hour of the day, an integer from 0 through 23.

Usage Guidelines

Use this command to configure the tariff-time-based triggers for G-MBMS-CDR generation in MBMS user data service.
Examples

The following command configures the tariff-time-based trigger to generate G-MBMS-CDRs every day at 11 hours and 30 min:

gtp mbms tariff timel 30 11
**gtpp mbms volume**

Configures the download traffic data volume based trigger for GTPP MBMS Charging Data Record (G-MBMS-CDR) generation.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

- `gtpp mbms volume download_bytes`
- `no gtpp mbms volume`

- **no**
  
  Disables the configured download traffic data volume based trigger for G-MBMS-CDR generation for MBMS user service data.

- **volume download_bytes**
  
  Specifies the threshold of downlink data volumes that (in bytes) must be met before a G-MBMS-CDR should be closed as an integer from 100000 through 4000000000. Default: Disabled

**Usage Guidelines**

Use this command to configure the traffic data volume (download) based G-MBMS-CDR generation triggers for MBMS user data service.

**Examples**

The following command configures the traffic data volume (download) limit to trigger to generate G-MBMS-CDRs after reaching 150,000 octets:

```
gtpp mbms volume download_bytes
```
**gtpp redirection-allowed**

Configures the system to allow/disallow the redirection of CDRs when the primary CGF is unavailable.

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

**Privilege**
- Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

```plaintext
configure > context context_name > gtpp group group_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```plaintext
| default | no | gtpp redirection-allowed
```

**default**
Resets the system to allow redirection of CDRs.

**no**
Removes the redirection definition 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, the system 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.
The following command configures the system to allow the redirection of CDRs when the primary CGF is unavailable:

```
default gtpp redirection-allowed
```
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 in GTPP server group that the system is to communicate with.

**Product**

- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

- `gtpp server ip_address | max msgs | [ priority priority ] | [ udp-port port ] | [ node-alive { enable | disable } ] | [ -noconfirm ]`
- `no gtpp server ip_address | udp-port port`

`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 msgs`

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.

`msgs` can be configured to an integer from 1 to 256. Default: 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.

**Important**

---

### priority priority

Default: 1000

Specifies the relative priority of this CGF as an integer from 1 through 1000. When multiple CGFs are configured, the priority is used to determine which CGF server to send accounting data to. 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.

### udp-port port

Specifies the UDP port over which the GGSN communicates with the CGF. as an integer from 1 through 65535. Default: 3386

### node-alive { enable | disable }

Enable or disables GGSN sending Node Alive Request to a GTPP Server (such as CGF). This configuration can be done per GTPP Server. Default: Disable.

### `-noconfirm`

Executes this 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 subject to the following limits:

- Up to 4 CGFs can be configured in one GTPP server group
- Total of 32 CGFs can be configured per 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.
```
gtp server 192.168.2.2 priority 5
```

The following command deletes a previously configured CGF with an IP address of 100.10.35.7:
```
no gtp server 100.10.35.7
```
gtpp source-port-validation

Configures whether the system validates the UDP source port in received GTPP messages.

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

**Privilege**
Security Administrator, Administrator

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

configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
<table>
<thead>
<tr>
<th>default</th>
<th>no</th>
<th>gtpp source-port-validation</th>
</tr>
</thead>
</table>

**default**
Restores this parameter to its default setting of enabled.

**no**
Validates the IP source address but not the UDP source port.

**Usage Guidelines**
This command configures whether the system validates the UDP source port in received GTPP messages.

**Examples**
The following command disables UDP port validation:

```
no gtpp source-port-validation
```
gtpp storage-server

Configures information for the GTPP back-up storage server.

Product
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

Privilege
Security Administrator, Administrator

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

configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

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

Syntax Description
[no] gtpp storage-server ip_address port port_num

no
Removes a previously configured back-up storage server.

ip_address
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 GGSN communicates with the back-up storage server. Default: 3386

Usage Guidelines
This command identifies the connection to the GSS. One backup storage server can be configured per GTPP group.

Examples
The following command configures a GSS 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.

<table>
<thead>
<tr>
<th>Product</th>
<th>GGSN</th>
<th>IPSG</th>
<th>PDG/TTG</th>
<th>P-GW</th>
<th>SAEGW</th>
<th>SGSN</th>
<th>S-GW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

```
configure > context context_name > gtppgroup group_name
```

Entering the above command sequence results in the following prompt:

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

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 name_pattern | purge-interval purge_interval | push { encrypted-url encrypted_url | url url | encrypted-secondary-url encrypted_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 } | rotation { cdr-count | time-interval | volume } start-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
```

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.

format custom1 .. 8
Configures the file format to be used to format files to be stored locally.

  custom1 — File format custom1 - this is the default file format.

  custom2 to custom5 Customer specific CDR file formats.

  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.u format for file naming

      where:

      • date is date in MMDDYYYY (01312010) for mat
      • time is time in HHMMSS (023508) format
      • fixed-length-seq-num is the fixed length of the sequence number for s specific file having a 6-digit

        counter starting from 000001 and ending at 999999. When file sequence reaches 999999, the sequence

        is reset to 000001.

name format string
Allows the format of the CDR filenames to be configured independently so that the name format contains the
file name with conversion specifications.

  string —is an alphanumeric string of 1 through 127 characters. It 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
      • %% = This field is used to add % to the CDR file name.

      • 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 file name format). In which case the CDR filenames are generated based on the file format as before (maintains backward compatibility).

**name prefix prefix**

Defines the prefix to be used for the file name. By default the file name prefix would be "GTPP-group-name + VPN-ID". It is possible to have a NULL value prefix where the system would enter a default, which would be `group+vpn`.

`prefix` — is an alphanumeric string of 1 through 64 characters, Do not enter a value (NULL).

**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:*.*".

---

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:*.*: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
When a file transfer to primary fails four times, the transfer of files will automatically be failed over to the secondary server. The transfer will switch back to the original primary after 30 minutes, or if there are four transfer failures to the secondary server.

**via-local-context**: Pushes the CDR files via SPIO in the local context.
Default: Pushes via the group's context.

**Important**
If the push is done through gtpp context, then the push rate is lesser compared to via local context as the HDD is attached to the local context.

```
rotation { cdr-count count | time-interval time | force-rotation | volume 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 for file rotation (in seconds) as an integer from 30 through 86400. Default: 3600 (1 hour).
- **force-file-rotation**: Forces CDR file-rotation at a specified interval configured via the **time-interval** keyword, even if no CDRs were generated. By default this keyword is Disabled.
- **volume size**: Configures the file volume (in megabytes) for file rotation as an integer from 2 through 40. This trigger can not be disabled. Default: 10

```
start-file-seq-num seq_num [ recover-file-seq-num ]
```

Default: disabled

Enables the continuous file sequence number function. **start-file-seq-num** specifies the lowest number to be used as a file sequence number in the case of an aaaproxy or a chassis restart/reboot.

`seq_num` is an integer from 1 to 4294967295. Entering a value of 1 disables the recover file sequence number function. Entering any other number, for example 10, would instruct the system to always start from 10 as the file sequence number in the event of an aaaproxy or chassis reload.

When files are moved, the file sequence numbers are synced and stored in both RAM and the hard disk drive (HDD). **recover-file-seq-num** instructs the system to recover the last (largest) stored file sequence number, in the event of an aaaproxy/chassis restart/reboot, to continue file sequence numbering rather than resetting the file sequence numbering to the lowest start file sequence number.

**Usage Guidelines**
This command configures the parameters for storage of GTPP packets as files on the local server - meaning the hard disk drive (HDD).

**Examples**
The following command configures rotation for every 1.5 hours for locally stored files.

```
gtpp storage-server local file rotation time-interval 5400
```
Configuring file name format along with max-file-seq-no:
```
gtpp storage-server local file name format processed_2g_%Y%m%d_%5Q_%N.cdr max-file-seq-no 2345
```

Configuring file name prefix with a NULL value:
```
gtpp storage-server local file name prefix NULL
```

Configure the file name pattern and purge interval to setup file purging from the HDD:
```
gtpp storage-server local file purge-processed-files file-name-pattern *.z purge-interval 4
```
**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
- SGSN
- S-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration
  - configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
| default | gtpp storage-server max-retries max_attempts
```

- **default**
  Restores the system to the default value of 2 retry attempts.

- **max_attempts**
  Specifies the number of times the system attempts to communicate with a GTPP back-up storage server that is not responding as an integer from 1 to 15. Default: 2

**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 retries. Refer to the description of this command for additional information.

**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 the storage mode (local, remote or streaming for CDRs) to be used. Local storage mode is available with ASR 5000 platforms only.

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

**Privilege**
- Security Administrator, Administrator

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

```
configure > context context_name > gtpp group group_name
```

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

**Syntax Description**
- `gtpp storage-server mode { local | remote | streaming [ parallel ] }`
- `default gtpp storage-server mode`

**default**

Returns the GTPP group configuration to the default "remote" value for the GTPP storage server mode.

**local**

Specifies the use of the hard disk for storing CDRs. Default: Disabled

**Important**

This option is available with ASR 5000 platforms only.

**remote**

Specifies the use of an external server for storing CDRs. This is the default value.
When the external server is down, the Session Managers will start buffering up to a maximum of 26400 CDRs or a total of 120 MB worth of CDRs, whichever limit reaches first. The maximum CDR limit specified is per the session manager. The chassis level limit varies depending on the number of session manager instances and number of active cards.

**Important**

streaming [ parallel ]

Specifies the use of HDD to store CDRs in case if CGF fails and then stream the CDRs to the CGF when CGF is up. Streaming can be done in a First-In-First-Out (FIFO) or parallel mode. Default: streaming (FIFO)

**streaming:** This keyword 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.

In the streaming mode, when the CGF becomes active, CDRs in HDD are streamed in a First-In-First-Out order. In this mode, newly generated CDRs are routed to CGF via HDD.

**parallel:** In this mode, when the CGF becomes active, CDRs in HDD are streamed at slower pace. Newly generated CDRs are sent directly to CGF servers along with CDRs streamed from HDD.

In PARALLEL mode, rate of streaming from HDD will be slow. The maximum requests that can be streamed from HDD will be either set to 1 or 25% of the available bandwidth (i.e. max outstanding - outstanding req) if it is greater than 1. It is expected that the billing domain should be capable of handling Out-Of-Order CDRs in parallel streaming mode.

**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.

```plaintext
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
- SGSN
- S-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
| default | gtpp storage-server timeout duration
```

**default**

Restores the timeout duration to the default of 30 seconds.

**duration**

Specifies the maximum amount of time (in seconds) that 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. Default: 30

**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

Suppresses the CDRs with zero byte data count, so that the OCG node is not overloaded with a flood of CDRs. By default this mode is "disabled".

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.

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

| Privilege      | Security Administrator, Administrator |

| Command Modes | Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration |

| Syntax Description |

```
gtpp suppress-cdrs zero-volume { final-cdr | internal-trigger-cdr | external-trigger-cdr } +
{ default | no } gtpp suppress-cdrs zero-volume

default | no
Disables the CDR suppression mode. By default this command is disabled and system will not suppress any CDR.

final-cdr
Suppresses only the Final Zero Volume CDRs i.e. the CDRs that are generated when the session ends.

internal-trigger-cdr
Suppresses Zero Volume interim CDRs that are generated due to internal triggers such as volume limit, time limit, tariff change or user generated interims through the CLI commands.```
**external-trigger-cdr**

Supresses Zero Volume interim CDRs that are generated due to external triggers such as QoS Change, RAT change and so on.

**Usage Guidelines**

Use this command to suppress the CDRs (G-CDRs, eG-CDR, PGW-CDRs, SGW-CDRs, SGSN CDRs) with zero-volume session due to any reason.

This feature allows the customers to suppress the CDRs with zero byte data count, so that the OCG node is not overloaded with a flood of CDRs.

The CDRs can be categorized as follows:

- **final-cdr**: These CDRs are generated when the session ends.
- **internal-trigger-cdr**: These CDRs are generated due to internal triggers such as volume limit, time limit, tariff change or user generated interims through the CLI commands.
- **external-trigger-cdr**: These CDRs are generated due to external triggers such as QoS Change, RAT change and so on. All triggers which are not considered as final-cdrs or internal-trigger-cdrs are considered as external-trigger-cdrs.

Customers can select the CDRs they want to suppress. This feature is disabled by default to ensure backward compatibility.

**Examples**

The following command configures the system to suppress Zero Volume Final CDRs, interim CDRs due to internal and external triggers:

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

Suppresses the CDRs created by session having zero duration and/or zero volume. By default this mode is "disabled".

Product

GGSN
P-GW
SAEGW
S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp suppress-cdrs zero-volume-and-duration { gcdrs [ egcdrs ] | egcdrs [ gcdrs ] }
default gtpp suppress-cdrs zero-volume-and-duration

default

Disables the CDR suppression mode.

gcdrs [ egcdrs ]

Specifies that this command will handle G-CDRs before eG-CDR/P-CDRs.

gcdrs [ egcdrs ]

Specifies that this command will handle eG-CDR/P-CDRs before G-CDRs.

Usage Guidelines

Use this command to suppress the CDRs (G-CDRs and eG-CDR/P-CDRs) which were created due with zero-duration session and zero-volume session due to any reason. By default this command is disabled and system will not suppress any CDR.
Examples

The following command configures the system to suppress the eG-CDR/P-CDRs created for a zero duration session or zero volume session:

gtp 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 CGF.

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

**Privilege**
Security Administrator, Administrator

**Command Modes**
`Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration`
`configure > context context_name > gtpp group group_name`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
| default | gtpp timeout time |
```

**default**

Resets the systems GTPP timeout value to 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. Default: 20

**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 transport-layer

Selects the transport layer protocol for Ga interface for communication between AGW (GSNs) and GTPP servers.

Product
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration
configure > context context_name > gtpp group group_name

Syntax Description
- gtpp transport-layer { tcp | udp }
- default gtpp transport-layer

  default
  Resets the transport layer protocol to GTPP servers to the default of UDP.

  tcp
  Enables the system to implement TCP as transport layer protocol for communication with GTPP server. Default: Disabled

  udp
  Enables the system to implement UDP as transport layer protocol for communication with GTPP server. Default: Enabled

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).
Examples

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

```
gtp transport-layer tcp
```
**gtpp trigger**

Disables GTPP trigger conditions that cause either partial CDR record closure or opening of a new CDR record container. GTPP Triggers are specified in 3GPP TS 32.251 v6.6.0. All GTPP trigger changes take effect immediately, except `volume-limit`.

**Product**
- ECS
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

    `configure > context context_name > gtpp group group_name`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
gtppp trigger { apn-ambr-change | default-bearer-only | all-non-gbr-bearers | all-bearers | cell-update | dcca | direct-tunnel | egdmax-losdv | ggsn-preservation-mode-change | inter-plmn-sgsn-change | ms-timezone-change | plmn-id-change | qos-change | rat-change | generate { cdr | container } } | routing-area-update | service-idle-out | serving-node-change-limit | sgsn-change-limit | tariff-time-change | time-limit | uli-change | volume-limit }

default gtpp trigger


default

Sets the specified trigger condition back to the default setting. All trigger conditions are enabled by default.

no

Disables the specified trigger condition.
apn-ambr-change [ default-bearer-only | all-non-gbr-bearers | all-bearers ]

Default: Disabled

Enables APN AMBR trigger only for default-bearer or for all bearers for that PDN or selectively for apn-non-gbr bearers.

Important
This keyword option will be available only if a valid license is installed. For more information, contact your Cisco account representative.

The APN Aggregate Maximum Bit Rate (AMBR) is a subscription parameter stored per APN. It limits the aggregate bit rate that can be expected to be provided across all non-GBR bearers and across all PDN connections of the same APN. Each of these non-GBR bearers potentially utilize the entire APN AMBR, e.g. when the other non-GBR bearers do not carry any traffic.

In 15.0 and later releases, this CLI command should be configured along with the following additional options to enable APN-AMBR trigger for SGW-CDRs in all GTPP dictionaries.

- default-bearer-only: Adds container only to default bearer.
- all-non-gbr-bearers: Adds container to all non-gbr-bearers.
- all-bearers: Adds containers for all bearers.

Important
This CLI command and the associated options are not available for products other than S-GW and P-GW.

The first container of each CDR includes apn-ambr fields along with QoS. In the following containers this field is present if previous change condition is "QoS change" or "APN AMBR Change".

cell-update
Enables the cell update trigger for S-CDRs, if the dictionary specified in the gtpp dictionary configuration includes support for cell update. This trigger is available only for 2G. Currently, custom18 dictionary supports the cell update trigger.

dcca
This keyword enables or disables the addition of LOSDV in PGW-CDR for the following DCCA generated triggers.

- Time Threshold Reached
- Volume Threshold Reached
- Service Specific Unit Threshold Reached
- Time Exhausted
- Volume Exhausted
- Validity Timeout
- Reauthorization Request
- Continue Ongoing Session
- Retry And Terminate Ongoing Session
- Terminate Ongoing Session
- Service Specific Unit Exhausted
- Envelope Closure

**direct-tunnel**
Enables the direct tunnel trigger for CDRs.

**egcdr max-losdv**
Enables the trigger for an eG-CDR/P-CDR if the List of Service Data Volume (LoSDV) containers crosses the configured limit for LOSDV containers. Default: Disabled

**ggsn-preservation-mode-change**
This keyword is for GGSN only.
This trigger enables the preservation-mode-change trigger for G-CDR.

**inter-plmn-sgsn-change**
This keyword is for GGSN only.
Disabling this trigger ignores an Inter-PLMN SGSN change and doesn't release a G-CDR. Default: Enabled

**ms-timezone-change**
This keyword is specific to GGSN.
No partial record closure for a time zone change occurs when this trigger is disabled. MS time zone change should be applicable only for 3GPP R6 based GTPP dictionaries. Default: Enabled

**plmn-id-change**
This trigger keyword is specific to the 2G SGSN and is proprietary (non-standard).
Enables the PLMNID change trigger for S-CDRs if the dictionary specified in the **gtpp dictionary** configuration supports the PLMNID change. If enabled, the SGSN generates a partial S-CDR when the MS changes the PLMN while under the same SGSN (intra-system intra-SGSN PLMN-ID handover). Currently, custom18 dictionary supports this trigger. Default: Disabled

**qos-change**
Enables the QoS-change trigger for CDRs. Disabling this trigger ignores a QoS-change and does not open a new CDR for it. Default: Enabled
When QoS changes are observed, the system generates only containers. However when the max-container condition is reached, an interim CDR is generated.

**rat-change [ generate { cdr | container } ]**
Enables or disables the partial record closure for a RAT change. If disabled, no partial record closure for a RAT change occurs. RAT change should be applicable only for 3GPP R6 based GTPP dictionaries. Default: Enabled
In SGSN, RAT change trigger (2G<->3G) means inter-service handoff (SGSN service <-> GPRS service). If this trigger is enabled, after the RAT change interim CDR is generated. After this RAT change CDR, CDR thresholds such as volume/time etc. and GTPP Group are applicable from new service. If RAT change trigger is disabled, the CDR thresholds and GTPP group etc. will not change and will continue to use from old service.

After the RAT change, the System Type field in CDR changes to indicate the new system type. If this trigger is disabled, then the next CDR generated will indicate System Type, but the data count in the CDR does not necessarily belong to the system type indicated in CDR; instead, it may belong to both 2G and 3G as CDR is not closing when handover takes place.

Important: The System Type field in CDR-related change is not applicable to customized CDR formats, which does not use the System Type field.

generate { cdr | container }: Sets generation of CDR or just a Container on a RAT change.

cdr: Generates a CDR on a RAT-change.

container: Generates a container only on a RAT-change.

routing-area-update
Enables the routing-area-update trigger for CDRs.

service-idle-out
This keyword enables or disables the addition of LOSDV in PGW-CDR when a service idles out. Note that the CDR module receives service idle out trigger from DCCA module when the quota hold timer expires, or from ACS manager when rulebase has a service idle out configuration.

serving-node-change-limit [ also-intra-sgsn-multiple-address-group-change ]
This keyword is enabled for P-GW, S-GW, and GGSN. However, the also-intra-sgsn-multiple-address-group-change is enabled only for GGSN. Default: Enabled
Disabling this trigger ignores an SGSN change and does not add the SGSN IP address into the SGSN address list of the CDR. This helps to reduce the release of CDRs due to SGSN changes crossing the configured limit.
also-intra-sgsn-multiple-address-group-change: This keyword includes Intra-SGSN group changes as an SGSN change.

sgsn-change-limit [ also-intra-sgsn-multiple-address-group-change ]
This keyword is obsolete and is available to maintain the backward compatibility for existing customers. The new keyword for sgsn-change-limit is serving-node-change-limit. Default: Enabled
Disabling this trigger ignores an SGSN change and does not add the SGSN IP address into the SGSN address list of the CDR. This helps to reduce the release of CDRs due to SGSN changes crossing the configured limit.
also-intra-sgsn-multiple-address-group-change: This keyword includes Intra-SGSN group changes as an SGSN change.

tariff-time-change
When this trigger is disabled, container closure does not happen for a tariff-time change. Default: Enabled
This trigger is applicable for G-MB-CDRs for MBMS session too.
**time-limit**
When this trigger is disabled, no partial record closure occurs when the configured time limit is reached. Default: Enabled
This trigger is applicable for G-MB-CDRs for MBMS session too.

**uli-change**
Enables the user location update trigger for eG-CDRs/PGW-CDRs/SGW-CDRs, if the dictionary specified in the GTPP dictionary configuration includes support for user location update trigger. Default: Enabled

**volume-limit**
When this trigger is disabled no partial record closure occurs when volume limit is reached. Default: Enabled
This trigger is applicable for G-MB-CDRs for MBMS session too.

**Usage Guidelines**
Use this command to disable or enable GTTP triggers that can cause partial CDR record closure or cause a new CDR to be created.

**Examples**
The following command disables partial record closure when a configured time limit is reached:
```plaintext
gtp trigger time-limit
```
The following command re-enables partial record closure when a configured time limit is reached:
```plaintext
no gtp trigger time-limit
```
GTP-U Service Configuration Mode Commands

The GTP-U Service Configuration Mode is used to manage parameters applied to incoming GTP-U packets.

**Command Modes**

Exec > Global Configuration > Context Configuration > GTP-U Service Configuration

`configure > context context_name > gtpu-service service_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-gtpu-service)#`

**Important**

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

- bind, page 1219
- echo-interval, page 1221
- echo-retransmission-timeout, page 1223
- end, page 1225
- exit, page 1226
- extension-header, page 1227
- ip qos-dscp, page 1228
- ipsec-allow-error-ind-in-clear, page 1231
- ipsec-tunnel-idle-timeout, page 1232
- max-retransmissions, page 1233
- path-failure clear-trap, page 1234
- path-failure detection-policy, page 1236
- retransmission-timeout, page 1238
- sequence-number, page 1240
- source-port, page 1241
- udp-checksum, page 1243
**bind**

Configures the IP address to use for GTP-U data packets.

**Product**
- ePDG
- GGSN
- P-GW
- SAEGW
- SaMOG
- SGSN
- S-GW

**Privilege**
Administrator

**Command Modes**
```
Exec > Global Configuration > Context Configuration > GTP-U Service Configuration
```
```
configure > context context_name > gtpu-service service_name
```

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

**Syntax Description**
```
[ no ] bind { ipv4-address ipv4_address | crypto-template crypto_template | [ ike-bind-address { ipv4-address } | [ ipv6-address ipv6_address | bearer-type { non-ims-media | ims-media | all } ] | [ ipv6-address ipv6_address | crypto-template crypto_template | [ ike-bind-address { ipv6-address } | [ ipv4-address ipv4_address | [ bearer-type { non-ims-media | ims-media | all } ] ]
```

- **no**
  Removes a configured IP address from this service.

- **ipv4-address ipv4_address**
  Binds this service to the IPv4 address of a configured interface.
  `ipv4_address` must be entered using IPv4 dotted-decimal notation.

- **bearer-type non-ims-media | ims-media | all**
  Specifies the type of bearer to be associated with the bind address. Default behavior is for that the address will be used for all bearer types.
  **non-ims-media** Configures bind address for non-ims media only.
**ims-media** Configures bind address for ims-media traffic only.
**all** configures bind address to handle all types of bearer traffic. This is the default setting.

**ipv6-address ipv6_address**
Binds this service to the IPv6 address of a configured interface.
*ipv6_address* must be entered using IPv6 colon-separated-hexadecimal notation.

**crypto-template crypto_template**
Configures crypto template for IPSec, which enables IPSec tunneling for this GTP-U address. Must be followed by the name of an existing crypto template.
*crypto_template* must be an alphanumeric string of 1 through 127 characters.

**ike-bind-address ip_address**
Configures an IKE bind address. Must be followed by IPv4 or IPv6 address; IP address type must be the same as the GTP-U address type.
*ipv4_address* must be entered using IPv4 dotted-decimal notation.
*ipv6_address* must be entered using IPv6 colon-separated-hexadecimal notation.

**bearer-type non-ims-media | ims-media | all**
Specifies the type of bearer to be associated with the bind address. Default behavior is for that the address will be used for all bearer types.

*non-ims-media* configures bind address for non-ims media only.
*ims-media* configures bind address for ims-media traffic only.
*all* configures bind address to handle all types of bearer traffic. This is the default setting.

---

**Usage Guidelines**

Use this command to bind the service to an interface for sending/receiving GTP-U packets.

---

**Important**

A GTP-U service can support a maximum of 12 GTP-U endpoints/interfaces.

---

**Examples**

The following command configures the IPv4 address for this GTP-U service as 10.2.3.4:

```
bind ipv4-address 10.2.3.4
```
echo-interval

Configures the rate at which GPRS Tunneling Protocol (GTP) v1-U echo packets are sent.

**Product**
- ePDG
- GGSN
- P-GW
- SAEGW
- SaMOG
- SGSN
- S-GW

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GTP-U Service Configuration

```bash
configure > context context_name > gtpu-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpu-service)#
```

**Syntax Description**

```bash
echo-interval seconds | dynamic | smooth-factor multiplier |
{ default | no } echo-interval
```

default
Disables the configured echo-interval setting.

no
Removes the configured echo-interval setting.

seconds
Specifies the number of seconds between the sending of a GTP-Uv1 echo packet. seconds must be an integer from 60 through 3600. Default: 60

dynamic | smooth-factor multiplier |
Enables the dynamic echo timer for the GTP-U service.
smooth-factor multiplier: Introduces a multiplier into the dynamic echo timer as an integer from 1 through 5. Default: 2

Usage Guidelines
Use this command to configure the rate at which GTP-Uv1 echo packets are sent.

Examples
The following command sets the rate between the sending of echo packets at 120 seconds:

```plaintext
echo-interval 120
```
echo-retransmission-timeout

Configures the timeout for GTP-U echo message retransmissions for this service.

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

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GTP-U Service Configuration
`configure > context context_name > gtpu-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpu-service)#
```

**Syntax Description**
`echo-retransmission-timeout seconds`
`default echo-retransmission-timeout`

`default`
Returns the command to its default setting of 5.

`seconds`
Default: 5
Configures the echo retransmission timeout, in seconds, for the GTP-U service as an integer ranging from 1 to 20.

**Usage Guidelines**
Use this command to configure the amount of time, in seconds, before the GTP-U service transmits another echo request message. The value set in this command is used, as is, for the default echo. If dynamic echo is enabled (`echo-interval dynamic`) the value set in this command serves as the dynamic minimum (if the RTT multiplied by the smooth factor is less than the value set in this command, the service uses this value).
The following command sets the retransmission timeout for echo messages to 2 seconds:

```
echo-retransmission-timeout 2
```
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.
extension-header

Configures the addition of an extension header in the GTP-U packet header, allowing for error indication messages.

Product
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

Privilege
Administrator

Command Modes
- Exec > Global Configuration > Context Configuration > GTP-U Service Configuration
- configure > context context_name > gtpu-service service_name

Entering the above command sequence results in the following prompt:

([context_name]host_name(config-gtpu-service)#

Syntax Description
[ default | no ] extension-header source-udp-port

default
Returns the command to its default setting of disabled.

no
Disables the feature.

source-udp-port
Configures extension header type UDP Port support in GTP-U header for GTP-U Error Indication messages.

Usage Guidelines
Use this command to configure the addition of an extension header in the GTP-U packet to allow for error indication messages.

Examples
The following command enables the inclusion of an extension header to allow for error indication messages:

extension-header source-udp-port
ip qos-dscp

Configures the quality of service (QoS) differentiated service code point (DSCP) per-hop behavior (PHB) to be marked on the outer header of signalling packets originating from the LTE component.

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

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GTP-U Service Configuration

`configure > context context_name > gtpu-service service_name`

Entering the above command sequence results in the following prompt:

```
/context_name/host_name(config-gtpu-service)#
```

**Syntax Description**

```
ip qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }
| default | no | ip qos-dscp
```

**default**
Sets/restores default value.

**no**
Disables DSCP marking.

```
af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef
```

Specifies the IP QoS DSCP PHB to be marked on the outer header of signalling packets originating from the LTE component. This is a standards-based feature (RFC 2597 and RFC 2474).

Note that CS (class selector) mode options below are provided to support backward compatibility with the IP precedence field used by some network devices. CS maps one-to-one to IP precedence, where CS1 is IP precedence value 1. If a packet is received from a non-DSCP aware router that used IP precedence markings, then the DSCP router can still understand the encoding as a Class Selector code point.

The following forwarding types are supported:
• **af11**: Designates the use of Assured Forwarding 11 PHB. This is the default setting.
• **af12**: Designates the use of Assured Forwarding 12 PHB.
• **af13**: Designates the use of Assured Forwarding 13 PHB.
• **af21**: Designates the use of Assured Forwarding 21 PHB.
• **af22**: Designates the use of Assured Forwarding 22 PHB.
• **af23**: Designates the use of Assured Forwarding 23 PHB.
• **af31**: Designates the use of Assured Forwarding 31 PHB.
• **af32**: Designates the use of Assured Forwarding 32 PHB.
• **af33**: Designates the use of Assured Forwarding 33 PHB.
• **af41**: Designates the use of Assured Forwarding 41 PHB.
• **af42**: Designates the use of Assured Forwarding 42 PHB.
• **af43**: Designates the use of Assured Forwarding 43 PHB.
• **be**: Designates the use of Best Effort forwarding PHB.
• **cs1**: Designates the use of Class Selector code point "CS1".
• **cs2**: Designates the use of Class Selector code point "CS2".
• **cs3**: Designates the use of Class Selector code point "CS3".
• **cs4**: Designates the use of Class Selector code point "CS4".
• **cs5**: Designates the use of Class Selector code point "CS5".
• **cs6**: Designates the use of Class Selector code point "CS6".
• **cs7**: Designates the use of Class Selector code point "CS7".
• **ef**: Designates the use of Expedited Forwarding PHB typically dedicated to low-loss, low-latency traffic.

The assured forwarding behavior groups are listed in the table below.

<table>
<thead>
<tr>
<th>Class</th>
<th>Class 1</th>
<th>Class 2</th>
<th>Class 3</th>
<th>Class 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low Drop</td>
<td>AF11</td>
<td>AF21</td>
<td>AF31</td>
<td>AF41</td>
</tr>
<tr>
<td>Medium Drop</td>
<td>AF12</td>
<td>AF22</td>
<td>AF32</td>
<td>AF42</td>
</tr>
<tr>
<td>High Drop</td>
<td>AF13</td>
<td>AF23</td>
<td>AF33</td>
<td>AF43</td>
</tr>
</tbody>
</table>

Traffic marked with a higher class is given priority during congestion periods. If congestion occurs to traffic with the same class, the packets with the higher AF value are dropped first.

**Usage Guidelines**  
Use this command to implement DSCP marking only for GTP-U ECHO Request and Response messages.
Examples

Use the following command to set the use of Best Effort forwarding PHB:

```
ip qos-dscp be
```
ipsec-allow-error-ind-in-clear

Configures whether error-indication is dropped or sent without IPSec tunnel.

**Product**

S-GW
SAEGW
SGSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GTP-U Service Configuration

```
configure > context context_name > gtpu-service service_name
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-gtpu-service)#
```

**Syntax Description**

```
[ default | no ] ipsec-allow-error-ind-in-clear
```

**default**

Error-indication is dropped if no IPSec tunnel is present for that peer.

**no**

Disables the feature.

**Usage Guidelines**

Use this command to determine whether error-indication is dropped or sent without an IPSec tunnel.

On receiving data packets for a session that does not exist, error-indication needs to be sent back to the peer. If there is no IPSec tunnel present with that peer, error-indication may be either dropped or sent without any IPSec tunnel.

**Examples**

The following command allows error-indication to be sent without any IPSec tunnel:

```
ipsec-allow-error-ind-in-clear
```
ipsec-tunnel-idle-timeout

Configures the IPSec tunnel idle timeout after which IPSec tunnel deletion is triggered.

Product
- S-GW
- SAEGW
- SGSN

Privilege
Administrator

Command Modes
- Exec
- Global Configuration
- Context Configuration
- GTP-U Service Configuration

configure > context context_name > gtpu-service service_name

Entering the above command sequence results in the following prompt:

(context_name)host_name(config-gtpu-service)#

Syntax Description
- ipsec-tunnel-idle-timeout seconds
- default ipsec-tunnel-idle-timeout

seconds
Default: 60
Specifies the number of seconds an IPSec tunnel is idle before tunnel deletion is triggered. seconds must be an integer from 10 through 600.

default
Returns the command to its default setting of 60.

Usage Guidelines
When there are no bearers on a particular IPSec tunnel, GTPUMGR initiates the delete for that tunnel. This timer helps to avoid unnecessary IPSec tunnel deletions for an idle tunnel.

Examples
The following command sets the IPsec tunnel idle timeout to 100 seconds:

ipsec-tunnel-idle-timeout 100
**max-retransmissions**

Configures the maximum retry limit for GTP-U echo retransmissions.

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

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GTP-U Service Configuration

```
configure > context context_name > gtpu-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpu-service)#
```

**Syntax Description**

```
max-retransmissions num
no max-retransmissions
```

**num**
- Default: 4
- Specifies the number of GTP-U echo message retransmissions allowed before triggering a path failure error condition. `num` must be an integer from 0 through 15.

**no**
- Disables the feature.

**Usage Guidelines**
Use this command to set the maximum number of GTP-U echo message retransmissions in order to define a limit that triggers a path failure error.

**Examples**
The following command sets the maximum GTP-U echo message retransmissions for this service to 10:

```
max-retransmissions 10
```
### path-failure clear-trap

Configures a trigger for clearing the path failure trap.

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

**Privilege**
Administrator

**Command Modes**

```
Exec > Global Configuration > Context Configuration > GTP-U Service Configuration
```

```
configure > context context_name > gtpu-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name (config-gtpu-service) #
```

**Syntax Description**

```
path-failure clear-trap gtp echo
[ default | no ] path-failure clear-trap
```

**gtp echo**

Sets the clearing trigger/trap to detect a failure upon reaching the maximum number of GTP-U echo message retransmissions.

**default**

Resets the command to its default setting of enabled.

**no**

Disables the feature.

**Usage Guidelines**

Use this command to set the detection policy for path failures. By default, path failure trap is cleared on receiving first control plane message for that GTP-U peer allocation.
Examples

The following command sets the clearing trigger to detect failures upon reaching the maximum number of GTP-U echo message retries:

`path-failure clear-trap gtp echo`
path-failure detection-policy

Configures a path failure detection policy on GTP-U echo messages that have been retransmitted the maximum number of retry times.

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

**Privilege**
Administrator

**Command Modes**

```
Exec > Global Configuration > Context Configuration > GTP-U Service Configuration
```
```
configure > context context_name > gtpu-service service_name
```

Entering the above command sequence results in the following prompt:
```
<context_name> host_name (config-gtpu-service) #
```

**Syntax Description**

```
path-failure detection-policy gtp echo
[ default | no ] path-failure detection-policy
```

**gtp echo**
Sets the detection policy to detect a failure upon reaching the maximum number of GTP-U echo message retransmissions.

**default**
Resets the command to its default setting of enabled.

**no**
Disables the feature.

**Usage Guidelines**
Use this command to set the detection policy for path failures.
Examples

The following command sets the path failure detection policy to detect failures upon reaching the maximum number of GTP-U echo message retries:

```
path-failure detection-policy gtp echo
```
retransmission-timeout

Configures retransmission timeout for GTPU echo message retransmissions for this service.

**Important**

In release 14.0 and later versions, this command is replaced by the `echo-retransmission-timeout` command.

**Product**

- ePDG
- GGSN
- P-GW
- SAEGW
- S-GW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > GTP-U Service Configuration

```plaintext
configure > context context_name > gtpu-service service_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-gtpu-service)#
```

**Syntax Description**

- `retransmission-timeout seconds`
- `default retransmission-timeout`

**Syntax Description**

- `default`
  
  Returns the command to its default setting of 5.

- `seconds`
  
  Default: 5
  
  Specifies the number of seconds between the re-sending of GTP-U echo messages. `seconds` must be an integer from 1 through 20.

**Usage Guidelines**

Use this command to set the number of seconds between the retransmission of GTP-U echo messages.
Examples

The following command sets the number of seconds between the sending of GTP-U echo messages to 7:

```
retransmission-timeout 7
```
**sequence-number**

Enables addition of the sequence number to every GTP-U packet. Default is disabled.

**Product**

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

**Privilege**

Administrator

**Command Modes**

- Exec > Global Configuration > Context Configuration > GTP-U Service Configuration
- configure > context context_name > gtpu-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpu-service)#
```

**Syntax Description**

| no | sequence-number |

**Usage Guidelines**

Use this command to enable/disable addition of the sequence number to every GTP-U packet coming from Gi interface and going towards Gn/Gp interface. If GTP-U packets are received out of sequence, sequence numbers would allow the packets to be reorded.

**Examples**

The following command enables addition of the sequence number to every GTP-U packet:

```
sequence-number
```
source-port

Configures GTP-U data packet source port related parameters.

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

**Privilege**
Administrator

**Command Modes**

```
Exec > Global Configuration > Context Configuration > GTP-U Service Configuration
```

```
configure > context context_name > gtpu-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpu-service)#
```

**Syntax Description**

```
source-port { non-standard | standard }
default source-port
```

- **default**
  Configures GTP-U service to use standard port 2152 as source port for all GTP-U data packets.
  By default, standard port 2152 will be configured as GTP-U data packet source port (same as existing behavior).

- **non-standard**
  Configures GTP-U service to use multiple non-standard ports defined by system as a source port for GTP-U data packets. Starting port is 25500. Non-standard port number is unique per session manager instance.

- **standard**
  Configures GTP-U service to use standard port 2152 as source port for all GTP-U data packets.

**Usage Guidelines**
Currently, for forwarding GTP-U data packets, standard UDP port (2152) as source and destination port are used for outgoing GTP-U packet. This creates hardship to balance traffic properly over the LAG interfaces between the different L2/L3 elements in the network. Some routers use source UDP port to do load balancing of packets towards destination.
This command allows the source port outgoing GTP-U packet to be different for each SESSMGR. The destination port should remain as 2152, as per protocol.

**Examples**

The following command configures GTP-U service to use standard port 2152 as source port for all GTP-U data packets:

```
source-port standard
```
udp-checksum

Inserts UDP-checksum in the UDP header of GTP-U packet.

**Product**
- GGSN
- HNB-GW
- P-GW
- SGSN
- S-GW

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > GTP-U Service Configuration

```
configure > context context_name > gtpu-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpu-service)#
```

**Syntax Description**
```
udp-checksum { no-optimize | optimize }
[ default | no ] udp-checksum
```

**default**
Through releases 14.0: Enables the UDP checksum, but no optimization is attempted. Releases 15.0 and later: Enables the UDP checksum, and attempts optimization of the UDP checksum in UDP header of GTP-U packet using the inner payload transport checksum.

**no**
Outer UDP checksum is marked as 'ZERO,' effectively disabling UDP checksum. Applicable only for IPv4 data.

**no-optimize**
No optimization attempt over UDP checksum in UDP header of GTP-U packet.

**optimize**
Attempts optimization of UDP checksum in UDP header of GTP-U packet using inner payload transport checksum.
**Usage Guidelines**

This command is used for enabling optimization of UDP checksum in UDP header of the GTP-U packet. An option to completely disable the UDP checksum of GTP-U packet is also introduced.

**Examples**

The following command enables the optimization of UDP checksum in UDP header of the GTP-U packet:

```
udp-checksum optimize
```
HA Proxy DNS Configuration Mode Commands

**Important**

HA Proxy DNS Intercept is a license-enabled feature.

The HA Proxy DNS Configuration Mode is used to create rules for Home Agent (HA) proxy DNS intercept lists that redirect packets with unknown foreign DNS addresses to a home network DNS server.

**Command Modes**

Exec > Global Configuration > Context Configuration > Proxy DNS Configuration

configure > context context_name > proxy-dns intercept-list list_name

Entering the above command sequence results in the following prompt:

(context_name)host_name(config-proxy-dns-intercept-list)#

**Important**

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

- description, page 1246
- end, page 1247
- exit, page 1248
- pass-thru, page 1249
- redirect, page 1251
**description**

Allows you to enter descriptive text for this configuration.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

description *text*

no
description

*no*

Clears the description for this configuration.

*text*

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

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

**Usage Guidelines**

The description should provide useful information about this configuration.
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

end

Usage Guidelines

Use this command to return to the Exec mode.
exit

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

exit

**Usage Guidelines**

Use this command to return to the parent configuration mode.
pass-thru

Sets IP addresses that should be allowed through the proxy DNS intercept feature.

Product  
HA

Privilege  
Security Administrator, Administrator

Command Modes  
Exec > Global Configuration > Context Configuration > Proxy DNS Configuration  
configure > context context_name > proxy-dns intercept-list list_name

Entering the above command sequence results in the following prompt:

[context_name] host_name (config-proxy-dns-intercept-list) #

Syntax Description

[ no ] pass-thru { ipv4_address | ipv6_address } [ /ip_mask ]

no

Removes the DNS IP address from the pass-thru rule.

pass-thru ip_address [ /ip_mask ]

Specifies an DNS IP address that is allowed through the intercept feature.

ip_address [ /ip_mask ]: Specifies the IP address and network mask bits. ip_address [ /ip_mask ] is specified using IPv4 dotted decimal or IPv6 colon-separated-hexadecimal notation. The mask bits are a numeric value which is the number of bits in the subnet mask (CIDR notation).

Usage Guidelines

Use this command to identify DNS IP addresses that should be allowed through the intercept feature. For a more detailed explanation of the proxy DNS intercept feature, see the proxy-dns intercept-list command in the Context Configuration Mode Commands chapter. A maximum of 16 intercept rules (either redirect or pass-thru) are allow for each intercept list.

Important

To allow packets through that do not match either the pass-thru or redirect rules, set a pass-thru rule address as: 0.0.0.0/0. If a packet does not match either the pass-thru or redirect rule, the packet is dropped.
The following command allows a foreign network's DNS with an IP address of 10.2.55.12 to avoid being redirected:

```bash
pass-thru 10.2.55.12
```
**redirect**

Redirects DNS IP addresses from foreign networks matching an IP address in this command to a home network DNS.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Proxy DNS Configuration

```bash
configure > context context_name > proxy-dns intercept-list list_name
```

Entering the above command sequence results in the following prompt:

```bash
(context_name)host_name(config-proxy-dns-intercept-list)#
```

**Syntax Description**

```bash
redirect { ipv4_address | ipv6_address } [ primary-dns { ipv4_address | ipv6_address } + | [ secondary-dns { ipv4_address | ipv6_address } + ] ]
no redirect { ipv4_address | ipv6_address }
```

**no**

Removes the DNS IP address from the redirect rule.

**primary-dns { ipv4_address | ipv6_address } +**

Specifies the IP address of the primary home network DNS.

- `ipv4_address` must be an IPv4 address in dotted-decimal notation.
- `ipv6_address` must be an IPv6 address in colon-separated hexadecimal notation.

+ indicates that the keyword and variable option can be used multiple times in the same command.

**secondary-dns { ipv4_address | ipv6_address } +**

Specifies the IP address of the secondary home network DNS.

- `ipv4_address` must be an IPv4 address in dotted-decimal notation.
- `ipv6 address` must be an IPv6 address in colon-separated hexadecimal notation.

+ indicates that the keyword and variable option can be used multiple times in the same command.
Usage Guidelines

Use this command to identify DNS IP addresses from foreign networks that are to be redirected to the home DNS. For a more detailed explanation of the Proxy DNS feature, see the proxy-dns intercept-list command in the Context Configuration Mode Commands chapter. A maximum of 16 intercept rules (either redirect or pass-thru) are allow for each intercept list.

Since this command is configured in the source context, the destination context containing the path to the home network DNS is identified using the Context Configuration Mode command ip dns-proxy source-address.

Important

If a packet does not match the pass-thru or redirect rule, the packet is dropped. If primary-dns or secondary-dns is not configured, DNS messages are redirected to the primary-dns-server (or the secondary-dns-server) configured for the subscriber OR inside the context.

Examples

The following command identifies a foreign network DNS with an IP address of 10.2.55.12 and redirects it to a primary home network DNS with an IP address of 10.3.4.5:

```
redirect 10.2.55.12 primary-dns 10.3.4.5 primary-dns 10.5.3.5 secondary-dns 10.4.3.2
```
HA Service Configuration Mode Commands

The HA Service Configuration Mode is used to create and manage the Home Agent (HA) services within the current context.

**Command Modes**

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-ha-service) #
```

**Important**

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

- a11-signalling-packets, page 1256
- aaa, page 1257
- access-network, page 1259
- associate, page 1260
- authentication, page 1261
- bind, page 1264
- binding-update, page 1266
- default, page 1267
- default subscriber, page 1270
- description, page 1271
- encapsulation, page 1272
- end, page 1274
- exit, page 1275
• fa-ha-spi, page 1276
• gre, page 1279
• idle-timeout-mode, page 1281
• ikev1, page 1283
• ip context-name, page 1285
• ip local-port, page 1286
• ip pool, page 1287
• isakmp, page 1288
• min-reg-lifetime, page 1290
• mn-ha-spi, page 1291
• nat-traversal, page 1293
• optimize tunnel-reassembly, page 1294
• per-domain statistics-collection, page 1295
• policy bc-query-result, page 1296
• policy nw-reachability-fail, page 1297
• policy overload, page 1299
• policy null-username, page 1301
• private-address allow-no-reverse-tunnel, page 1302
• reg-lifetime, page 1303
• reverse-tunnel, page 1304
• revocation, page 1306
• setup-timeout, page 1309
• simul-bindings, page 1310
• threshold dereg-reply-error, page 1311
• threshold init-rrq-rcvd-rate, page 1313
• threshold ipsec-call-req-rej, page 1315
• threshold ipsec-ike-failrate, page 1317
• threshold ipsec-ike-failures, page 1319
• threshold ipsec-ike-requests, page 1321
• threshold ipsec-tunnels-established, page 1323
• threshold ipsec-tunnels-setup, page 1325
• threshold reg-reply-error, page 1327
• threshold rereg-reply-error, page 1329
• wimax-3gpp2 interworking, page 1331
**a11-signalling-packets**

Applies Differentiated Services Code Point (DSCP) marking for IP headers carrying outgoing signalling packets.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

```
>ha-service
```

**(Syntax Description)**

```
a11-signalling-packets ip-header-dscp ip-header-dscp
{ default | no } a11-signalling-packets ip-header-dscp
```

- **no**
  Disables DSCP marking for IP header encapsulation for the HA service.

- **default**
  Configures DSCP marking for IP header encapsulation for a specific HA service.

  **ip-header-dscp**
  Is a hexadecimal number between 0x0 and 0x3F.

**Usage Guidelines**

Use this command to apply DSCP marking for IP header carrying outgoing signalling packets.

**Examples**

The following command applies DSCP marking for IP header carrying outgoing signalling packets.

```
a11-signalling-packets ip-header-dscp 0x2f
```
aaa

Configures the sending of subscriber session AAA accounting by the HA service.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration
configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ha-service)#

Syntax Description

AAA { accounting [roaming] | group string }
no AAA { accounting | group }
default AAA accounting

no

Disables AAA accounting for the HA service.

default

Configures AAA parameters for specific HA service

accounting

accounting Enables the sending of AAA accounting information for subscriber sessions by the Home Agent (HA), by default is enabled.
roaming Enables the sending of AAA accounting information for subscriber sessions by the Home Agent (HA) only for roaming subscribers.

group

group configures aaa group for ha-service, group has lower priority than subscriber/apn config.
string: size ranges between 1 and 63.

Usage Guidelines

Enabling the HA service will send all accounting data (start, stop, and interim) to the configured AAA servers.
The chassis is shipped from the factory with the AAA accounting enabled.
In order for this command to function properly, AAA accounting must be enabled for the context in which the HA service is configured using the `aaa accounting subscriber radius` command.

**Examples**

The following command disables AAA accounting for the HA service:

```bash
no aaa accounting
```
access-network

Configures a specific access network configuration.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HA Service Configuration

```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax Description**

```
access-network accounting identifier access_network_accounting_identifier
no access-network accounting identifier
```

no
Disables a specific access network configuration.

accounting
Specifies an access network configuration for accounting

identifier
Specifies an access network accounting identifier

```
access_network_accounting_identifier
```

This is an alphanumeric string of 1 through 128 characters.

**Usage Guidelines**

This command is used to configure an access network for accounting.

**Examples**
The following command configures an access network for accounting with the identifier *idnt*:

```
access-network accounting identifier idnt
```
associate

Associates an HA-service with a QoS policy.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HA Service Configuration

`configure > context context_name > ha-service service_name`

Entering the above command sequence results in the following prompt:

`{context_name}host_name(config-ha-service)#`

**Syntax Description**

- `associate qci-qos-mapping string`
- `no associate qci-qos-mapping`

- `no`
  Disables the association of an HA-service with a QoS policy.

- `qci-qos-mapping string`
  Maps a QoS Class Identifier (QCI) for this HA service.
  `string` is an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**
This command associates an HA-service with a QoS policy.

**Examples**
The following command associates an HA-service with a QCI `map01`.

`associate qci-qos-mapping map01`
**authentication**

Configures authentication parameters for a specific HA service within a context.

**Product**

HA
ASN-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HA Service Configuration
configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax Description**

```
authentication { aaa-distributed-mip-keys [ disabled | optional | required ] | dmu-refresh-key | imsi-auth
| mn-aaa { allow-noauth | always | dereg-noauth | noauth | renew-reg-noauth | renew-and-dereg-noauth
} | mn-ha { allow-noauth | always } | pmip-auth | stale-key-disconnect }
no authentication { imsi-auth | pmip-auth }
default authentication { aaa-distributed-mip-keys | dmu-refresh-key | imsi-auth | mn-aaa | mn-ha | pmip-auth | stale-key-disconnect }

no
Disable the parameter.

default
Resets the specified option to its default setting.

aaa-distributed-mip-keys [ disabled | optional | required ]
Configures use of AAA distributed MIP keys for authenticating RRQ for WiMAX HA calls.
Default is disabled.

disabled: Disables using AAA distributed WiMAX Mobile IP (MIP) keys for authenticating MIP RRQ.
optional: Uses AAA distributed WiMAX MIP keys for authenticating RRQ with fallback option to use static/3GPP2 based MIP keys.
required: AAA distributed WiMAX MIP keys for authenticating MIP RRQ are mandatory
```
**dmu-refresh-key**

Typically, when a Dynamic Mobile IP Update (DMU) resets, the next MIP re-registration causes MN-HA authorization failure and the HA rejects the MIP RRQ. This parameter enables the HA to retrieve the MN-HA key again from the AAA during the call and to use the freshly retrieved key value to recheck authentication. Default is disabled.

**imsi-auth**

Enable uses the International Subscriber Mobile identity (IMSI) to determine if MN-AAA or MN-FAC extensions are not present in the RRQ. Default is disabled.

**mn-aaa**

\{ allow-noauth | always | dereg-noauth | noauth | renew-reg-noauth | renew-and-dereg-noauth \}

Specifies how mobile node-to-AAA authentication extension in registration requests from the mobile node should be handled by the HA service. Default is always.

- **allow-noauth**: Specifies that the HA service does not require authentication for every mobile node registration request. However, if the mn-aaa extension is received, the HA service will authenticate it.
- **always**: Specifies that the HA service will perform authentication each time a mobile node registers.
- **dereg-noauth**: Disables authentication request upon de-registration.
- **noauth**: Specifies that the HA service will not look for mn-aaa extension and will not authenticate it.
- **renew-reg-noauth**: Specifies that the HA service will not perform authentication for mobile node re-registrations. Initial registration and de-registration will be handled normally.
- **renew-and-dereg-noauth**: Disables authentication request upon re-registration and de-registration.

**mn-ha**

\{ allow-noauth | always \}

Specifies whether the HA service looks for an MN-HA authentication extension in the RRQ. Default is always.

- **allow-noauth**: Allows a request that does not contain the auth extension.
- **always**: A request should always contain the auth extension to be accepted.

**pmip-auth**

Specifies whether the HA service looks for an MN-HA authentication extension in the RRQ. Default is always.

- **allow-noauth**: Allows a request that does not contain the auth extension.
- **always**: A request should always contain the auth extension to be accepted.

**stale-key-disconnect**

If MN-HA auth fails for MIP renew and dereg, disconnects the call immediately. Disabled by default.
Usage Guidelines

The **authentication** command, combined with a keyword, can be used to specify how the system will perform authentication of registration request messages.

Examples

The following command configures the HA service to always perform mobile node authentication for every registration request.

```plaintext
authentication mn-aaa always
```

The following command configures the HA service to always look for an MN-HA authentication extension in the RRQ.

```plaintext
authentication mn-ha always
```
bind

Binds the HA service to a logical IP interface serving as the Pi interface and specifies the maximum number of subscribers that can access this service over the interface.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration
configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-ha-service)#

Syntax Description

bind address { range_IPv4address ip_mask | range_IPv4address/bitmask } [ max-subscribers count ]

no bind address

range_IPv4address ip_mask | range_IPv4address/bitmask

Specifies the pool of IP addresses (in IPv4 dotted-decimal notation) of the interface configured as the Pi interface with an enterprise HA (EHA). ip_mask and bitmask specifies the number of subnet bits, representing the subnet mask in CIDR notation and must be a value between 1 to 32.

range_IPv4address is a preconfigured range of IPv4 addresses in Loopback Interface Configuration Mode to enable the Enterprise HA support with enhanced capacity and configured

max-subscribers count

Default: 2500000

Specifies the maximum number of subscribers that can access this service on this interface.

count can be configured to an integer from 0 through 4000000.

Important

The maximum number of subscribers supported is dependant on the license key installed and the number of active packet processing cards installed in the system.
**Usage Guidelines**

Associate the HA service to a specific logical IP address. The logical IP address or interface takes on the characteristics of a Pi interface. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.

When configuring the `max-subscribers` option, be sure to consider the following:

- The total number of interfaces that you will configuring for use as Pi interfaces
- The maximum number of subscriber sessions that all of these interfaces may handle during peak busy hours
- The average bandwidth for each of the sessions
- The type of physical port to which these interfaces will be bound

Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.

IP range support is provided through `ranged_address` value. This value enables the pool of IPv4 addresses to support Enterprise HA on HA service to connect enhanced number of enterprise nodes. Refer *HA Administration Guide* for more information.

Use the `no bind address` command to delete a previously configured binding.

**Examples**

The following command would bind the logical IP interface with the address of `192.168.3.1` to the HA service and specifies that a maximum of 600 simultaneous subscriber sessions can be facilitated by the interface/service at any given time.

```
bind address 192.168.3.1
max-subscribers 600
```

The following command disables a binding that was previously configured:

```
no bind address
```

The following command binds the range of IP addresses with HA service to be used with Enterprise HA support:

```
bind address 10.2.3.0/24
```
**binding-update**

Configures MIP binding-update message related parameters.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-ha-service)#

**Syntax Description**

binding-update { max-retransmission num | retransmission-timeout seconds }

max-retransmission num

Default 3.

Configures the number of times the message shall be transmitted. num must be an integer from 1 through 5.

retransmission-timeout seconds

Default 2.

Configures the transmission timeout for the message in seconds. seconds must be an integer from 1 through 60.

**Usage Guidelines**

Configure binding update parameters.

**Examples**

Set the maximum number of times a MIP binding update message is transmitted to 4 with the following command:

binding-update max-retransmission 4
default

Restores default values assigned for a specified parameter.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ha-service)#

Syntax Description

default { authentication { imsi-auth | mn-aaa | mn-ha } | binding-update { max-retransmission | retransmission-timeout } | encapsulation | gre { checksum | checksum-verify | reorder-timeout | sequence-mode | sequence-numbers } | ip local-port | policy { null-username | nw-reachability-fail | overload } | private-address allow-no-reverse-tunnel | reg-lifetime | reverse-tunnel | revocation | enable | max-retransmission | retransmission-timeout | trigger handoff | setup-timeout | simul-bindings }

authentication

imsi-auth: Restores IMSI authentication to its default: disabled.

mn-aaa: Restores the Foreign Agent (FA) mobile node re-registration authentication setting to its default: always.

mn-ha: Configures the HA service to its default behavior of looking for an MN-HA authentication extension in the RRQ.

binding-update { max-retransmission | retransmission-timeout }

Sets the MIP binding-update message related parameters to their defaults.

max-retransmission: Default 3.

Configures the number of times the message shall be transmitted to 3.

retransmission-timeout: Configures the transmission timeout for the message to 2 seconds.

capsulation

Sets MIP data encapsulation using GRE to its default: enabled.
```

gre \{ checksum | checksum-verify | reorder-timeout | sequence-mode | sequence-numbers \}
Sets default Generic Routing Encapsulation (GRE) parameters.

checksum: Disables the introduction of the checksum field in outgoing GRE packets.
checksum-verify: Disables verification of the GRE checksum (if present) in incoming GRE packets.
reorder-timeout: Sets the maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets to the default setting: 100.
sequence-mode: Disables the reordering of incoming out-of-sequence GRE packets by setting this parameter to the default setting: none.
sequence-numbers: Disables the insertion or removal of GRE sequence numbers in GRE packets.

ip local-port
Restores the IP local-port setting to its default: 434.

policy \{ null-username | nw-reachability-fail | overload \}
Restores the Home Agent service session policy settings.
null-username: Rejects all RRQs that do not have an NAI.
 nw-reachability-fail: If the network is not reachable, rejects all incoming sessions.
overload: Restores the Home Agent service session overload policy setting to its default: reject.

private-address allow-no-reverse-tunnel
Resets the HA so that it does not accept MIP calls that use a private address without reverse tunneling.

reg-lifetime
Restores the Mobile IP session registration lifetime setting configured by the reg-lifetime command to its default: 600 seconds.

reverse-tunnel
Restores the reverse tunneling setting to its default: enabled.

revocation \{ enable | max-retransmission | retransmission-timeout | trigger \{ handoff | idle-timeout \} \}
Resets the MIP Registration Revocation settings to their default values. When no optional keywords are specified all revocation settings are set to their defaults.

enable: Disables MIP Registration Revocation on the FA.
max-retransmission: Sets the maximum number of retransmissions to 3.
retransmission-timeout: Sets the retransmission timeout to 3 seconds.
trigger \{ handoff | idle-timeout \}: handoff enables inter-Access Gateway/FA handoff as a trigger for MIP Registration Revocation. idle-timeout enables session idle timer expiration as a trigger for MIP Registration Revocation.

setup-timeout
Restore the maximum amount of time allowed for setting up a session to the default: 60 seconds.
```
simul-bindings
Restores the simultaneous bindings setting to its default: 3.

Usage Guidelines
After the system has been modified from its default values, this command is used to set/restore specific parameters to their default values.

Examples
The following command is used to return the IP local-port parameter to its default value:

default ip local-port
default subscriber

Specifies the name of a subscriber profile configured within the same context as the HA service from which to base the handling of all other subscriber sessions handled by the HA service.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration
configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

{context_name}host_name{config-ha-service}#

Syntax Description

| no | default subscriber  profile_name |

profile_name

Specifies the name of the configured subscriber profile. profile_name is an alphanumeric string of 1 through 127 characters that is case sensitive.

Usage Guidelines

Each subscriber profile specifies "rules" such as permissions, PPP settings, and timeout values. By default, the HA service will use the information configured for the subscriber named default within the same context. This command allows for multiple HA services within the same context to apply different "rules" to sessions they process. Each set of rules can be configured under a different subscriber name which is pointed to by this command.

Use the no default subscriber profile_name command to delete the configured default subscriber.

Examples

To configure the HA service to apply the rules configured for a subscriber named user1 to every other subscriber session it processes, enter the following command:

default subscriber user1
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.
encapsulation

Configures Mobile IP (MIP) encapsulation types supported for a specific HA service.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-ha-service)#

Syntax Description

| no | encapsulation allow { gre | keyless-gre } |

no
Disables MIP encapsulation types supported for specific HA service

allow
Allows encapsulation type for MIP data.

gre
Default: Enabled.
Specifies the use of Generic Routing Encapsulation (GRE) for MIP data.

keyless-gre
Default: Disabled.
Specifies the use of GRE without exchanging keys for MIP data.

Usage Guidelines

Use to disable or re-enable the use of GRE encapsulation or Key-less encapsulation for MIP sessions.
In case of chassis HA operating with other vendor equipment, which does not support the 3GPP2 to exchange key, this command with keyless-gre keyword will make the chassis HA to accept MIP data with legacy GRE.
Examples

To disable GRE for MIP sessions, enter the following command:
```
no encapsulation allow
gre
```
To re-enable GRE for MIP sessions, enter the following command:
```
encapsulation allow
gre
```
To enable key-less GRE for MIP sessions, enter the following command:
```
encapsulation allow
keyless-gre
```
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

del

Usage Guidelines

Use this command to return to the Exec mode.
exit

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

exit

**Usage Guidelines**

Use this command to return to the parent configuration mode.
fa-ha-spi

Configures the security parameter index (SPI) for specific HA service parameters.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration
configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-ha-service)#

Syntax Description

fa-ha-spi remote-address {fa_ip_address | fa_ip_address_mask} spi-number number {encrypted secret
enc_secret | secret secret | | allow-fa-ha-auth-extension | | description string | |
disable-fa-ha-auth-extension | | hash-algorithm {hmac-md5 | md5 | rfc2002-md5} | | replay-protection
{nonce | timestamp | timestamp-tolerance tolerance | } | | timestamp-tolerance tolerance |
nofa-ha-spi remote-address {fa_ip_address | fa_ip_address_mask} spi-number number

no

Disables the security parameter index (SPI) for specific HA service parameters.

remote-address {fa_ip_address | fa_ip_address_mask}

Specifies the IP address of the FA. fa_ip_address is entered using IPv4 dotted-decimal notation with CIDR
for the subnet mask.

**Important**
The system supports unlimited peer FA addresses per HA but only maintains statistics for a maximum of
8,192 peer FAs. If more than 8,192 FAs are attached, older statistics are overwritten.

**spi-number number**

Specifies the SPI (number) which indicates a security context between the FA and the HA in accordance with
RFC 2002.

*number* is an integer value from 256 through 4294967295.
encrypted secret \texttt{enc\_secret} | secret \texttt{secret}

Configures the shared-secret between the HA service and the FA. The secret can be either encrypted or non-encrypted.

\texttt{encrypted secret enc\_secret}: Specifies the encrypted shared key between the HA service and the FA. \texttt{enc\_secret} must be an alphanumeric string of 1 through 236 characters that is case sensitive.

\texttt{secret secret}: Specifies the shared key between the HA service and the FA. \texttt{secret} must be an alphanumeric string of 1 through 236 characters that is case sensitive.

\texttt{allow-fa-ha-auth-extension}

Allows validation of FA HA Authentication extension.

\texttt{description string}

This is a description for the SPI. \texttt{string} must be an alphanumeric string of 0 through 31 characters.

\texttt{hash-algorithm \{ hmac-md5 | md5 | rfc2002-md5 \}}

Default: hmac-md5

Specifies the hash-algorithm used between the HA service and the FA.

\texttt{hmac-md5}: Configures the hash-algorithm to implement HMAC-MD5 per RFC 2002bis.

\texttt{md5}: Configures the hash-algorithm to implement MD5 per RFC 1321.

\texttt{rfc2002-md5}: Configures the hash-algorithm to implement keyed-MD5 per RFC 2002.

\texttt{replay-protection \{ timestamp \[ timestamp-tolerance tolerance \] \[ nonce \] \}}

Specifies the replay-protection scheme that should be implemented by the FA service for this SPI.

\texttt{nonce}: Configures replay protection to be implemented using NONCE per RFC 2002.

\texttt{timestamp}: Configures replay protection to be implemented using timestamps per RFC 2002.

\texttt{timestamp-tolerance}: Specifies the allowable difference (tolerance) in timestamps that is acceptable. If the difference is exceeded, then the session will be rejected. \texttt{tolerance} is measured in seconds and can be configured to an integer from 1 and 65535. The default is 60.

**Usage Guidelines**

An SPI is a security mechanism configured and shared by the HA service and the FA. Please refer to RFC 2002 for additional information.

Though it is possible for FAs and HAs to communicate without SPIs being configured, the use of them is recommended for security purposes. It is also recommended that a "default" SPI with a remote address of 0.0.0.0/0 be configured on both the HA and FA to prevent hackers from spoofing addresses.

**Important**

The SPI configuration on the HA must match the SPI configuration for the FA service on the system in order for the two devices to communicate properly.

A maximum of 2,048 SPIs can be configured per HA service.

Use the \texttt{no} version of this command to delete a previously configured SPI.
The following command configures the FA service to use an SPI of 512 when communicating with an HA with the IP address 192.168.0.2. The key that would be shared between the HA and the FA service is q397F65. When communicating with this HA, the FA service will also be configured to use the rfc2002-md5 hash-algorithm.

```
fa-ha-spi remote-address
192.168.0.2 spi-number 512 secret q397F65 hash-algorithm rfc2002-md5
```

The following command deletes the configured SPI of 400 for an HA with an IP address of 172.100.3.200:

```
no fa-ha-spi remote-address
172.100.3.200 spi-number 400
```
**gre**

Configures Generic Routing Encapsulation (GRE) parameters.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

()[context_name]host_name(config-ha-service)#

**Syntax Description**

`gre { checksum | checksum-verify | reorder-timeout timeout | sequence-mode { none | reorder } | sequence-numbers }

default gre { checksum | checksum-verify | reorder-timeout | sequence-mode | sequence-numbers }

no
disables the specified functionality.

default
sets or restores default value assigned for specified parameter.

checksum

default: disabled

Enables the introduction of the checksum field in outgoing GRE packets.

checksum-verify

default: disabled

Enables verification of the GRE checksum (if present) in incoming GRE packets.

reorder-timeout timeout

default: 100
Configures the maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets. \textit{timeout} must be an integer from 0 through 5000.

\textbf{sequence-mode} \{ none | reorder \}
Default: none
Configures how incoming out-of-sequence GRE packets should be handled.
\textbf{none}: Disables reordering of incoming out-of-sequence GRE packets.
\textbf{reorder}: Enables reordering of incoming out-of-sequence GRE packets.

\textbf{sequence-numbers}
Default: Disabled
 Enables the insertion of sequence numbers into the GRE packets.

\textbf{Usage Guidelines} Use this command to configure how the HA service handles GRE packets.

\textbf{Examples} To set the maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets to 500 milliseconds, enter the following command:
\texttt{gre reorder-timeout 500}
To enable the reordering of incoming out of sequence GRE packets, enter the following command:
\texttt{gre sequence-mode reorder}
To enable the insertion or removal of GRE sequence numbers in GRE packets, enter the following command:
\texttt{gre sequence-numbers}
idle-timeout-mode

Configures the sessions idle-timer reset behavior.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HA Service Configuration

```bash
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax Description**

```
idle-timeout-mode { aggressive | handoff | normal } | upstream-only |
```

**default idle-timeout-mode**

```
default
```

Resets the idle timeout mode to the default settings.

**aggressive**

Resets the session idle timer only when MIP user data is detected. This is the default behavior.

**handoff**

Resets the session idle timer when MIP user data is detected and an inter-Access Gateway/FA handoff occurs.

**normal**

Resets the session idle timer when MIP user data is detected and any MIP control signaling occurs.

**upstream-only**

Only upstream user data (data from the mobile node) resets the idle timer for the session. This is disabled by default.

**Usage Guidelines**

Use this command to set how the current HA service resets the idle timer for a session.
**Examples**

To reset the idle timer whenever user data is detected or whenever an inter-Access Gateway/FA occurs, use the following command:

`idle-timeout-mode handoff`
ikev1

Configures IPSec Internet Key Exchange (IKE) parameters.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ha-service)#

Syntax Description

ikev1 { aaa-context aaa_context_string | peer-fa IPAddress crypto-map crypto_map_string | encrypted | secret secret_string | skew-lifetime seconds }

no ikev1 { aaa-context | peer-fa IPAddress | skew-lifetime }

no

Disables IPSec IKE parameters.

aaa-context aaa_context_string

Configures AAA context from which to retrieve IKE keys. Must be followed by the context name.

aaa_context_string is an alphanumeric string of 1 through 63 characters.

peer-fa IPAddress

Sets the IKE crypto-map for a peer Foreign Agent (FA).

IPAddress is IP address entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

crypto-map crypto_map_string

Configures IKE crypto-map. Must be followed by the crypto-map name.

crypto_map_string is an alphanumeric string of 1 through 63 characters.

encrypted designates use of encryption

secret secret_string uses a secret that is shared between FA and HA. secret_string is an alphanumeric string of 1 through 256 characters.
skew-lifetime seconds
Configures the "S" lifetime Skew (in seconds). *seconds* is an integer from 1 through 65534. Default is 10.

**Usage Guidelines**
Use this command to configure IPSec IKE parameters.

**Examples**
ikev1 peer-fa 11.22.33.44 crypto-map er encrypted secret ert
**ip context-name**

Specifies name of the destination context to be applied to the subscribers.

This configuration overrides the local subscriber configuration as well as the return attributes sent by RADIUS. All calls coming to this HA service are assigned this destination context; the IP address is allocated from the specified IP pool or group that is configured in the context specified in the service.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

\[context_name\]host_name(config-ha-service)#

**Syntax Description**

```plaintext
ip context-name name
{ default | no } ip context-name

default
Sets the default value assigned for context-name.

no
Removes the current assigned context from the subscriber's data.

name
Specifies the name of the context to assign the subscriber to once authenticated. name must be an alphanumeric string from 1 through 79 characters.
```

**Usage Guidelines**

Set the name of the destination context to be applied to the subscribers.

**Examples**

The following command configures the IP context name of sampleName:

```bash
ip context-name sampleName
```
**ip local-port**

Configures the local User Datagram Protocol (UDP) port for the Pi interface's IP socket on which to listen for Mobile IP Registration messages.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HA Service Configuration

```bash
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(config-ha-service)#
```

**Syntax Description**

**ip local-port number**

default ip local-port

default

Sets or restores the default value assigned for the IP local port.

**number**

Specifies the UDP port number.

*number* is an integer from 1 through 65535. Default is 434.

**Usage Guidelines**

Specify the UDP port that should be used for communications between the FA service and the HA.

**Examples**

The following command specifies a UDP port of 3950 for the HA service to use to communicate with the HA on the Pi interface:

```bash
ip local-port 3950
```
ip pool

Specifies name of the IP address pool or group to use for subscriber IP address allocation.
This configuration overrides the local subscriber configuration, as well as the return attributes sent by RADIUS.
All calls coming to this HA service are assigned this destination context and an IP address is allocated from
the specified IP pool or group that is configured in the context specified in the service.

Product
HA

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > HA Service Configuration
configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:
[context_name]host_name(config-ha-service)#

Syntax Description
ip pool name
{ default | no } ip pool

name
Specifies the logical name of the IP address pool. name must be an alphanumeric string of 1 through 31
characters.

no
Removes the specified IP address pool specified from the current context or disables the option for an IP pool.

default
Cleans the IP address pool or group setting.

Usage Guidelines
Define a pool of IP addresses for the context to use in assigning IPs for this service.

Examples
The specifies name of the IP address pool or group to use for subscriber IP address allocation:
ip pool pool1
The following command removes the specified IP address pool:
no ip pool
isakmp

Configures the crypto map for a peer HA and the default crypto map for the FA service.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HA Service Configuration
configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-ha-service)#

Syntax Description

isakmp { peer-fa fa_address | [ [ encrypted | secret ] ] | skew-lifetime time | aaa-context context_name }

no isakmp { peer-fa fa_address | default | skew-lifetime | aaa-context }

no

Deletes the reference to the crypto map for the specified HA; deletes the reference for the default crypto map; resets the skew-lifetime to the default; or resets the aaa-context to the default.

peer-fa fa_address { crypto map map_name | [ [ encrypted | secret ] ] }

Configures a crypto map for a peer FA.

- *fa_address*: IP address of the peer FA to which this IPSec SA will be established.
- *crypto map map_name*: The name of a crypto map configured in the same context that defines the IPSec tunnel properties. *map_name* is an alphanumeric string of 1 through 63 characters.
- *encrypted*: This keyword is intended only for use by the chassis while saving configuration scripts. The system displays the *encrypted* keyword in the configuration file as a flag that the variable following the *secret* keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.
- *secret secret*: The pre-shared secret that will be used to during the IKE negotiation. *secret* is an alphanumeric string of 1 through 127 characters.

skew-lifetime time

Default: 10 seconds
Configures the IKE pre-shared key's time skew.

`time` is the amount of time the fetched from AAA that is considered valid after the key has expired. It is measured in seconds and can be configured to an integer from 1 through 65534.

```
aaa-context context_name
```

Default: The context in which the service is configured

Configures the name of the context on the system in which AAA functionality is performed.

`context_name` is the name of the context through which the HA service accesses the HAAA server to fetch the IKE S Key and S Lifetime parameters. It is an alphanumeric string of 1 through 63 characters that is case sensitive.

**Usage Guidelines**

Use this command to configure the FA-service's per-HA IPSec parameters. These dictate how the HA service is to establish an IPSec SA with the specified FA.

**Important**

For maximum security, this command be executed for every possible FA with which the HA service communicates.

Note that once an IPSec tunnel is established between the FA and HA for a particular subscriber, all new Mobile IP sessions using the same FA and HA are passed over the tunnel regardless of whether or not IPSec is supported for the new subscriber sessions. Data for existing Mobile IP sessions is unaffected.

**Examples**

The following command creates a reference for an HA with the IP address 10.2.3.4 to a crypto map named `map1`:

```
isakmp peer-fa 10.2.3.4 crypto-map map1
```

The following command deletes the crypto map reference for the HA with the IP address 10.2.3.4.

```
o isakmp peer-fa 10.2.3.4 crypto-map map1
```

The following command sets the time an S key can used after the S lifetime expires to 120 seconds.

```
isakmp skew-lifetime 120
```

The following command creates the default reference for an HA to a crypto map named `map1`, where peer address is unknown:

```
isakmp default crypto-map map1
```
min-reg-lifetime

Configures Mobile IP session minimum registration lifetime, in seconds.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HA Service Configuration
`configure > context context_name > ha-service service_name`

Entering the above command sequence results in the following prompt:
```
{context_name}\host_name{(config-ha-service) #}
```

**Syntax Description**
<table>
<thead>
<tr>
<th>`</th>
<th>no</th>
<th>default</th>
<th>min-reg-lifetime</th>
<th>min_reg_lifetime_seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables the min registered lifetime.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>default</td>
<td>Configures Mobile IP session minimum registration lifetime to default which is 0.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use this command to configure Mobile IP session minimum registration lifetime, in seconds, between 1 and 65534. Default is 0 seconds.

**Examples**
Use the following command to configure mobile IP session to minimum registered life time to 100 seconds:
```
min-reg-lifetime 100
```
**mn-ha-spi**

Configures the security parameter index (SPI) between the HA service and the mobile node (MN).

**Product**  
HA

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration > Context Configuration > HA Service Configuration

```bash
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```bash
[context_name]host_name(config-ha-service)#
```

**Syntax Description**

```
mn-ha-spi spi-number number [ description string ] [ encrypted secret enc_secret ] [ hash-algorithm { hmac-md5 | md5 | rfc2002-md5 } ] [ permit-any-hash-algorithm ] [ replay-protection { nonce | timestamp } ] [ secret secret ] [ timestamp-tolerance tolerance ]
```

- **spi-number**  
  Specifies the SPI (number) which indicates a security context between the mobile node and the HA service in accordance with RFC 2002. `number` can be configured to an integer from 256 through 4294967295.

- **description string**  
  This is a description for the SPI. `string` is an alphanumeric string of 1 through 31 characters.

- **encrypted secret enc_secret | secret secret**  
  Configures the shared-secret between the HA service and the mobile node. The secret can be either encrypted or non-encrypted.

  - **encrypted secret enc_secret**: Specifies the encrypted shared key between the HA service and the mobile node. `enc_secret` must be an alphanumeric string of 1 through 254 characters that is case sensitive.

  - **secret secret**: Specifies the shared key between the HA service and the mobile node. `secret` must be an alphanumeric string of 1 through 127 characters that is case sensitive.

  The `encrypted` keyword is intended only for use by the chassis while saving configuration scripts. The system displays the `encrypted` keyword in the configuration file as a flag that the variable following the `secret` keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.
hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }
Default: hmac-md5
Specifies the hash-algorithm used between the HA service and the mobile node.
hmac-md5: Configures the hash-algorithm to implement HMAC-MD5 per RFC 2002bis.
md5: Configures the hash-algorithm to implement MD5 per RFC 1321.
rfc2002-md5: Configures the hash-algorithm to implement keyed-MD5 per RFC 2002.

permit-any-hash-algorithm
Default: disabled
Allows verification of the MN-HA authenticator using all other hash-algorithms after failure with configured
hash-algorithm. The successful algorithm is logged to aid in troubleshooting and used to create the MN-HA
authenticator in the Registration Reply message.

replay-protection { nonce | timestamp }
Default: timestamp
Specifies the replay-protection scheme that should be implemented by the HA service for this SPI.
nonce: configures replay protection to be implemented using NONCE per RFC 2002.
timestamp: configures replay protection to be implemented using timestamps per RFC 2002.

timestamp-tolerance tolerance
Default: 60
Specifies the allowable difference (tolerance) in timestamps that is acceptable. If the difference is exceeded,
then the session will be rejected. If this is set to 0, timestamp tolerance checking is disabled at the receiving
end.
Tolerance is measured in seconds and can be configured to an integer from 0 through 65535.

Usage Guidelines
An SPI is a security mechanism configured and shared by the HA service and the mobile node. Please refer
to RFC 2002 for additional information.
Use the no version of this command to delete a previously configured SPI.

Examples
The following command configures the HA service to use an SPI of 640 when communicating with a mobile
node. The key that would be shared between the mobile node and the HA service is q397F65.

mn-ha-spi spi-number 640 secret q397F65

The following command deletes the configured SPI of 400:

no mn-ha-spi spi-number 400
**nat-traversal**

This command enables NAT traversal and also configures the forcing of UDP tunnels for NAT traversal.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HA Service Configuration

```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax Description**

```
[ default | no ] nat-traversal [ force-accept ]
```

- **no**
  
  Disables NAT traversal or disables forcing the acceptance of UDP tunnels for NAT traversal.

- **default**
  
  Reset the defaults for this command.
  
  Default: NAT traversal disabled, force-accept disabled.

- **force-accept**
  
  This keyword configures the HA to accept requests when NAT is not detected but the Force (F) bit is set in the RRQ with the UDP Tunnel Request. By default this type of request is rejected if NAT is not detected.

**Usage Guidelines**

Use this command to enable NAT traversal and enable the forcing of UDP tunnels for NAT traversal.

**Examples**

The following command enables NAT traversal for the current HA service and forces the HA to accept UDP tunnels for NAT traversal:

```
nat-traversal force-accept
```

---

**HA Service Configuration Mode Commands**

- **nat-traversal**

---

**Command Line Interface Reference, Modes G - H, StarOS Release 19**

1293
**optimize tunnel-reassembly**

Designates that tunnel reassembly optimization will be used for fragmented large packets passed between HA and FA. Default is disabled.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

```
/context_name/host_name(config-ha-service)#
```

**Syntax Description**

| default | no | optimize tunnel-reassembly |

**Usage Guidelines**

Enabling this functionality fragments large packets prior to encapsulation for easier processing.

Tunnel reassembly optimization is disabled by default.

---

**Important**

You should *not* use this command without first consulting Cisco Systems Technical Support. This command applies to very specific scenarios where packet reassembly is not supported at the far end of the tunnel. There are cases where the destination network may either discard the data, or be unable to reassemble the packets.

---

**Important**

This functionality works best when the HA service is communicating with an FA service running in a system. However, an HA service running in the system communicating with an FA from a different manufacturer will operate correctly even if this parameter is enabled.

Use the `no` version of this command to disable tunnel optimization if enabled.

**Examples**

The following command enables tunnel reassembly optimization:

```
optimize tunnel-reassembly
```
**per-domain statistics-collection**

Enables per-domain statistics collection.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HA Service Configuration

```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax Description**

```
[ no ] per-domain statistics-collection
```

**no**

Disables per-domain statistics collection.

**Usage Guidelines**

Use this command to enable per-domain statistics collection.

**Examples**

The following command enables per-domain statistics collection.

```
per-domain statistics-collection
```
policy bc-query-result

Configure the binding cache (BC) query Response Result code.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HA Service Configuration

```configure > context context_name > ha-service service_name```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax Description**

- `policy bc-query-result network-failure code`
- `default policy bc-query-result network-failure`

`network-failure code`

Default: 0xFFFF

Specify the response code for BC responses sent on network failures.

`code` must be either 0xFFFF or 0xFFFE.

**Usage Guidelines**

Use this command to specify the type of response code to send in a P-MIP BC query result.

**Examples**

The following command sets the P-MIP BC query result response code to 0xFFFE:

```policy bc-query-result network-failure 0xFFFE```
policy nw-reachability-fail

Specifies the action to take upon detection of an up-stream network -reachability failure.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HA Service Configuration

```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax Description**

```
policy nw-reachability-fail { redirect ip_addr1 [ weight value ] ... ip_addr16 [ weight value ] | reject [ use-reject-code { admin-prohibited | insufficient-resources } ] } no policy nw-reachability-fail { redirect ip_addr1 ... ip_addr16 }
```

`no`

Deletes the network reachability policy completely or deletes the specified redirect addresses fro the policy.

`reject [ use-reject-code { admin-prohibited | insufficient-resources } ]`

Upon network reachability failure, reject all new calls for this context.

`use-reject-code { admin-prohibited | insufficient-resources }`: When rejecting calls send the specified reject code. If this keyword is not specified the admin-prohibited reject code is sent by default.

`reject [ use-reject-code { admin-prohibited | insufficient-resources } ]`

Upon network reachability failure reject all new calls for this context. If no reject code is specified, the HA sends a registration reply code of 81H (admin-prohibited).

`use-reject-code { admin-prohibited | insufficient-resources }`: Use the specified reject code when rejecting traffic.

admin-prohibited: When this keyword is specified and traffic is rejected, the error code 81H (admin-prohibited) is returned.

insufficient-resources: When this keyword is specified and traffic is rejected, the error code 82H (insufficient resources) is returned.
redirect ip_addr1 [ weight value ] | ip_addr2 [ weight value ] ... ip_addr16 [ weight value ] |

Upon network reachability failure redirect all calls to the specified IP address.

ip_addr1: This must entered using IPv4 dotted-decimal notation. Up to 16 IP addresses and optional weight values can be entered on one command line.

weight value: When multiple addresses are specified, they are selected in a weighted round-robin scheme. If a weight is not specified the entry is automatically assigned a weight of 1. value must be an integer from 1 through 10.

Usage Guidelines

Use this command to set the action for the HA service to take upon a network reachability failure.

---

**Important**

Refer to the Context Configuration mode command `nw-reachability server` to configure network reachability servers.

---

**Important**

Refer to the Subscriber Configuration 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 Context Configuration mode `ip pool` command to bind the network reachability server to an IP pool.

---

Examples

To set the HA service to reject all new calls on a network reachability failure, enter the following command:

```
policy nw-reachability-fail reject
```

Use the following command to set the HA service to redirect all calls to the HA at IP address 192.168.100.10 and 192.168.200.10 on a network reachability failure:

```
policy nw-reachability-fail redirect 192.168.100.10 192.168.200.10
```
policy overload

Configures the overload policy within the HA service.

Product  
HA

Privilege  
Security Administrator, Administrator

Command Modes  
Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ha-service)#

Syntax Description

policy overload { redirect address [ weight weight_num ] | address2 [ weight weight_num ] ... address16 [ weight weight_num ] | reject [ use-reject-code { admin-prohibited | insufficient-resources } ] }

no policy overload [ redirect address | address2...address16 ]

Deletes a previously set policy or removes a redirect IP address.

overload: Without any options deletes the complete overload policy from the PDSN service.

overload redirect address [ address2 ... address16 ]: deletes up to 16 IP addresses from the overload redirect policy. The IP addresses must be expressed in IP v4 dotted-decimal notation

redirect address [ weight weight_num ] | address2 [ weight weight_num ] ... address16 [ weight weight_num ]

This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the HA service rejects new sessions with a Registration Reply Code of 136H (unknown home agent address) and provides the IP address of an alternate HA. This command can be issued multiple times.

address: The IP address of an alternate HA expressed in IP v4 dotted-decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy, the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.

weight weight_num: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. weight_num must be an integer from 1 through 10.
reject | use-reject-code { admin-prohibited | insufficient-resources } |

This option causes any overload traffic to be rejected. If no reject code is specified, the HA sends a registration reply code of 81H (admin-prohibited).

use-reject-code { admin-prohibited | insufficient-resources }: Use the specified reject code when rejecting traffic.

admin-prohibited: When this keyword is specified and traffic is rejected, the error code 81H (admin-prohibited) is returned.

insufficient-resources: When this keyword is specified and traffic is rejected, the error code 82H (insufficient resources) is returned.

Usage Guidelines

The system invokes the overload policy if the number of calls currently being processed exceeds the licensed limit for the maximum number of sessions supported by the system.

The system automatically invokes the overload policy when an on-line software upgrade is started.

Use the no version of this command to restore the default policy.

The setting for overload policy is reject.

Examples

The following command enables an overload redirect policy for the HA service that will send overload calls to either of two destinations with weights of 1 and 10 respectively:

```
policy overload redirect 192.168.100.10 weight 1 192.168.100.20 weight 10
```
policy null-username

Configures the current HA service to accept or reject an RRQ without an NAI extension.

Important
This command is customer specific and license enabled.

Product
HA

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > HA Service Configuration
configuration > context context_name > ha-service service_name
Entering the above command sequence results in the following prompt:
(context_name)host_name(config-ha-service)#

Syntax Description
policy null-username { accept-static | reject }
no policy null-username

no
Set the HA back to the default behavior of rejecting an RRQ without an NAI extension.

accept-static
This enable the HA to accept an RRQ with a static (non-zero) home address request but without NAI extension, when MN-AAA authentication is disabled at the HA. MN-NAI is required for MN-AAA authentication.

reject
Default. This is the default behavior of rejecting an RRQ without an NAI extension.

Usage Guidelines
Use this command to enable or disable the HA from accepting an RRQ without an NAI.

Examples
The following command enables the current HA service to accept RRQs that do not have an NAI extension:
policy null-username accept-static
private-address allow-no-reverse-tunnel

This command allows the HA service to accept private addresses without using reverse tunneling.

---

**Important**

This command is customer specific and license enabled.

---

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HA Service Configuration

`configure > context context_name > ha-service service_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ha-service)#`

**Syntax Description**

`[ no ] private-address allow-no-reverse-tunnel`

*no*

Reject MIP calls that use private addresses and do not use reverse tunneling.

**Usage Guidelines**

Use this command to enable or disable the HA from accepting calls that use private addresses without reverse tunneling.

**Examples**

The following command enables the current HA service to accept MIP calls that use private addresses but do not use reverse tunneling:

`private-address allow-no-reverse-tunnel`
**reg-lifetime**

Configures Mobile IP session registration lifetime.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HA Service Configuration

```bash
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax Description**

```
reg-lifetime  time  
{ default | no } reg-lifetime
```

- **no**
  
  Sets the registration lifetime to infinite.

- **default**
  
  Sets the registration lifetime to default value, 600.

- **time**
  
  Specifies the registration lifetime in seconds.
  
  `time` is an integer from 1 through 65534.

**Usage Guidelines**

Use this command to limit a mobile node's lifetime. If the mobile node requests a shorter lifetime than what is specified, it is granted. However, per RFC 2002, should a mobile node request a lifetime that is longer than the maximum allowed by this parameter, the HA service will respond with the value configured by this command as part of the Registration Reply. The default is 600 seconds.

**Examples**

The following command configures the registration lifetime for the HA service to be 2400 seconds:

```
reg-lifetime 2400
```

The following command configures an infinite registration lifetime for MIP calls:

```
no reg-lifetime
```
reverse-tunnel

Enables use of reverse tunneling for Mobile IP session. Use no reverse-tunnel command to disable. If disabled, mobile node (MN) packets are not tunneled to the HA in the reverse direction.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HA Service Configuration

```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
<context_name>@context_name>host_name(config-ha-service)#
```

**Syntax Description**

```
| default | no | reverse-tunnel
```

- **no**
  
  Indicates the reverse tunnel option is to be disabled. When omitted, the reverse tunnel option is enabled.

- **default**
  
  Indicates the reverse tunnel option is to be set to the default. When omitted, the reverse tunnel option is enabled.

**Usage Guidelines**

Reverse tunneling involves tunneling datagrams originated by the mobile node to the HA service via the FA. When an MN arrives at a foreign network, it listens for agent advertisements and selects an FA that supports reverse tunnels. The MN requests this service when it registers through the selected FA. At this time, the MN may also specify a delivery technique such as Direct or the Encapsulating Delivery Style.

Among the advantages of using reverse-tunneling are that:

- All datagrams from the mobile node seem to originate from its home network
- The FA can keep track of the HA to which the mobile node is registered and tunnel all datagrams from the mobile node to its HA

Use the **no** version of this command to disable reverse tunneling. If reverse tunneling is disabled, and the mobile node does not request it, triangular routing will be performed.

Routing will be used.
The default setting is reverse tunnel enabled.

**Important** If reverse tunneling is disabled on the system and a mobile node requests it, the call will be rejected with a reply code of 74H (reverse-tunneling unavailable).

**Examples**
The following command disables reverse-tunneling support for the HA service:
```
no reverse-tunnel
```
revocation

Configures the Registration Revocation feature for a specific HA service.

Product
HA

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > HA Service Configuration
  configure > context context_name > ha-service service_name

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

Syntax Description

  revocation { enable | max-retransmission number | negotiate-i-bit | retransmission-timeout secs | send-nai-ext | trigger { handoff | idle-timeout } }
  no revocation { enable | negotiate-i-bit | send-nai-ext | trigger { handoff | idle-timeout } }
  default revocation { enable | max-retransmission | negotiate-i-bit | retransmission-timeout | send-nai-ext | trigger { handoff | idle-timeout } }

  no
  Completely disables registration revocation on the HA, disables trigger handoff, or disables revocation on idle timer expiration.

  default
  Sets or restores the default value assigned for specified parameter.

  enable
  Enables the MIP registration revocation feature on the HA. When enabled, if revocation is negotiated with an FA and a MIP binding is terminated, the HA can send a Revocation message to the FA. This feature is disabled by default.

  max-retransmission number
  Default: 3
  The maximum number of retransmissions of a Revocation message before the revocation fails. number must be an integer from 0 through 10.
negotiate-i-bit
Default: disabled
Enables the HA to negotiate the i-bit via PRQ/RRP messages and processes the i-bit revocation messages.

retransmission-timeout secs
Default: 3
The number of seconds to wait for a Revocation Acknowledgement from the FA before retransmitting the Revocation message. secs must be an integer from 1 through 10.

send-nai-ext
Default: off
Enables sending the NAI extension in the revocation message.

trigger { handoff | idle-timeout }

handoff: Default: Enabled
Triggers the HA to send a Revocation message to the FA when an inter-Access Gateway/FA handoff of the MIP session occurs. If this is disabled, the HA is never triggered to send a Revocation message.

idle-timeout: Default: Enabled
Triggers the HA to send a Revocation message to the FA when a session idle timer expires.

Usage Guidelines
Use this command to enable or disable the MIP revocation feature on the HA or to change settings for this feature. Both the HA and the FA must have Registration Revocation enabled and FA/HA authorization must be in use for Registration Revocation to be negotiated successfully.

Examples
The following command enables Registration Revocation on the HA:

```
revocation enable
```

The following command sets the maximum number of retries for a Revocation message to 10:

```
revocation max-retransmission 10
```

The following command sets the timeout between retransmissions to 3:

```
revocation retransmission-timeout 3
```

The behavior of send MIP revocation to FA is as follows:

- 1st retry: Retransmit in 3 seconds after previous MIP revocation send.
- 2nd retry: Retransmit in 6 seconds after previous MIP revocation send (9 seconds after sending initial MIP revocation).
- 3rd retry: Retransmit in 12 seconds after previous MIP revocation send (21 seconds after sending initial MIP revocation).
- 4th retry: Retransmit in 24 seconds after previous MIP revocation send (45 seconds after sending initial MIP revocation).
- 5th retry: Retransmit in 48 seconds after previous MIP revocation send (93 seconds after sending initial MIP revocation).
The value of retransmission-timeout doubles. HA disconnects the session forcibly in 120 seconds after sending initial MIP revocation.
**setup-timeout**

The maximum time allowed for session setup in seconds. Default is 60 seconds.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HA Service Configuration

```bash
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-ha-service)#
```

**Syntax Description**

`setup-timeout seconds`

`default setup-timeout`

`default`

Sets or restores the default value.

`seconds`

Default: 60 seconds

The maximum amount of time (in seconds) to allow for setup of a session. `seconds` must be an integer from 1 through 1000000

**Usage Guidelines**

Use this command to set the maximum amount of time allowed for setting up a session.

**Examples**

To set the maximum time allowed for setting up a session to 5 minutes (300 seconds), enter the following command:

```bash
setup-timeout 300
```
**simul-bindings**

Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address.

**Product**  
HA

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration > Context Configuration > HA Service Configuration  
`configure > context context_name > ha-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax Description**

- `simul-bindings number`
  - `default simul-bindings`
  - `default`
  - `number`

  **Number**
  
  Configures the maximum number of simultaneous "care-of" bindings that the HA service will maintain for any given subscriber.
  
  It is an integer from 1 through 3.

**Usage Guidelines**

Per RFC 2002, the HA service creates a mobile binding record (MBR) for each subscriber session it is facilitating. Each MBR is associated with a care-of address. As the mobile node roams, it is possible that the session will be associated with a new care of address.

Typically, the HA service will delete an old binding and create a new one when the information in the Registration Request changes. However, the mobile could request that the HA maintain previously stored MBRs. This command allows you to configure the maximum number of MBRs that can be stored per subscriber if the requested. The default value is 3.

**Examples**

The following command configures the HA service to support up to 4 MBRs per subscriber:

```
simul-bindings 4
```
threshold dereg-reply-error

Sets an alarm or alert based on the number of de-registration reply errors per HA service.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HA Service Configuration

```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-ha-service)#
```

**Syntax Description**

```
threshold dereg-reply-error high_thresh | clear low_thresh |
no threshold dereg-reply-error
```

- **no**
  
  Deletes the alert or alarm.

- **high_thresh**
  
  Default: 0

  Specifies the high threshold number of de-registration reply errors that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to an integer from 0 through 100000.

- **clear low_thresh**
  
  Default: 0

  The low threshold number of de-registration reply errors that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to an integer from 0 through 100000.

**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 number of de-registration reply errors is equal to or greater than a specified number of calls per second.
Alerts or alarms are triggered for the number of de-registration reply errors on the following rules:

- **Enter condition**: Actual number of de-registration reply errors > High Threshold
- **Clear condition**: Actual number of de-registration reply errors < Low Threshold

**Examples**

The following command configures a de-registration reply error threshold of **1000** and a low threshold of **500** for a system using the Alarm thresholding model:

```
threshold dereg-reply-error 1000 clear 500
```
**threshold init-rrq-rcvd-rate**

Sets an alarm or alert based on the average number of calls setup per second for the context.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HA Service Configuration

`configure > context context_name > ha-service service_name`

Entering the above command sequence results in the following prompt:

\[(context_name)host_name(config-ha-service)#\]

**Syntax Description**

`threshold init-rrq-rcvd-rate high_thresh [clear low_thresh]`

`no threshold init-rrq-rcvd-rate`

- **no**
  
  Deletes the alert or alarm.

- **high_thresh**
  
  Default: 0
  
  Specifies 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. *high_thresh* is an integer from 0 through 100000.

- **clear low_thresh**
  
  Default: 0
  
  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. *low_thresh* is an integer from 0 through 100000.

---

**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 setup per second is equal to or greater 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 is greater than the high threshold.
- **Clear condition**: Actual number of calls setup per second is less than the 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 init-rrq-rcvd-rate 1000 clear 500
```
threshold ipsec-call-req-rej
Configures a threshold for the total IPSec calls request rejected.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HA Service Configuration
configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:
context_name

**Syntax Description**

```
threshold ipsec-call-req-rej high_thresh [ clear low_thresh ]
no threshold ipsec-call-req-rej
```

- **no**
  Deletes the alert or alarm.

- **high_thresh**
  Default: 0
  Specifies the high threshold number of IPSec call requests rejected per second that must be met or exceeded within the polling interval to generate an alert or alarm.
  high_thresh is an integer from 0 through 1000000.

- **clear low_thresh**
  Default: 0
  Specifies the low threshold number of IPSec call requests rejected per second that must be met or exceeded within the polling interval to clear an alert or alarm.
  low_threshold is an integer from 0 through 1000000.

**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.

---

Command Line Interface Reference, Modes G - H, StarOS Release 19
Usage Guidelines

Use this command to set an alert or an alarm when the number of IPSec call requests rejected is equal to or greater than a specified number per second.

Alerts or alarms are triggered for the number of IPSec IKE requests on the following rules:

- **Enter condition**: Actual number of IPSec IKE requests is greater than the high threshold.
- **Clear condition**: Actual number of IPSec IKE requests is less than the low threshold.

Examples

The following command configures a number of IPSec call requests rejected threshold of 1000 and a low threshold of 800 for a system using the Alarm thresholding model:

```
threshold ipsec-call-req-rej 1000 clear 800
```
threshold ipsec-ike-failrate

Configures a threshold for the percentage of IPSec IKE failures.

Product
HA

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > HA Service Configuration
configure > context context_name > ha-service service_name

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

Syntax Description
threshold ipsec-ike-failrate high_thresh [ clear low_thresh ]
no threshold ipsec-ike-failrate

no
Deletes the alert or alarm.

high_thresh
Default: 0
Specifies the high threshold percentage of IPSec IKE failures per second that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 100.

clear low_thresh
Default: 0
Specifies the low threshold percentage of IPSec IKE failures per second that must be met or exceeded within the polling interval to clear an alert or alarm.
low_thresh is an integer from 0 through 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

Use this command to set an alert or an alarm when the percentage of IPSec IKE failures is equal to or greater than a specified number per second.

Alerts or alarms are triggered for the percentage of IPSec IKE failures on the following rules:

- **Enter condition:** Percentage of IPSec IKE failures is greater than the high threshold.
- **Clear condition:** Percentage of IPSec IKE failures is less than the low threshold.

Examples

The following command configures a percentage of IPSec IKE failures threshold of 1000 and a low threshold of 800 for a system using the Alarm thresholding model:

```
threshold ipsec-ike-failrate 90 clear 80
```
threshold ipsec-ike-failures

Configures a threshold for the total IPSec IKE failures.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HA Service Configuration

```bash
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax Description**

```bash
threshold ipsec-ike-failures high_thresh [ clear low_thresh ]
```

- **no**
  Deletes the alert or alarm.

  - **high_thresh**
    Default: 0
    Specifies the high threshold number of IPSec IKE failures per second that must be met or exceeded within the polling interval to generate an alert or alarm.
    `high_thresh` is an integer from 0 through 1000000.

  - **clear low_thresh**
    Default: 0
    Specifies the low threshold number of call IPSec IKE failures per second that must be met or exceeded within the polling interval to clear an alert or alarm.
    `low_thresh` is an integer from 0 through 1000000.

**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 number of IPSec IKE failures is equal to or greater than a specified number per second.

Alerts or alarms are triggered for the number of IPSec IKE failures on the following rules:

• **Enter condition**: Actual number of IPSec IKE failures is greater than the high threshold.

• **Clear condition**: Actual number of IPSec IKE failures is less than the low threshold.

Examples

The following command configures a number of IPSec IKE failures threshold of 1000 and a low threshold of 800 for a system using the Alarm thresholding model:

```
threshold ipsec-ike-failures 1000 clear 800
```
**threshold ipsec-ike-requests**

Configures a threshold for the total IPSec IKE requests.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HA Service Configuration

```console
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax Description**

```
threshold ipsec-ike-requests high_thresh | clear low_thresh |
no threshold ipsec-ike-requests
```

**no**

Deletes the alert or alarm.

**high_thresh**

Default: 0

Specifies the high threshold number of IPSec IKE requests per second that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 1000000.

**clear low_thresh**

Default: 0

Specifies the low threshold number of call IPSec IKE requests per second that must be met or exceeded within the polling interval to clear an alert or alarm.

*low_thresh* is an integer from 0 through 1000000.

---

**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 number of IPSec IKE requests is equal to or greater than a specified number per second.

Alerts or alarms are triggered for the number of IPSec IKE requests on the following rules:

- **Enter condition**: Actual number of IPSec IKE failures is greater than the high threshold.
- **Clear condition**: Actual number of IPSec IKE failures is less than the low threshold.

Examples

The following command configures a number of IPSec IKE requests threshold of 1000 and a low threshold of 800 for a system using the Alarm thresholding model:

```
threshold ipsec-ike-requests 1000 clear 800
```
threshold ipsec-tunnels-established

Configures a threshold for the total IPSec tunnels established.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HA Service Configuration

*configure > context context_name > ha-service service_name*

Entering the above command sequence results in the following prompt:

*[context_name]*host_name(config-ha-service)#

**Syntax Description**

threshold ipsec-tunnels-established high_thresh [ clear low_thresh ]

no threshold ipsec-tunnels-established

no

Deletes the alert or alarm.

*high_thresh*

Default: 0

Specifies the high threshold number of IPSec tunnels established per second that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 1000000.

*clear low_thresh*

Default: 0

Specifies the low threshold number of call IPSec tunnels established per second that must be met or exceeded within the polling interval to clear an alert or alarm.

*low_thresh* is an integer from 0 through 1000000.

---

**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 number of IPSec tunnels established is equal to or greater than a specified number per second.

Alerts or alarms are triggered for the number of IPSec tunnels established on the following rules:

- **Enter condition**: Actual number of IPSec tunnels established is greater than the high threshold.
- **Clear condition**: Actual number of IPSec tunnels established is less than the low threshold.

Examples

The following command configures a number of IPSec tunnels established threshold of 1000 and a low threshold of 800 for a system using the Alarm thresholding model:

```
threshold ipsec-tunnels-established 1000 clear 800
```
threshold ipsec-tunnels-setup

Configures a threshold for the total IPSec tunnels setup.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HA Service Configuration

```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax Description**

```
threshold ipsec-tunnels-setup high_thres [ clear low_thres ]
no threshold ipsec-tunnels-setup
```

**no**

Deletes the alert or alarm.

**high_thres**

Default: 0

Specifies the high threshold number of IPSec tunnels setup per second that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thres` is an integer from 0 through 1000000.

**clear low_thres**

Default: 0

Specifies the low threshold number of call IPSec tunnels setup per second that must be met or exceeded within the polling interval to clear an alert or alarm.

`low_thres` is an integer from 0 through 1000000.

**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 number of IPSec tunnels setup is equal to or greater than a specified number per second.

Alerts or alarms are triggered for the number of IPSec tunnels setup on the following rules:

- **Enter condition**: Actual number of IPSec tunnels setup is greater than the high threshold.
- **Clear condition**: Actual number of IPSec tunnels setup is less than the low threshold.

Examples

The following command configures a number of IPSec tunnels setup threshold of 1000 and a low threshold of 800 for a system using the Alarm thresholding model:

`threshold ipsec-tunnels-setup 1000 clear 800`
threshold reg-reply-error

Set an alarm or alert based on the number of registration reply errors per HA service.

Product
HA

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > HA Service Configuration
configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:
context_name host_name(config-ha-service)#

Syntax Description
threshold reg-reply-error high_thresh | clear low_thresh |
no threshold reg-reply-error

no
Deleting the alert or alarm.

high_thresh
Default: 0
Specifies the high threshold number of registration reply errors that must be met or exceeded within the polling interval to generate an alert or alarm. high_thesh is an integer from 0 through 100000.

clear low_thresh
Default:0
Specifies the low threshold number of registration reply errors that must be met or exceeded within the polling interval to clear an alert or alarm. low_thesh is an integer from 0 through 100000.

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 number of registration reply errors is equal to or greater than a specified number of calls per second.
Alerts or alarms are triggered for the number of registration reply errors on the following rules:

- **Enter condition**: Actual number of registration reply errors is greater than the high threshold.
- **Clear condition**: Actual number of registration reply errors is less than the low threshold.

**Examples**

The following command configures a registration reply error threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

```
threshold reg-reply-error 1000 clear 500
```
threshold rereg-reply-error

Set an alarm or alert based on the number of re-registration reply errors per HA service.

**Product** HA

**Privilege** Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-ha-service)#
```

**Syntax Description**

```
threshold rereg-reply-error high_thresh [ clear  low_thresh ]
no threshold rereg-reply-error
```

*no*

Deletes the alert or alarm.

*high_thresh*

Default: 0

Specifies the high threshold number of re-registration reply errors that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thresh* is an integer from 0 through 100000.

*clear low_thresh*

Default: 0

Specifies the low threshold number of re-registration reply errors that must be met or exceeded within the polling interval to clear an alert or alarm. *low_thresh* is an integer from 0 through 100000.

---

**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 number of re-registration reply errors is equal to or greater than a specified number of calls per second.
Alerts or alarms are triggered for the number of re-registration reply errors on the following rules:

- **Enter condition**: Actual number of re-registration reply errors is greater than the high threshold.
- **Clear condition**: Actual number of re-registration reply errors is less than the low threshold.

**Examples**

The following command configures a re-registration reply error threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

```
threshold rereg-reply-error 1000 clear 500
```
wimax-3gpp2 interworking

Configures the interworking between WiMAX and 3GPP2 network at HA. This support provides handoff capabilities from 4G to 3G (PDSN) network access and vice-versa.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HA Service Configuration

```bash
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax Description**

| no | default | wimax-3gpp2 interworking |

**no**

Disables the pre-configured interworking between WiMAX and 3GPP2 networks at HA level.

**default**

Configures the **WiMAX-3GPP2 interworking** to default setting: disabled.

**Usage Guidelines**

Use this command to enable/disable the interworking between WiMAX and 3GPP2 network for seamless session continuity.

This functionality provides HA support for both 4G and 3G technology HA (WiMAX HA and PDSN/HA) for handoff from 4G and 3G network access (ASN GW/FA and PDSN/FA) and vice-versa.

**Important**

Use this command in conjunction with the `authentication aaa-distributed-mip-keys required` command.

**Examples**

The following command enables the interworking for a subscriber between WiMAX and 3GPP2 network.

`wimax-3gpp2 interworking`
wimax-3gpp2 interworking
HD Storage Policy Configuration Mode Commands

The HD Storage Policy Configuration Mode is used to configure directory name and file parameters for Diameter record files being stored on the HD storage device.

**Command Modes**

Exec > Global Configuration > HD Storage Policy Configuration

**configure > hd storage-policy policy_name**

Entering the above command sequence results in the following prompt:

[local]host_name(config-hd-storage-policy)#

**Important**

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

- directory, page 1334
- end, page 1335
- exit, page 1336
- file, page 1337
**directory**

Configures the name of the directory on the HD storage drive where Diameter records are stored.

**Product**

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

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > HD Storage Policy Configuration

**Syntax Description**

`directory name dir_name`

`default directory name`

- **default**
  
  Returns the command to its default setting of using the policy name as the directory name.

- **name dir_name**
  
  Specifies the name to be applied to the directory. `dir_name` must be an alphanumeric string of 1 through 63 characters.

  When configured, the actual directory path is:

  `/hd-raid/records/<record-type>/<dir_name>/`

  So if the directory name variable is entered as "sgwpgw", the path is:

  `/hd-raid/records/acr/sgwpgw`

**Usage Guidelines**

Use this command to name a directory on the HD storage drive where Diameter records are to be stored.

**Examples**

The following command configures a directory named `cdr1`:

```
directory name cdr1
```
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>
</table>

| **Privilege** | Security Administrator, Administrator |

| **Syntax Description** | exit |

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

Configures file parameters for Diameter records being stored on the HD storage device.

**Product**

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

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > HD Storage Policy Configuration

```
configure > hd storage-policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-hd-storage-policy)#
```

**Syntax Description**

```
file { format acr { custom1...custom10 } | name { extension string | prefix string } | rotation { record-count num | time-interval sec | volume mb mbytes } } 
default file { format acr | name prefix | rotation { record-count | time-interval | volume } } 
no file { extension | rotation { record-count | time-interval } }

default

Returns the command to the default settings for the specified keywords.

no

Removes the configuration for the specified parameters.

**format acr { custom1...custom10 }**

Default: **custom1**

Specifies the file format used when storing records on the HD storage device. **custom1** is a vendor-specific file format.

**name { extension string | prefix string }**

Specifies a string to be pre-pended or appended to the filenames. By default, the policy name is used for the prefix.
**extension** *string*: Specifies a file extension to append to the filename. *string* must be an alphanumeric string of 1 through 10 characters.

**prefix** *string*: Specifies a file prefix to append to the filename. *string* must be an alphanumeric string of 1 through 63 characters. This parameter replaces the policy name used by default.

**rotation** { **record-count** *num** | **time-interval** *sec** | **volume** *mb** *mbytes** }

specifies the triggers that prompt file rotation on the HD storage drive. All options can be configured and upon reaching any of the thresholds, file rotation is initiated.

**record-count** *num*: File rotation occurs when the number of records reaches the number configured in this keyword. *num* must be an integer from 1000 through 65000. Default = 10000

**time-interval** *sec*: File rotation occurs at time intervals (in seconds) configured by this keyword. *sec* must be an integer from 30 through 86400. Default = 3600 (1 hour)

**volume** *mb** *mbytes**: File rotation occurs when the record volume exceeds the value (in megabytes) configured by this keyword. *mbytes* must be an integer from 2 through 40. Default = 4

**Usage Guidelines**

Use this command to configure file parameters for Diameter records being stored on the HD storage device.

**Examples**

The following command sets the file rotation thresholds for files being stored on the HD storage device:

```
file rotation volume mb 4
file rotation record-count 15000
file rotation time-interval 7200
```

The following command replaces the policy name as the prefix of all files being stored through this policy with the prefix *sgw*:

```
file name prefix sgw
```
HeNB-GW Access Service Configuration Mode Commands

A new service "henbgw-access-service" is defined under Context Configuration Mode to initialize HeNB-GW functionality. This service configuration controls the S1-MME interface for communication between HeNB-GW to HeNB(s). HeNBs connect to the S1-MME bind address configured in this service.

**Command Modes**

Exec > Global Configuration > Context Configuration > HeNBGW-Access Service Configuration

configure > context context_name > henbgw-access-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-henbgw-access-service)#
```

**Important**

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

- associate hembgw-network-service, page 1341
- associate sctp-param-template, page 1343
- associate x2gw-service, page 1344
- bind s1-mme, page 1345
- csg-optimized-paging, page 1346
- end, page 1347
- exit, page 1348
- mme-id, page 1349
- nas-node-selection, page 1351
- plmn, page 1352
- s1-mme ip qos-dscp, page 1353
- s1-mme sctp port, page 1355
- s1u-relay, page 1356
- security-gateway, page 1357
- timeout, page 1359
associate henbgw-network-service

Associates a previously configured HeNB-GW Network service to the this HeNB-GW Access service. An HeNB-GW Network service must be configured in Context Configuration mode before using this configuration.

**Product**

HeNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HeNBGW-Access Service Configuration

configure > context context_name > henbgw-access-service service_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-henbgw-access-service)#

**Syntax Description**

`associate henbgw-network-service svc_name [context context_name]`

`no associate henbgw-network-service`

`no`

Removes the associated HeNB-GW Network service from this HeNB-GW Access service configuration.

`svc_name`

Identifies the name of the pre-configured HeNB-GW Network service to associate with this HeNB-GW Access service.

`svc_name` is an alphanumeric string of 1 through 63 characters.

`context context_name`

Identifies the name of the context to which the HeNBGW service belongs.

`context_name` is an alphanumeric string of 1 through 79 characters.

**Usage Guidelines**

Use this command to bind/associate a pre-configured HeNB-GW Network service to the this HeNB-GW Access service. The HeNB-GW Network service can be configured in Context configuration mode. The associate configuration is used to establish associations with other helper services in general.
Examples

Following command associates an HeNB-GW Network service named *henb-network* with specific HeNB-GW Access service.

```
associate henbgw-network-service henb-network
```
**associate sctp-param-template**

Associates a previously configured SCTP Parameter Template to the this HeNB-GW Access service. A SCTP Parameter Template must be configured globally before using this configuration.

**Product**

HeNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HeNBGW-Access Service Configuration

```
configure > context context_name > henbgw-access-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-henbgw-access-service)#
```

**Syntax Description**

- `associate sctp-param-template` *template_name*
- `no associate sctp-param-template`

- **no**
  
  Removes the associated SCTP Parameter Template from this HeNB-GW Access service configuration.

- **template_name**
  
  Identifies the name of the pre-configured SCTP Parameter Template to associate with this HeNB-GW Access service.

  *template_name* is an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to bind/associate a pre-configured SCTP Parameter Template to the this HeNB-GW Access service. The SCTP Parameter Template can be configured global mode. The associate configuration is used to establish associations with other helper services in general.

**Examples**

Following command associates an SCTP Parameter Template named *sctp_tmpl* with specific HeNB-GW Access service.

```
associate sctp-param-template sctp_tmpl
```
**associate x2gw-service**

This command Configures x2gw-service for this HENBGW ACCESS service.

**Product**

HeNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HeNBGW-Access Service Configuration

`configure > context context_name > henbgw-access-service service_name`

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-henbgw-access-service)#
```

**Syntax Description**

`associate x2gw-service` associate_x2gw-service_name context context_name

`no associate x2gw-service`

**no**

Removes the association of x2gw-service interface from this HeNB-GW Access service configuration.

`associate_x2gw-service_name`

Name of the service that will be used by this HENBGW ACCESS service to associate with. Name of the string is an alphanumeric, 1 through 63 characters.

`context_name`

Name of the context that will be used by this HENBGW ACCESS service to associate with. Name of the string is an alphanumeric, 1 through 79 characters.

**Usage Guidelines**

Use this command to associate x2gw-service with HeNBGW Access service.

**Examples**

Following command associates an x2gw-service with specific HeNB-GW Access service with name gate123:

`associate x2gw-service gate123 context ctx1`
bind s1-mme

Binds the pre configured HeNB-GW Access Service to the IP address of the S1-MME interface.

**Product**

HeNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HeNBGW-Access Service Configuration

configure > context context_name > henbgw-access-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-henbgw-access-service)#

**Syntax Description**

```
bind s1-mme {ipv4-address | ipv6-address} ip_addr max-subscribers max_sub

no

no bind s1-mme
```

- **ip_addr**
  
  Identifies the IP address of the S1-MME interface to associate with this HeNB-GW Access service.
  
  `addr_val` must be entered in the IPv4 (dotted decimal notation) or IPv6 (`/` notation).

- **max-subscribers max_sub**
  
  Configures the maximum number of subscribers HENBGW ACCESS service can support.
  
  `max_sub` is an integer ranging from 0 through 4000000.

**Usage Guidelines**

Use this command to bind the pre configured IPv4 address of the S1-MME interface to the HeNB-GW Access Service.

**Examples**

Following command binds the S1-MME interface having 192.68.111.61 IP address with specific HeNB-GW Access service.

```
bind s1-mme ipv4-address 192.68.111.61 max-subscribers 20
```
csg-optimized-paging

Configures the support for Paging Optimization Function on this HeNB-GW Access service based on the CSG-ID in the Paging message

Product
HeNB-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > HeNBGW-Access Service Configuration

configure > context context_name > henbgw-access-service service_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-henbgw-access-service)#

Syntax Description
no | csg-optimized-paging

no
Removes the paging optimization function from this HeNB-GW Access service configuration.

Usage Guidelines
Use this command to enable the CSG-ID based paging optimization function to the HeNB-GW Access Service.

Examples
Following command enables the CSG-ID based paging optimization on a specific HeNB-GW Access service.
csg-optimized-paging
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.
mme-id

Configures the MME ID for this HeNB-GW Access service. For this configuration, MME Group ID and MME Code has to be configured.

**Product**
HeNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HeNBGW-Access Service Configuration
configure > context context_name > henbgw-access-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-henbgw-access-service)#
```

**Syntax Description**

```
mme-id [group-id mme_group_id] mme-code mme_code
no mme-id
```

*no*
Removes the configured MME ID from this HeNB-GW Access service configuration.

*group-id mme_group_id*
Identifies the MME Group ID which must be entered as an integer between 32768 and 65535.

*mme-code*
Identifies the MME code which is again an integer value between 0 and 255.

**Usage Guidelines**
Use this command to configure the MME Identifier which includes the MME Group ID and MME Code for this HeNB-GW Access service. MME ID configuration is required, because it is the same ID which HeNB-GW sends in response messages to HeNBs.

⚠️ **Caution**
Changing the MME ID is a disruptive operation. HeNB-GW service is restarted on any change.
Examples

Following command configures 32770 as the MME Group ID and 105 as MME code on a specific HeNB-GW Access service.

```
mme-id group-id 32770 mme-code 105
```
**nas-node-selection**

This command configures the selection of logical eNodeB/ MME based on TAI or Global eNodeB id.

**Product**

HeNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HeNBGW-Access Service Configuration

```plaintext
configure > context context_name > henbgw-access-service service_name
```

Entering the above command sequence results in the following prompt:

```plaintext
[context_name]host_name(config-henbgw-access-service)#
```

**Syntax Description**

```plaintext
nas-node-selection { global-eNodeB-id-based | tai-based }
```

**Important**

This command is functional for 8 logical eNodeBs only.

- **global-eNodeB-id-based**
  
  Specifies the Global eNodeB id Based selection.

- **tai-based**
  
  Specifies the TAI based selection. This is the default option.

**Usage Guidelines**

Use this command to configure the selection of logical eNodeB/ MME based on TAI or Global eNodeB id.

**Examples**

Following command configures the selection of logical eNodeB/ MME based on Global eNodeB id.

```plaintext
nas-node-selection global-eNodeB-id-based
```
plmn

Configures the PLMN identifier for this HeNB-GW Access service. Other identifiers that are configured along with the PLMN include the MCC and MNC values too.

Product

HeNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HeNBGW-Access Service Configuration
configure > context context_name > henbgw-access-service service_name

Entering the above command sequence results in the following prompt:

(context_name)host_name(config-henbgw-access-service)#

Syntax Description

| no | plmn id mcc mcc_val mnc mnc_val |

| no |

Removes the existing PLMN configuration from this HeNB-GW Access service configuration.

mcc_val

Identifies the mobile country code for the IMSI which must be entered between 100 and 999 as a string of size 3.

mnc_val

Identifies the Mobile Network Code which is a value between 00 and 999, as a string of size 2 to 3.

Usage Guidelines

Use this command to configure the PLMN related configuration for this HeNB-GW Access service.

Examples

Following command configures 123 as the MCC value and 456 as the MNC value as part of the PLMN configuration for this HeNB-GW Access service.

plmn id mcc 123 mnc 456
s1-mme ip qos-dscp

This command configures the quality of service (QoS) differentiated service code point (DSCP) marking for IP packets sent out on the S1-MME interface, from the HeNB-GW to the HeNB(s).

**Product**
HeNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HeNBGW-Access Service Configuration

```
configure > context context_name > henbgw-access-service service_name
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-henbgw-access-service)#
```

**Syntax Description**

```
s1-mme ip qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }
```

```
default s1-mme ip qos-dscp
```

```
qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }
```

Default: \texttt{af11}

Specifies the DSCP for the specified QoS traffic pattern. \texttt{qos-dscp} can be configured to any one of the following:

- \texttt{af11}: Assured Forwarding 11 per-hop-behavior (PHB)
- \texttt{af12}: Assured Forwarding 12 PHB
- \texttt{af13}: Assured Forwarding 13 PHB
- \texttt{af21}: Assured Forwarding 21 PHB
- \texttt{af22}: Assured Forwarding 22 PHB
- \texttt{af23}: Assured Forwarding 23 PHB
- \texttt{af31}: Assured Forwarding 31 PHB
- \texttt{af32}: Assured Forwarding 32 PHB
- \texttt{af33}: Assured Forwarding 33 PHB
- \texttt{af41}: Assured Forwarding 41 PHB
- \texttt{af42}: Assured Forwarding 42 PHB
af43: Assured Forwarding 43 PHB
be: Best effort forwarding PHB
cs0: Designates use of Class Selector 0 PHB. This is same as DSCP Value BE
cs1: Designates use of Class Selector 1 PHB
cs2: Designates use of Class Selector 2 PHB
cs3: Designates use of Class Selector 3 PHB
cs4: Designates use of Class Selector 4 PHB
cs5: Designates use of Class Selector 5 PHB
cs6: Designates use of Class Selector 6 PHB
cs7: Designates use of Class Selector 7 PHB
ef: Expedited forwarding PHB

default
Specifies the default DSCP for the specified QoS traffic pattern. The default value of DSCP is af11.

Usage Guidelines
DSCP levels can be assigned to specific traffic patterns to ensure that data packets are delivered according to the precedence with which they are tagged. The diffserv markings are applied to the IP header of every subscriber data packet transmitted over the S1-MME interface(s).

Examples
The following command sets the DSCP-level for data traffic sent over the S1-MME interface to af12:
s1-mme ip qos-dscp af12
s1-mme sctp port

This command configures the local Stream Control Transmission Protocol (SCTP) port used for binding the SCTP socket to communicate with the HeNBs over S1-MME interface.

**Product**

HeNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HeNBGW-Access Service Configuration

configure > context context_name > henbgw-access-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-henbgw-access-service)#
```

**Syntax Description**

- `s1-mme sctp port port_num`
- `default s1-mme sctp port`

**Syntax Description**

- `s1-mme sctp port port_num`
  - `default`
    - Sets the SCTP port to the default value of 36412 to communicate with the HeNBs using S1-MME interface.
  - `port_num`
    - Specifies the SCTP port number to communicate with the HeNBs using S1-MME interface as an integer from 1 through 65535. Default: 36412

**Usage Guidelines**

Use this command to assign the SCTP port with SCTP socket to communicate with the HeNB using S1AP. Only one SCTP port can be associated with one MME service.

**Examples**

The following command sets the default SCTP port number 699 for to interact with Home eNodeB using S1AP on S1-MME interface:

```
default s1-mme sctp port
```
s1u-relay

This command configures the S1-U Relay service for the HeNB-GW Access service. The user enters in the S1-U Relay configuration mode using this command.

**Product**
HeNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HeNBGW-Access Service Configuration
configure > context context_name > henbgw-access-service service_name

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-henbgw-access-service)#
```

**Syntax Description**
| no | s1u-relay |

no

Removes the S1-U Relay service function from this HeNB-GW Access service configuration.

**Usage Guidelines**
Use this command to enable the S1-U Relay service function to the HeNB-GW Access Service. S1-U relay service is disabled by default.

**Examples**
Following command enables the S-U Relay service on a specific HeNB-GW Access service.

```
s1u-relay
```
security-gateway

This command configuration defines the IPv4 address to be used as the connection point for establishing IKEv2 sessions and specify the crypto template to use for the security gateway (SeGW) for the HeNB-GW Access service.

**Product**

HeNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HeNBGW-Access Service Configuration

```plaintext
configure > context context_name > henbgw-access-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-henbgw-access-service)#
```

**Syntax Description**

```plaintext
security gateway bind ipv4-address ipv4_addr crypto-template template_name [ context ctxt_name ]
no security gateway bind
```

**no**

Removes the security gateway related configuration associated with this HeNB-GW Access service configuration.

**ipv4_addr**

Identifies the security gateway address used for this HeNB-GW Access service. It must be entered in dotted decimal notation.

**template_name**

Identifies the crypto template name for security gateway for this HeNB-GW Access service. It must be entered a string of size 0 to 127.

**ctxt_name**

Identifies the context name where crypto template is defined for this HeNB-GW Access service. It must be entered a string of size 1 to 79.

**Usage Guidelines**

Use this command to configure the security gateway (SeGW) related configuration for this HeNB-GW Access service. SeGW configuration includes crypto template configuration as part of IPSec settings, therefore if the
crypto-template is defined in a different context than the current HeNB-GW Access service, the context name has to be specified.

**Examples**

Following command configures 192.68.111.15 as the SeGW address and crypto-temp as the crypto template name on a specific HeNB-GW Access service.

```
security gateway bind ipv4-address 192.68.111.15 crypto-template crypto-temp
```
timeout

Configures the maximum duration of the session for this HeNB-GW Access service, in seconds, before system automatically reports/terminates the session.

**Product**

HeNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HeNBGW-Access Service Configuration

`configure > context context_name > henbgw-access-service service_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-henbgw-access-service)#`

**Syntax Description**

`timeout long-duration dur action {detection | disconnect}

no timeout long-duration`

**no**

Removes the currently setup maximum duration of session.

`dur`

Specifies the number of seconds for the session's timeout duration, before system automatically terminates the session or a defined action is to be taken.

`dur` is an integer from 1 through 2147483647. Default: 0

**Usage Guidelines**

Use this command to configure the maximum duration of the session, in seconds, before system automatically reports/terminates the session of this HeNB-GW Access service.

**Examples**

The following command sets the timeout duration of 60 seconds for a particular HeNB-GW Access service and disconnect the session:

`timeout long-duration 60 action disconnect`
timeout
HeNBGW Qci Dscp Mapping Table Configuration Mode Commands

Creates HeNBGW Qci Dscp Mapping Table configuration mode.

**Command Modes**

```
Exec > LTE Policy > HENBGW QCI DSCP Mapping Table Configuration
configure > lte-policy > henbgw qci-dscp-mapping-table table_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name (config-henbgw-qci-dscp-mapping-table) #
```

- dscp-marking-default, page 1362
- end, page 1364
- exit, page 1365
- qci, page 1366
**dscp-marking-default**

This command is used to configure default dscp-marking value for qci.

**Product**

HeNBGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

`Exec > LTE Policy > HENBGW QCI DSCP Mapping Table Configuration`  
`configure > lte-policy > hcnbgw qci-dscp-mapping-table table_name`

Entering the above command sequence results in the following prompt: 

```
{context_name}@host_name(config-henbgw-qci-dscp-mapping-table)#
```

**Syntax Description**

```
dscp-marking-default {af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef} 
no dscp-marking-default
```

**dscp-marking-default**

- **af11**: Assured Forwarding 11 per-hop-behavior (PHB)  
- **af12**: Assured Forwarding 12 PHB  
- **af13**: Assured Forwarding 13 PHB  
- **af21**: Assured Forwarding 21 PHB  
- **af22**: Assured Forwarding 22 PHB  
- **af23**: Assured Forwarding 23 PHB  
- **af31**: Assured Forwarding 31 PHB  
- **af32**: Assured Forwarding 32 PHB  
- **af33**: Assured Forwarding 33 PHB  
- **af41**: Assured Forwarding 41 PHB

Disables the configuration of default dscp-marking value for qci.

```
dscp-marking-default {af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef} 
```

Specifies the default dscp-marking value for qci. 

**dscp-marking-default** designates the use of one of the following as default value:

- **af11**: Assured Forwarding 11 per-hop-behavior (PHB)  
- **af12**: Assured Forwarding 12 PHB  
- **af13**: Assured Forwarding 13 PHB  
- **af21**: Assured Forwarding 21 PHB  
- **af22**: Assured Forwarding 22 PHB  
- **af23**: Assured Forwarding 23 PHB  
- **af31**: Assured Forwarding 31 PHB  
- **af32**: Assured Forwarding 32 PHB  
- **af33**: Assured Forwarding 33 PHB  
- **af41**: Assured Forwarding 41 PHB
af42: Assured Forwarding 42 PHB
af43: Assured Forwarding 43 PHB
be: Best effort forwarding PHB. This is same as DSCP value CS0.
cs0: Class Selector 0 PHB. This is same as DSCP Value BE.
cs1: Class Selector 1 PHB.
cs2: Class Selector 2 PHB.
cs3: Class Selector 3 PHB.
cs4: Class Selector 4 PHB.
cs5: Class Selector 5 PHB.
cs6: Class Selector 6 PHB.
cs7: Class Selector 7 PHB.
ef: Expedited forwarding PHB

Usage Guidelines
Use this command to configure default dscp-marking value for qci.

Examples
Following command configures cs6 as the default dscp-marking value for qci:
```
dscp-marking-default cs6
```
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

dec

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.
qci

This command is used to configure qci value for HENBGW.

Product

HENBGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > LTE Policy > HENBGW QCI DSCP Mapping Table Configuration

campaign > lte-policy > hnwbgw qci-dscp-mapping-table table_name

Entering the above command sequence results in the following prompt:

<context_name>host_name(config-henbgw-qci-dscp-mapping-table)#

Syntax Description

qci qci_value dscp-marking { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }

no qci qci_value

no

Disables the configuration of qci value for HENBGW.

qci_value

This is an integer between 0 and 255.

dscp-marking { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }

Configures dscp-marking value for qci. dscp-marking designates the use of one of the following as qci value:

af11: Assured Forwarding 11 per-hop-behavior (PHB)
af12: Assured Forwarding 12 PHB
af13: Assured Forwarding 13 PHB
af21: Assured Forwarding 21 PHB
af22: Assured Forwarding 22 PHB
af23: Assured Forwarding 23 PHB
af31: Assured Forwarding 31 PHB
af32: Assured Forwarding 32 PHB
af33: Assured Forwarding 33 PHB
af41: Assured Forwarding 41 PHB
af42: Assured Forwarding 42 PHB
af43: Assured Forwarding 43 PHB
be: Best effort forwarding PHB. This is same as DSCP value CS0.
cs0: Class Selector 0 PHB. This is same as DSCP Value BE.
cs1: Class Selector 1 PHB.
cs2: Class Selector 2 PHB.
cs3: Class Selector 3 PHB.
cs4: Class Selector 4 PHB.
cs5: Class Selector 5 PHB.
cs6: Class Selector 6 PHB.
cs7: Class Selector 7 PHB.
ef: Expedited forwarding PHB

Usage Guidelines
Use this command to configure qci value for HENBGW.

Examples
Following command configures qci value as 5 with dscp marking as af11:
qci 5 dscp-marking af11
HeNB-GW Network Service Configuration Mode

Commands

A new service "henbgw-network-service" is defined under the Context configuration mode in order to support HeNB-GW functionality. This service configuration controls the S1-MME interface functionality between HeNB-GW and MME node.

Command Modes

Exec > Global Configuration > Context Configuration > HeNBGW-Network Service Configuration

configure > context context_name > henbgw-network-service service_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-henbgw-network-service)#

Important

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

- anr-info-retrieval, page 1370
- associate sctp-param-template, page 1371
- default-paging-drx, page 1372
- end, page 1373
- exit, page 1374
- logical-enb, page 1375
- paging-rate-control, page 1377
- public-warning-system, page 1379
- pws, page 1380
- s1ap-max-retransmissions, page 1382
- s1ap-retransmission-timeout, page 1383
anr-info-retrieval

This command enables the HeNB-GW to intercept and respond to the Automatic Neighbor Relation (ANR) related SON messages with the requested information.

**Product**

HeNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HeNBGW-Network Service Configuration

configure > context context_name > henbgw-network-service service_name

Entering the above command sequence results in the following prompt:

{(context_name)host_name (config-henbgw-network-service) #

**Syntax Description**

| no | default | anr-info-retrieval |

no

Removes the ANR information retrieval related function from this HeNB-GW Network service configuration.

default

Sets/Restores the default value assigned for the ANR information retrieval related function from the configured HeNB-GW Network service.

**Usage Guidelines**

Use this command to enable the ANR information retrieval function to the HeNB-GW Network Service.

**Examples**

Following command enables the ANR information retrieval function on a specific HeNB-GW Network service.

anr-info-retrieval
associate sctp-param-template

Associates a previously configured SCTP Parameter Template to the this HeNB-GW Network service. A SCTP Parameter Template must be configured globally before using this configuration.

**Product**
HeNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HeNBGW-Access Service Configuration

```plaintext
configure > context context_name > he nbgw-access-service service_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-he nbgw-access-service)#
```

**Syntax Description**

- `associate sctp-param-template template_name`
- `no associate sctp-param-template`

**no**
Removes the associated SCTP Parameter Template from this HeNB-GW Network service configuration.

**template_name**
Identifies the name of the pre-configured SCTP Parameter Template to associate with this HeNB-GW Network service.

*template_name* is an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**
Use this command to bind/associate a pre-configured SCTP Parameter Template to the this HeNB-GW Network service. The SCTP Parameter Template can be configured global mode. The associate configuration is used to establish associations with other helper services in general.

**Examples**
Following command associates an SCTP Parameter Template named *sctp_tmpl* with specific HeNB-GW Network service.

```plaintext
associate sctp-param-template sctp_tmpl
```
default-paging-drx

This command is used to configure the Default paging DRX value that is sent to the MME(s) in the S1 SETUP request message.

**Product**
HeNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HeNBGW-Network Service Configuration
`configure > context context_name > henbgw-network-service service_name`

Entering the above command sequence results in the following prompt:

```
<context_name>@host_name(config-henbgw-network-service) #
```

**Syntax Description**

```
default-paging-drx { v128 | v256 | v32 | v64 }
default default-paging-drx
```

**default**
Sets/Restores the default value assigned for Default-Paging-DRX for the configured HeNB-GW Network service.

```
default-paging-drx { v128 | v256 | v32 | v64 }
```

Any one of the following DRX values can be configured:

- v128: Designates use of Paging DRX v128.
- v256: Designates use of Paging DRX v256.
- v32: Designates use of Paging DRX v32.
- v64: Designates use of Paging DRX v64.

**Usage Guidelines**
Use this command to configure the Default Paging DRX value for this HeNB-GW Network service.

**Examples**
Following command configures v256 as the Default Paging DRX value on a specific HeNB-GW Network service.
```
default-paging-drx v256```
end

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

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HeNBGW-Network Service Configuration

configure > context context_name > henbgw-network-service service_name

Entering the above command sequence results in the following prompt:

{context_name} host_name (config-henbgw-network-service) #

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

**Command Modes**

Exec > Global Configuration > Context Configuration > HeNBGW-Network Service Configuration

configure > context context_name > henbgw-network-service service_name

Entering the above command sequence results in the following prompt:

{context_name}host_name (config-henbgw-network-service) #

**Syntax Description**

exit

**Usage Guidelines**

Use this command to return to the parent configuration mode.
**logical-enb**

This command enables the configuration of one or more logical eNodeBs within the HeNB-GW.

**Product**

HeNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HeNBGW-Network Service Configuration

configure > context context_name > henbgw-network-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name] host_name (config-henbgw-network-service) #
```

**Syntax Description**

```
logical-enb global-enb-id plmn id mcc mcc_val mnc mnc_val { home-enb-id henb_id | macro-enb-id menb_id } [ -noconfirm ]
no logical-enb global-enb-id plmn id mcc mcc_val mnc mnc_val { home-enb-id henb_id | macro-enb-id menb_id }
```

**no**

Removes the configured logical eNodeB from this HeNB-GGW Network service configuration.

**mcc mcc_val**

Identifies the mobile country code for the IMSI which must be entered between 100 and 999, as a string of size 3.

**mnc mnc_val**

Identifies the Mobile Network Code which is a value between 00 and 999, as a string of size 2 to 3.

**home-enb-id henb_id**

Identifies the Home eNodeB ID which is an integer from 1 to 268435455.

**macro-enb-id menb_id**

Identifies the Macro eNodeB ID which is again an integer value between 1 and 1048575.

**-noconfirm**

Creates a new HeNB-GW network service without prompting for confirmation.
Usage Guidelines

Use this command for the configuration of one or more logical eNodeBs within the HeNB-GW. The Logical eNodeB configuration can be used to support load balancing within a pool of TAI (i.e. Multiple logical eNodeBs can service calls connecting from a specific set of TAI). It can also be used to create and support disjoint serving areas, i.e., each logical eNodeB will serve a different set of TAI.

At least one logical eNodeB configuration is required to START an HeNB-GW Network service.

Caution

Deleting or modifying any of the parameters for a fully configured logical eNodeB is a disruptive operation. It will result in the termination of SCTP connections to MMEs from that logical eNodeB.

Examples

Following command configures a logical eNodeB having Home eNodeB ID as 1000 on a specific HeNB-GW Network service.

```
logical-enb global-enb-id plmn id mcc 123 mnc 456 home-enb-id 1000
```
**paging-rate-control**

This command is used to configure the Paging-Rate-Control which determines the maximum number of paging messages per second which an HeNB-GW can handle received from the MME(s).

**Product**

HeNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HeNBGW-Network Service Configuration

*configure > context context_name > henbgw-network-service service_name*

Entering the above command sequence results in the following prompt:

/context_name/host_name/config-henbgw-network-service#

**Syntax Description**

- `paging-rate-control number_of_msg`
- `no paging-rate-control`
- `no`

Removes the configured rate of paging messages from this HeNB-GW Network service configuration.

- `number_of_msg`

Identifies the number of paging messages to be handled by the HeNBGW service per second. This number must be entered as an integer between 1 and 65535 (min 1 and max 65535).

**Usage Guidelines**

Use this command to configure the number of paging messages per second to be handled by this HeNB-GW Network service. MME ID configuration is required, because it is the same ID which HeNB-GW sends in response messages to HeNBs.

This parameter is not part of logical-enb configuration and therefore it would include paging messages received from all the MMEs to which its HeNB-GW is connected on the network side.

- `Important` Paging messages exceeding the configured rate are dropped. Total Paging and Dropped Statistics is updated in the logs.
Examples

Following command configures 32770 as the number of paging messages per second to be handled on a specific HeNB-GW Network service.

`paging-rate-control 32770`
**public-warning-system**

This command enables / disables the Public warning system.

**Product**

HeNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HeNBGW-Network Service Configuration

`configure > context context_name > henbgw-network-service service_name`

Entering the above command sequence results in the following prompt:

`{context_name}@host_name (config-henbgw-network-service) #`

**Syntax Description**

`[no] public-warning-system`

- **no**
  
  Disables the Public warning system.

**Usage Guidelines**

Use this command to enable / disable the Public warning system.

**Examples**

Following command disables the Public warning system:

`no public-warning-system`
**pws**

This command sets values for parameters related to public warning system feature.

**Product**
HeNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HeNBGW-Network Service Configuration

```
configure > context context_name > henbgw-network-service service_name
```

Entering the above command sequence results in the following prompt:

```
(context_name)host_name (config-henbgw-network-service) #
```

**Syntax Description**

```
pws { kill-request-timeout kill_req_timeout_seconds | restart-indication-timeout restart_ind_timeout_seconds | warning-request-timeout warn_req_timeout_seconds } default pws { kill-request-timeout | restart-indication-timeout | warning-request-timeout }

default
```

Configures the default value to kill request timeout and warning request timeout of public warning system feature.

**kill-request-timeout kill_req_timeout_seconds**
Configures the Kill Request timeout value in seconds.

```
kill_req_timeout_seconds is an integer from 1 through 65535.
```

**restart-indication-timeout restart_ind_timeout_seconds**
Configures Restart Indication timeout value in seconds.

```
restart_ind_timeout_seconds is an integer from 1 through 65535.
```

**warning-request-timeout warn_req_timeout_seconds**
Configures the Warning request timeout value in seconds.

```
warn_req_timeout_seconds is an integer from 1 through 65535.
```

**Usage Guidelines**
Use this command to set the values for parameters related to public warning system feature for this HeNB-GW Network service.
Examples

Following command configures the Warning request timeout value to 100 seconds.

```plaintext
pws warning-request-timeout 100
```
s1ap-max-retransmissions

This command configures the number of times node level S1AP message is retransmitted towards MME.

**Product**
HeNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HeNBGW-Network Service Configuration

configure > context context_name > he nbgw-network-service service_name

Entering the above command sequence results in the following prompt:

(context_name)host_name(config-henbgw-network-service)#

**Syntax Description**

s1ap-max-retransmissions number_of_retries
default s1ap-max-retransmissions

default

Configures the default number of S1AP retransmissions for this HeNB-GW Network service configuration. Default number of retransmissions is 4.

**Usage Guidelines**

Use this command to configure the maximum number of Node level S1AP retransmissions for this HeNB-GW Network service.

**Caution**

Configuring s1ap-max-retransmissions to 0 will disable the S1AP retransmission support.

**Examples**

Following command configures default (which is also 4) S1AP retransmission on a specific HeNB-GW Network service.

default s1ap-max-retransmissions
s1ap-retransmission-timeout

This command configures the timeout interval to support Node Level S1AP retransmissions if there in no response received from the peer (MME).

Product
HeNB-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > HeNBGW-Network Service Configuration

configure > context context_name > henbgw-network-service service_name

Entering the above command sequence results in the following prompt:

{context_name} host_name (config-henbgw-network-service) #

Syntax Description
- s1ap-retransmission-timeout number_of_secs
- default s1ap-retransmission-timeout

- default
Configures the default S1AP retransmission timeout for this HeNB-GW Network service configuration. Default retransmission timeout is 60 seconds.

- number_of_secs
Identifies the number seconds as the S1AP retransmission timeout to be configured. This number must be entered as an integer between 1 and 600.

Usage Guidelines
Use this command to configure the timeout interval to support Node Level S1ap retransmissions for this HeNB-GW Network service.

Examples
Following command configures 100 as the S1AP retransmission timeout on a specific HeNB-GW Network service.

s1ap-retransmission-timeout 100
s1ap-retransmission-timeout
HLR Configuration Mode Commands

The HLR Configuration Mode is a sub-mode derived from the MAP Configuration Mode which controls the MAP service configuration. It is the MAP service that provides the application-layer protocol support used to connect the HLR to other nodes in the network such as the SGSN.

The HLR Configuration Mode provides the commands and parameters to configure the home location register (HLR) node that is the database containing the subscriber profile and connection information for a specific GPRS/UMTS core network.

**Command Modes**

Exec > Global Configuration > Context Configuration > MAP Service Configuration > HLR Configuration

`configure > context context_name > map-service service_name > hlr`

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-map-service-service_name-hlr)#
```

**Important**

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

- acn-version-retention, page 1386
- end, page 1387
- exit, page 1388
- imsi, page 1389
- policy routing, page 1391
- release-compliance, page 1392
acn-version-retention

This command configures the ACN version retention method.

Product
SGSN

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > MAP Service Configuration > HLR Configuration
configure > context context_name > map-service service_name > hlr

Entering the above command sequence results in the following prompt:
{context_name}host_name(config-map-service-service_name-hlr)#

Syntax Description
acn-version-retention { per-imsi-prefix | per-subscriber }
default acn-version-retention

default
Returns the configuration to the default value: retains the version information per IMSI prefix.

per-imsi-prefix
Retain ACN version information, for communication with the HLR, on a per IMSI prefix basis.

per-subscriber
Retain ACN version information, for communication with the HLR, on a per subscriber basis.

Usage Guidelines
By default, the SGSN sends ACN version 3 SAI (service area identity) to the HLR. If the SGSN receives an error message indicating that the HLR does not support that version, then the SGSN tries again with an ACN version 2 SAI. Next time the SGSN communicates with that HLR, it retains that version information and version persists based on the IMSI prefix.

Use this command to enable the SGSN to retain version according to subscriber.

Examples
Configure the SGSN to retain version information according to the IMSI prefix:
default acn-version-retention
end

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

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax Description

end

Usage Guidelines

Return to the Exec mode.
exit

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

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax Description**
exit

**Usage Guidelines**
Return to the MAP Service configuration mode.
This command sets up IMSI (International Mobile Subscriber Identity)-based configuration. The IMSI prefix includes the mobile country code (MCC) and the mobile network code (MNC).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > MAP Service Configuration > HLR Configuration
configure > context context_name > map-service service_name > hlr

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-map-service-service_name-hlr)#
```

**Syntax Description**

```
[ no ] imsi { any | starts-with prefix_number } { imsi | sgsn-source-address-format point-code-ssn | source-ssn ssn } | isdn isdn_number | mobile-global-title mgt_number | max-gt-address-len max_gt_address | point-code pt-code }
```

- **no**
  Removes the imsi-prefix definition from the configuration.

- **any**
  Configures acceptance of any IMSI prefix.

- **start-with prefix_number**
  Selects IMSI prefix-based routing.
  *prefix_number* is a string of up to 15 integers.

- **imsi**
  Enables configurable default behavior for routing.
  Entering **imsi** with the **any** keyword preserves the default behavior and the E.212 address is used as a destination address and the MAP request will be sent towards the HLR.
  If this keyword is not used with the **any** keyword, then the MAP request will be rejected.
isdn isdn_number
Defines the E.164 number of the HLR.
isdn_number is a string of integers, up to 15.

mobile-global-title mgt_number [ max-gt-address-len max_gt_address_length ]
Defines the mobile global title address that the MCC/MNC portion of the IMSI will be converted to. If the maximum GT address length is specified (optional) and if the length of the MGT string is greater than defined, then the least significant digits will be omitted.
mgt_number is a string of digits, up to 18 digits in length.
max_gt_address is an integer from 1 to 32.

point-code pt-code source-ssn ssn
Defines the point code for the HLR.
pt-code is a string of digits, up to 11; SS7 format preferred.

sgsn-source-address-format point-code-ssn
Selects HLR call process according to SCCP calling party address of the SGSN. This will be filled at MAP level, including the ITU point code address.

source-ssn ssn
Defines the SSN of the source that will be used for the call filtering.
ssn: Must be an integer from 1 to 255.

Usage Guidelines
Routing will be done according to IMSI parameters configured with this command or according to the mobile global title address (replacing the MCC/MNC portion of the IMSI) is so specified.

Examples
imsi starts-with 3 isdn 123456789 sgsn-source-address-form at point-code-ssn
policy routing

This command configures the policy for the routing of MAP messages. If this command is not configured or disabled (with the default keyword), then routing is done according to the configuration of the IMSI parameters.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > MAP Service Configuration > HLR Configuration

```
configure > context context_name > map-service service_name > hlr
```

Entering the above command sequence results in the following prompt:

```
{context_name} host_name (config-map-service-service_name-hlr) #
```

**Syntax Description**

policy routing { hlr-isdn | ms-isdn }
default policy routing
no policy routing

- **default**
  Resets the policy routing to the system default, disabled.

- **no**
  Removes the policy routing configuration from the system.

- **hlr-isdn**
  Selects HLR-ISDN based routing.

- **ms-isdn**
  Selects mobile station (MS)-ISDN based routing.

**Usage Guidelines**
Use this command to set the policy for routing MAP messages.

**Examples**

```
policy routing hlr-isdn
```
release-compliance

Enables/disables the sending of EPS information in the Update GPRS Location Request message to the HLR.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > MAP Service Configuration > HLR Configuration

```
configure > context context_name > map-service service_name > hlr
```

Entering the above command sequence results in the following prompt:

```
<context_name>host_name>(config-map-service-service_name-hlr)#
```

**Syntax Description**

- `release-compliance release-8`
- `no release-compliance`

`release-compliance release-8`

Enables the sending of EPS information in the UGL Request message to the HLR. This setting sets the 3GPP release compliance to *Release 8 and above*.

`no release-compliance`

Disables the sending of EPS information in the UGL Request message to the HLR. This command sets the 3GPP release compliance setting to *Pre-release 8*. This is the default setting.

**Usage Guidelines**

Use this command to enable or disable the sending of EPS information in the UGL Request message to the HLR.

Operators can use the `show map-service all` command to view the current 3GPP release compliance setting.

**Examples**

This command enables the sending of EPS information in the UGL Request message to the HLR.

`release-compliance release-8`
HNB-GW Global Configuration Mode Commands

The 3G UMTS Home-NodeB Gateway Global Configuration Mode provides the global configurations for multiple HNB-GW services on a chassis to manage the access to the UMTS core network in a 3G UMTS network through a Femto node. This configuration mode is supported from StarOS 14.0 onward.

**Command Modes**

```
Exec > Global Configuration > HNB-GW Global Configuration
configure > hnb-gw-global
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-hnggw-global)#
```

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

- access-control-db, page 1394
- end, page 1396
- exit, page 1397
- paging hybrid-hnb, page 1398
- paging open-hnb, page 1400
- scgp, page 1401
- session-collocation, page 1404
- tmsf-timer, page 1405
access-control-db

Configures the access control database parameters in HNB-GW Global configuration mode to control HNB and UE access to the HNB-GW node.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > HNB-GW Global Configuration
configure > hnbw-global

Entering the above command sequence results in the following prompt:

[local] host_name(config-hngw-global)#

Syntax Description

access-control-db imsi-purge-timeout { immediate | dur }
default access-control-db imsi-purge-timeout

default

Sets the default value to HNB-UE access control database on a chassis for HNB-GW Global configuration instance.

The default timeout duration for purging of the IMSI White List from the HNB-GW Access Control database is 24 hours. The HNB-GW service waits for 24 hours after all referenced HNBs have de-registered before purging the records.

immediate

Sets the HNB-GW Global configuration instance to purge the HNB-UE access control database immediately after all referenced HNBs have de-registered.

imsi-purge-timeout dur

Sets the timeout duration (in minutes) for the access control database to wait before purging the IMSI values received as a White List from HMS/BAC.

After all HNBs have de-registered, the Access Control database on HNB-GW maintains the IMSI White List received from HMS/BAC during HNB registration procedure for the configured durations before purging the list.

dur is an integer from 1 through 1440.
**Usage Guidelines**

Use this command to configure the HNB-UE access control database parameters on a chassis for HNB-GW Global configuration instance.

This command sets the timeout duration to maintain the IMSI White List received from HMS/BAC during HNB registration procedure in HNB-GW Global configuration instance for the configured \textit{dur} in minutes after de-registration of all referenced HNBs from HNB-GW node and then purge the database.

**Examples**

Following command sets the HNB-GW Global configuration instance to purge all IMSI records from HNB-UE access control database immediately after all referenced HNBs de-registered from HNB-GW service instance.

\texttt{access-control-db imsi-purge-timeout immediate}
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.
**paging hybrid-hnb**

Configures paging optimization parameters for hybrid HNBs connected through Hybrid Access mode in the HNB-GW Global parameter.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > HNB-GW Global Configuration

```
configure > hnbgw-global
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnggw-global)#
```

**Syntax Description**

```
paging hybrid-hnb always
paging hybrid-hnb hnb-where-ue-registered [ hnbss-having-imsi-in-whitelist ] fallback { always | never | only-if-with-paging-area }
paging hybrid-hnb hnbss-having-imsi-in-whitelist fallback { always | never | only-if-with-paging-area }
paging hybrid-hnb never
paging hybrid-hnb only-if-with-paging-area
default paging hybrid-hnb
```

**default**

Sets the default behavior of paging optimization configuration for a hybrid HNB while using Hybrid Access mode support.

By default the HNB-GW pages hybrid HNBs only if paging-area IE is received in the paging message.

```
{ always | never | only-if-with-paging-area }
```

Sets the HNB-GW Global parameter to page hybrid HNB for a paging message.

- **always**: Sets the system to ALWAYS page the hybrid HNBs irrespective of **paging-area** IE is received in paging messages.
- **never**: Sets the system to NEVER page any hybrid HNB.
- **only-if-with-paging-area**: Sets the system to page the hybrid HNBs only when **paging-area** IE is received in paging messages.

```
hnb-where-ue-registered fallback { always | never | only-if-with-paging-area }
```

Sets the HNB-GW Global parameter to page hybrid HNB from where the UE is registered.
always: Sets the system to ALWAYS page the hybrid HNBs from where the UE is registered. If the UE is not registered then it pages the hybrid HNBs irrespective of paging-area IE is received in paging messages.

never: Sets the system to page the hybrid HNBs from where the UE is registered. If the UE is not registered then it NEVER pages any hybrid HNB.

only-if-with-paging-area: Sets the system to ALWAYS page the hybrid HNBs from where the UE is registered. If the UE is not registered then it pages the hybrid HNBs only when paging-area IE is received in paging messages.

hnbs-having-imsi-in-whitelist fallback {always | never | only-if-with-paging-area}
Sets the HNB-GW Global parameter to page hybrid HNB where HNB have IMSI in white-list.

always: Sets the system to ALWAYS page Hybrid HNB which have requested IMSI in whitelist. If no such Hybrid HNB is found, then system will page Hybrid HNBs irrespective of presence or absence of paging-area IE in paging messages.

never: Sets the system to ALWAYS page Hybrid HNB which have requested IMSI in whitelist. If no such Hybrid HNB is found, then system will NEVER page Hybrid HNBs irrespective of presence or absence of paging-area IE in paging messages.

only-if-with-paging-area: Sets the system to ALWAYS page Hybrid HNB which have requested IMSI in whitelist. If no such Hybrid HNB is found, then system will page hybrid HNB only when paging-area IE is found in paging messages.

Usage Guidelines
Use this command to configure the paging optimization parameters for hybrid HNBs connected through Hybrid Access mode in HNB-GW Global parameter.

Examples
The following command configures the HNB-GW Global parameter to page an hybrid HNB from where the UE is registered and paging-area IE is received in paging message:

```
paging hybrid-hnb hnb-where-ue-registered fallback only-if-with-paging-area
```
paging open-hnb

Configures paging optimization parameters for open HNBs connected through Hybrid Access mode in the HNB-GW Global parameter.

This command is deprecated from release 16.0.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > HNB-GW Global Configuration
configure > hnbgw-global

Entering the above command sequence results in the following prompt:
[local]host_name(config-hnbgw-global)#

Syntax Description

paging open-hnb [hnb-where-ue-registered fallback] {always | never | only-if-with-paging-area}
default paging open-hnb

default

Sets the default behavior of paging optimization configuration for an open HNB while using Open Access mode support.

By default the HNB-GW pages open HNBs only if paging-area IE is received in the paging message.

{always | never | only-if-with-paging-area}

Sets the HNB-GW Global configuration instance to page open HNB for a paging message.

always: Sets the system to ALWAYS page the open HNBs irrespective of paging-area IE is received in paging messages.

never: Sets the system to NEVER page any open HNB.

only-if-with-paging-area: Sets the system to page the open HNBs only when paging-area IE is received in paging messages.

hnb-where-ue-registered fallback {always | never | only-if-with-paging-area}

Sets the HNB-GW Global configuration instance to page open HNB from where the UE is registered.
always: Sets the system to ALWAYS page the open HNBs from where the UE is registered. If the UE is not registered then it pages the open HNBs irrespective of `paging-area` IE is received in paging messages.

never: Sets the system to page the open HNBs from where the UE is registered. If the UE is not registered then it NEVER pages any open HNB.

only-if-with-paging-area: Sets the system to ALWAYS page the open HNBs from where the UE is registered. If the UE is not registered then it pages the open HNBs only when `paging-area` IE is received in paging messages.

Usage Guidelines
Use this command to configure the paging optimization parameters for open HNBs connected through Open Access mode in HNB-GW Global configuration instance.

Examples
The following command configures the HNB-GW Global configuration instance to page an open HNB from where the UE is registered and `paging-area` IE is received in paging message:

```
paging open-hnb hnb-where-ue-registered fallback only-if-with-paging-area
```
**sctp**

Configures the SCTP-related parameters like timeout duration for various timers and cookie life over an IuH interface on a chassis for HNB-GW Global configuration instance.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > HNB-GW Global Configuration

configure > hnbgw-global

Entering the above command sequence results in the following prompt:

\[local\] *host_name* (config-hnggw-global)#

**Syntax Description**

`sctp { alpha-rto alpha_rto_dur | beta-rto beta_rto_dur | max-in-strms in_strms | max-out-strms out_strms | max-retx { assoc | init | path } max_retry }

default sctp { alpha-rto | beta-rto | max-in-strms | max-out-strms | max-retx { assoc | init | path } }

default

Restores the SCTP parameters to default value in HNB-GW Global configuration instance. Default values for all parameters are as follows:

- **alpha-rto**: 5 seconds
- **beta-rto**: 10 seconds
- **max-in-strms**: 4
- **max-out-strms**: 4
- **max-retx assoc**: 10 retries
- **max-retx init**: 5 retries
- **max-retx path**: 5 retries

**alpha-rto alpha_rto_dur**

Sets the alpha retransmission timeout duration (in seconds) for SCTP association between HNB and HNB-GW as an integer from 0 through 65535. A "zero" value disables the timer in this configuration. Default: 5
**beta-rto beta_rto_dur**
Sets the beta retransmission timeout duration (in seconds) for SCTP association between HNB and HNB-GW an integer from 0 through 65535. A "zero" value disables the timer in this configuration. Default: 10

**max-retx { assoc | init | path } max_retry**
Sets the maximum number of retries allowed in SCTP states for SCTP association between HNB and HNB-GW.

**assoc**: Sets the maximum number of consecutive retransmissions to its peer is allowed. If the value of this counter exceeds the limit configured with this keyword the HNB-GW considers the peer HNB unreachable and stop transmitting any more data to it. The SCTP association is automatically closed when the peer endpoint becomes unreachable. Default number of attempts max_retry for this state is 10.

**init**: Sets the maximum attempts allowed after T1-init timer expires. If the T1-init timer expires then the HNB-GW retransmits INIT chunk and re-start the T1-init timer without changing state. This is repeated up to the configured times with this configuration. After that, the HNB-GW aborts the initialization process. Default number of attempts max_retry for this state is 5.

**path**: Sets the maximum attempts allowed after T3-rtx timer expires. Each time the T3-rtx timer expires on any address, or when a HEARTBEAT sent to an idle address is not acknowledged within a RTO, the error counter of that destination address incremented. When the value in the error counter exceeds this protocol parameter of that HNB address, the HNB-GW marks the destination transport address as inactive. Default number of attempts max_retry for this state is 5.

max_retry is an integer from 0 through 255.

**max-in-strms in_strms**
Sets the maximum number of inward SCTP streams allowed on HNB-GW for an associated HNB in an SCTP association as an integer from 1 through 16. Default: 4

**max-out-strms out_strms**
Sets the maximum number of outgoing SCTP streams allowed from HNB-GW for an associated HNB in an SCTP association as an integer from 1 through 16. Default: 4

**Usage Guidelines**
Use this command to configure the SCTP protocol messaging and session management parameters in SCTP association between HNB and HNB-GW.

**Examples**
The following command sets the maximum number of inward SCTP streams allowed to 4 on HNB-GW for the SCTP association:

default max-in-strms
**session-collocation**

This command is used to enable / disable iu and hnb in same session manager.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > HNB-GW Global Configuration

configure > hnbgw-global

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-hnggw-global) #
```

**Syntax Description**

```
| no | default | session-collocation { both | iucs | iups } |
```

no
Does not allow the enable / disable of the iu and hnb in same session manager.

default
Sets the timer value for enable / disable of the iu and hnb in same session manager.

both
Enables / disables both the iucs and iups with HNB in same session manager.

iucs
Enables / disables both the iucs with HNB in same session manager.

iups
Enables / disables both the iups with HNB in same session manager.

**Usage Guidelines**
Use this command to enable / disable iu and hnb in same session manager.

**Examples**
The following command enables iucs and hnb in same session manager.

```
session-collocation iucs
```
tnnsf-timer

Configures the NAS Node Selection Function (NNSF) timer (T-NNSF) which is used by the HNB-GW to store the IMSI and the relevant Global-CN-ID in the short term after Paging. This timer is used for Iu-Flex feature support.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > HNB-GW Global Configuration

configure > hnbgw-global

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbgw-global)#

Syntax Description

tnnsf-timer dur

| no | default | tnnf-timer

no

Disables/removes the configured timer value of NNSF timer (T-NNSF) for HNB-GW Global configuration instance.

default

Sets the timer value of NNSF timer (T-NNSF) for HNB-GW Global configuration instance to default value of 30 seconds.

Usage Guidelines

Use this command to configure the NNSF timer value in seconds for Iu-Flex support.

Whenever the MSC sends the paging request with IMSI, the HNB-GW stores the Global_CN_ID of the node which issued the paging request message for the given IMSI and HNB-GW starts the tnnf-timer. HNBGW stores the mapping of IMSI to Global_CN_ID until the tnnf-timer expires.
**Examples**

The following command sets the NNSF timer value to 30 seconds on a chassis for HNB-GW Global configuration instance:

```
default tnssf-timer
```
HNB-GW Service Configuration Mode Commands

The 3G UMTS Home-NodeB Gateway Service Configuration Mode manages access to the UMTS core network in a 3G UMTS network through a Femto node.

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-hnbgw-service) #
```

**Important**

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

- access-control-db, page 1410
- associate cbs-service, page 1412
- associate gtpu-service, page 1413
- associate rtp pool, page 1415
- authorised-macro-lai macro-info-ie-absent-action, page 1417
- authorised-macro-lai mce, page 1418
- common-plmn, page 1420
- end, page 1422
- exit, page 1423
- handin, page 1424
- hnb override-vsa location-based-service, page 1426
- hnb-access-mode closed, page 1427
- hnb-access-mode hybrid, page 1428
• hnb-access-mode mismatch-action, page 1429
• hnb-access-mode open, page 1430
• hnb-aggregation, page 1432
• hnb-config-transfer, page 1434
• hnb-identity, page 1435
• ip iu-qos-dscp, page 1436
• ip iub-qos-dscp, page 1439
• ipsec connection-timeout, page 1443
• iurh-handoff, page 1444
• iurh-handoff-guard-timer, page 1445
• mocn-max-reroute-attempts, page 1446
• mocn-reroute-timeout, page 1447
• paging cs-domain, page 1448
• paging imsi-purge-timer, page 1450
• paging ps-domain, page 1451
• paging open-hnb, page 1453
• radio-network-plmn, page 1455
• ranap reset, page 1457
• rtcp report, page 1459
• rtp address, page 1461
• rtp port, page 1463
• rtp mux, page 1465
• sctp bind, page 1466
• sctp checksum-type, page 1468
• sctp connection-timeout, page 1469
• sctp cookie-life, page 1471
• sctp heart-beat-timeout, page 1472
• sctp mtu-size, page 1474
• sctp rto, page 1475
• sctp sack-frequency, page 1476
• sctp sack-period, page 1477
• security-gateway bind, page 1478
• sessmgr-to-cbsmgr-pacing-timer, page 1480
• tnnsf-timer, page 1481
• ue registration-timeout, page 1482
**access-control-db**

Configures the access control database parameters in an HNB-GW service instance to control HNB and UE access to the HNB-GW node.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-hnbgw-service)#
```

**Syntax Description**

`access-control-db imsi-purge-timeout { immediate | dur }

default access-control-db imsi-purge-timeout`

**default**

Sets the default value to HNB-UE access control database on HNB-GW service instance.

The default timeout duration for purging of the IMSI White List from the HNB-GW Access Control database is 24 hours. The HNB-GW service waits for 24 hours after all referenced HNBs have de-registered before purging the records.

**immediate**

Sets the HNB-GW service to purge the HNB-UE access control database immediately after all referenced HNBs have de-registered.

**imsi-purge-timeout dur**

Sets the timeout duration (in minutes) for the access control database to wait before purging the IMSI values received as a White List from HMS/BAC.

After all HNBs have de-registered, the Access Control database on HNB-GW maintains the IMSI White List received from HMS/BAC during HNB registration procedure for the configured durations before purging the list.

*dur* is an integer from 1 through 1440.

**Usage Guidelines**

Use this command to configure the HNB-UE access control database parameters on HNB-GW service.
This command sets the timeout duration to maintain the IMSI White List received from HMS/BAC during HNB registration procedure in HNB-GW service for the configured \textit{dur} in minutes after de-registration of all referenced HNBs from HNB-GW node and then purge the database.

**Examples**

Following command sets the HNB-GW service instance to purge all IMSI records from HNB-UE access control database immediately after all referenced HNBs de-registered from HNB-GW service instance.

\texttt{access-control-db imsi-purge-timeout immediate}
associate cbs-service

Configures CBS service for this HNBGW service.

**Product**  
HNB-GW

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration  
```
configure > context context_name > hnbgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

**Syntax Description**  
```
associate cbs-service svc_name
no associate cbs-service
```

**no**  
Removes the configured CBS service from this HNB-GW service configuration.

**svc_name**  
Identifies the name of the pre-configured CBS service to associate with an HNB-GW service.  
```
svc_name
```

Identifies the name of the pre-configured CBS service to associate with an HNB-GW service.  
```
svc_name
```

Identifies the name of the pre-configured CBS service to associate with an HNB-GW service.  
```
svc_name
```

Identifies the name of the pre-configured CBS service to associate with an HNB-GW service.

**Usage Guidelines**  
Use this command to configure CBS service for HNB-GW service.

**Examples**  
Following command configures CBS service named `cbs_hnb1` with specific HNB-GW service.  
```
associate cbs-service cbs_hnb1
```
**associate gtpu-service**

Associates a previously configured GTP-U service to bind the HNB-GW service with an HNB towards the HNB side. A GTP-U service must be configured in Context Configuration mode before using this configuration.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbgw-service)#

**Syntax Description**

- **associate gtpu-service svc_name**
- **no associate gtpu-service**

- **no**
  Removes the associated GTP-U service from this HNB-GW service configuration.

  **svc_name**

  Identifies the name of the pre-configured GTP-U service to associate with an HNB-GW service towards the Home-NodeB side.

  **svc_name** is an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to configure GTP-U data plan between HNB-GW service and Home-NodeB. The service defined for GTP-U can be configured in Context configuration mode.

**Important**

Another GTP-U service can be used to bind the HNB-GW service towards the Core Network and can be configured in HNB-PS Configuration mode. For more information on GTP-U service configuration, refer **GTP-U Service Configuration Mode Commands**.
Examples

Following command associates GTP-U service named `gtpu_hnb1` with specific HNB-GW service towards Home-NodeB side.

```
associate gtpu-service gtpu_hnb1
```
**associate rtp pool**

Associates a previously defined RTP pool (IP pool) with the HNB-GW service. This pool is used by HNB-GW to send an IP address to HNB where HNB uses it to map the RTP streams over Iuh interface. This command is used for RTP stream management on HNB-GW.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

 Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

 configure > context context_name > hnbgw-service service_name

 Entering the above command sequence results in the following prompt:

 [local] host_name(config-hnbgw-service)#

**Syntax Description**

- **associate rtp pool pool_name**
- **no associate rtp pool**

  no

  Removes the associated RTP pool (IP pool) from this HNB-GW service configuration.

  **pool_name**

  Specifies the name of the pre-configured RTP IP pool that the HNB-GW uses to assign IP addresses when mapping RTP streams over the Iuh interface.

  **pool_name** is an alphanumeric string of 1 through 31 characters.

**Important**

For IP pool (RTP pool) configuration, refer **ip pool** command in *Context Configuration Mode Commands* chapter.

**Usage Guidelines**

Use this command to associate an RTP pool (IP Pool) with an HNB-GW service for allotment of RTP IP address to HNB-GW node and send the same to HNB for RTP stream management support. The HNB maps the RTP streams with received IP address(es) while communicating with HNB-GW over Iuh interface where HNB-GW communicates with MSC/VLR through IuCS-over-IP tunnel.

This command is used for RTP stream management on HNB-GW.
This command must be used to provide IP address for mapping of RTP streams on Iuh interface between HNB and HNB-GW.

**Examples**

Following command associates RTP pool named *rtp_1* with HNB-GW service for RTP stream end point from Home-NodeB:

```plaintext
associate rtp pool rtp_1
```
authorised-macro-lai macro-info-ie-absent-action

This command configures the Action if Macro Coverage information IE is absent in HNB Location Information. The HNB will be accepted for Action Accept and rejected for Action Reject.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-hnbgw-service)#

Syntax Description

authorised-macro-lai macro-info-ie-absent-action { accept | reject }
default authorised-macro-lai macro-info-ie-absent-action

default
Sets / Restores default value assigned for the Action if Macro Coverage information IE is absent in HNB Location Information. The default value is reject.

accept
Accepts HNB even if Macro Coverage information IE is absent in HNB Location Information.

reject
Rejects HNB if Macro Coverage information IE is absent in HNB Location Information.

Usage Guidelines
Use this command when Macro Coverage Info IE is absent in HNB Location information.

Examples
The following command accepts HNB even if Macro Coverage information IE is absent in HNB Location Information:

authorised-macro-lai macro-info-ie-absent-action accept
authorised-macro-lai mcc

This command configures MCC of Pre-Configured macro lai range for HNB Authorisation.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration
configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-hnbgw-service)#

**Syntax Description**
| no | authorised-macro-lai mcc mcc mnc mnc lac range min to max |

**no**
Removes the MCC of Pre-Configured macro lai range for HNB Authorisation.

**mcc mcc**
MCC of Pre-Configured macro lai range for HNB Authorisation.
mcc is a number ranging from 100 through 999.

**mnc mnc**
MNC of Pre-Configured macro lai range for HNB Authorisation.
mnc is a number ranging from 00 through 999.

**lac range min to max**
LAC of Pre-Configured macro lai range for HNB Authorisation.
LAC is configured as range, if single lac make min is equal to max.
Macro LAC from min to max integer values between 0 through 65535.

**Usage Guidelines**
Use this command to configure the MCC of Pre-Configured macro lai range for HNB Authorisation.
Examples

The following command configures the MCC of Pre-Configured macro lai range for HNB Authorisation with mcc 888, mnc 44 and lac range from 10 to 1000:

```
authorised-macro-lai mcc 678 mnc 788 lac range 10 to 1000
```
**common-plmn**

This command configures the Common PLMN along with rnc-id. This enables MOCN.

**Product**

HNB-GW

** privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbgw-service)#

**Syntax Description**

```
common-plmn mcc mcc mnc mnc  rnc-id rnc_id
no common-plmn
```

**no**

Removes the configuration of Common PLMN service.

```
mcc mcc
```

Configures the MCC of Common PLMN.

```
mcc is a number ranging from 100 through 999.
```

```
mnc mnc
```

Configures the MNC of Common PLMN.

```
mnc is a number ranging from 00 through 999.
```

```
rnc-id rnc_id
```

Configures the RNC-id for this HNBGW service.

```
rnc_id is a decimal value of integer ranging from 0 through 4095.
```

**Usage Guidelines**

Use this command to configure the Common PLMN along with rnc-id to HNB-GW service. This enables MOCN.
Examples

The following command configures Common PLMN with mcc 888, mnc 44 and rnc-id 66 to HNB-GW service:

```
common-plmn mcc 444 mnc 56 rnc-id 56
```
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.
handin

Allows or disallows the incoming hand-over of an MS in HNB-GW via the Serving Radio Network Subsystem (SRNS) Relocation procedure for the specified packet switched/circuit switched (PS/CS) core network (CN) domain.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Syntax Description

[ no | default | handin cn-domain ] [ cs | ps ]

no

Disallows the incoming MS hand-over for the particular CN domain via SRNS Relocation procedure in an HNB-GW service instance.

If hand-over is restricted the relocation request will be rejected with rejection cause "Relocation Not Supported In Target RNC Or Target System".

default

Sets the HNB-GW service instance to allow the incoming MS hand-over for the particular CN domain via SRNS Relocation procedure in an HNB-GW service instance.

cs

Sets the HNB-GW service instance to allow the incoming MS hand-over for the CS core network domain via SRNS Relocation procedure in an HNB-GW service instance.

ps

Sets the HNB-GW service instance to allow the incoming MS hand-over for the PS core network domain via SRNS Relocation procedure in an HNB-GW service instance.
Usage Guidelines  Use this command to set HNB-GW service instance for allowing/disallowing incoming hand-over of an MS in HNB-GW via SRNS Relocation procedure for PS or CS core network domain.

If hand-over is restricted the Relocation Request message will be rejected with rejection cause "Relocation Not Supported In Target RNC Or Target System".

Examples  The following command configures the HNB-GW service instance to allow hand-over of an MS in HNB-W via SRNS Relocation procedure for PS core network domain:

```
handin cn-domain ps
```
hnb override-vsa location-based-service

This command enables / disables overriding of a particular vendor specific attribute of configured location based HNB Service.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnb-gw-service service_name

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-hnb-gw-service)#
```

**Syntax Description**

| no | default | hnb override-vsa location-based-service |

- **no**
  - Disables the overriding of vendor specific attribute for location based service.

- **default**
  - When set to default, overriding of vendor specific attribute will be disabled.

**Usage Guidelines**

Use this command to enable / disable overriding of a particular vendor specific attribute of configured location based HNB Service.

**Examples**

The following command enables overriding of a particular vendor specific attribute of configured location based HNB Service:

```
hnb override-vsa location-based-service
```
hnb-access-mode closed

This command configures Closed Access Mode for HNB Access Mode Support.

Product  HNB-GW

Privilege  Security Administrator, Administrator

Command Modes  Exec > Global Configuration > Context Configuration > HSGW Service Configuration
configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:
[context_name] host_name (config-hsgw-service) #

Syntax Description  

  hnb-access-mode closed | max-registered-ue value | default hnb-access-mode closed

  default
  Sets/Restores the default value assigned for Closed Access Mode.

  max-registered-ue value
  Maximum Registered UEs per Close HNB. Default is 64.
  value is an integer ranging from 1 to 1000.

Important  Maximum registered UEs depends on the aggregation factor configuration of HNBGW service. If aggregation is enabled then Maximum registered UEs is 1 to 10000 otherwise it is 1 to 1000.

Usage Guidelines  Use this to configure Closed Access Mode for HNB Access Mode Support.

Examples  Following command configures the Maximum Registered UEs per Close HNB as 15.
  hnb-access-mode closed max-registered-ue 15
**hnb-access-mode hybrid**

This command configures the Hybrid HNB access mode in HNB-GW service instance and related parameters.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-hnbgw-service) #

**Syntax Description**

hnb-access-mode hybrid \[ max-non-access-controlled-ue num \] { no | default } hnb-access-mode hybrid

- **no**
  - Disables the Hybrid Access Mode of HNB service.

- **default**
  - Sets the default configuration of Hybrid Access Mode support. The default value of Maximum Non-Access-Controlled UEs per Hybrid HNB is 64.
  - By default, HNB-GW allows registration of Non-Access-Controlled UEs per Hybrid HNB and a maximum of 16 UEs can register from a hybrid HNB in an HNB-GW service instance.

max-non-access-controlled-ue num

- Maximum Non-Access-Controlled UEs per Hybrid HNB.
  - num is an integer from 0 through 64.

**Usage Guidelines**

Use this command to configure the Hybrid HNB access mode in HNB-GW service instance and related parameters.

**Examples**

The following command configures the Hybrid HNB access mode in HNB-GW service instance and related parameters.

hnb-access-mode hybrid
### hnb-access-mode mismatch-action

This command configures the mismatch action of HNB access mode in HNB-GW service instance and related parameters.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

```plaintext
configure > context context_name > hnbgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-hnbgw-service) #
```

**Syntax Description**

```plaintext
hnb-access-mode mismatch-action { accept-aaa-value | hnb-reg-rej }
default hnb-access-mode mismatch-action
```

**default**

Sets the default Hybrid Access Mode of HNB service. The default value of Maximum Non-Access-Controlled UEs per Hybrid HNB is 64.

**Syntax Description**

```plaintext
hnb-access-mode mismatch-action { accept-aaa-value | hnb-reg-rej }
default hnb-access-mode mismatch-action
```

**Usage Guidelines**

Use this command to configure the mismatch action of HNB access mode in HNB-GW service instance and related parameters.

**Examples**

The following command configures the mismatch action of HNB access mode in HNB Service to Accept AAA value:

```plaintext
hnb-access-mode mismatch-action accept-aaa-value
```
**hnb-access-mode open**

Configures the Open HNB access mode in HNB-GW service instance and related parameters.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

`Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration`

`configure > context context_name > hnbgw-service service_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-hnbgw-service) #
```

**Syntax Description**

```
hnb-access-mode open | max-registered-ue reg_ue_open| no | default } hnb-access-mode open
```

- **no**
  
  Disables Open Access mode support.
  
  If disabled and an Open HNB tries to register, the HNB-GW sends HNB-Registration-Reject message with "OAM Intervention" cause.

- **Important**
  
  UE-Reg/CS-Call/PS-Call requests (both existing and future) is allowed from already registered Open HNBs even after operator has disabled the Open Access support. No new Open HNB registration is allowed once operator disables the Open Access support.

- **default**

  Sets the default configuration of Open Access mode support.
  
  By default, HNB-GW allows registration of Open HNBs and a maximum of 64 UEs can register from an open HNB in an HNB-GW service instance.

- **max-registered-ue reg_ue_open**

  Sets the HNB-GW service instance to allow the maximum number of UEs through an open HNB under Open Access mode support.
reg_ue_open defines the maximum number of UEs that can register from an Open HNB as an integer from 1 through 64.

If a UE tries to register from an Open HNB which has already reached to the configured limit configured, the HNB-GW sends HNB-Registration-Reject message with "ue not allowed in this hnb" cause in an HNB-GW service instance.

**Usage Guidelines**

Use this command to configure the HNB-GW service instance for Open Access Mode support and related parameters.

This command enable Open Access mode support to allow the UEs that can register from an Open HNB. If a UE tries to register from an Open HNB with an HNB-GW service instance, which is already reached to the limit configured through max-registered-ue reg_ue_open the HNB-GW sends HNB-Registration-Reject message with "ue not allowed in this hnb" cause.

**Important**

If Operator has reduced the maximum number of UEs allowed per Open HNB during the session, this will not have any effect on already registered UEs/CS-Calls/PS-Calls even if previously configured reg_ue_open is beyond the newly configured reg_ue_open value. Limits is respected while handling new requests.

**Examples**

The following command configures the HNB-GW service instance to allow 16 UEs to register through an open HNB:

`hnb-access-mode open max-registered-ue 16`
**hnb-aggregation**

This command enables/disables HNB aggregation support for this hnbgw-service.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbgw-service)#

**Syntax Description**

hnb-aggregation { handin-with-aggregator | max-registered-ues-per-hnb value } [-noconfirm] |

no

Disables the HNB aggregation support for this hnbgw-service.

default

Sets the default value of HNB aggregation support for this hnbgw-service.

handin-with-aggregator

Enables or disables handin with the aggregators.

max-registered-ues-per-hnb

Configures the maximum number of UEs allowed per HNB.

**Caution**

Once set, any change in this configuration will cause all HNBs in this HNBGW service to get disconnected.

value defines the maximum number of UEs allowed per HNB as an integer from 1 through 10000.

**Usage Guidelines**

Use this command to enable/disable HNB aggregation support for this hnbgw-service.
Examples

The following command configures the maximum number of UEs allowed per HNB:

```
hnb-aggregation max-registered-ues-per-hnb 16
```

The following command enables handin with aggregators:

```
hnb-aggregation handin-with-aggregator
```
**hnb-config-transfer**

This command enables/disables Inclusion of Inner IP Address in HNB Configuration Transfer Response for HNBGW-service.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

`configure > context context_name > hnbgw-service service_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-hnbgw-service) #
```

**Syntax Description**

`| default | no | hnb-config-transfer add-inner-ip`

- **no**
  
  Disables the Inclusion of Inner IP Address in HNB Configuration Transfer Response for HNBGW-service.

- **default**
  
  Enables the default behavior of Inclusion of Inner IP Address in HNB Configuration Transfer Response for HNBGW-service. By default it is enabled.

- **add-inner-ip**
  
  Enables/Disables Inclusion of Inner IP Address in HNB Configuration Transfer Response for HNBGW-service.

**Usage Guidelines**

Use this command to enable / disable the Inclusion of Inner IP Address in HNB Configuration Transfer Response for HNBGW-service.

**Examples**

The following command enables the Inclusion of Inner IP Address in HNB Configuration Transfer Response for HNBGW-service:

```
hnb-config-transfer add-inner-ip
```
**hnb-identity**

Configures and also allows modification to the HNB ID before it is sent to the AAA server for authentication in HNB-GW service instance.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

```plaintext
configure > context context_name > hnbgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

**Syntax Description**

```
[default | no] hnb-identity oui discard-leading-char
```

- **no**
  
  Disables discarding of leading character of HNB-id if it contains Organizationally Unique Identifier

- **default**
  
  Enables the default behavior of discarding of leading character of HNB-id if it contains Organizationally Unique Identifier. By default this feature is deactivated.

- **oui discard-leading-char**
  
  This CLI allows to modify the HNB ID before it is sent to the AAA server for authentication. By using this CLI, first character of the HNB-id can be removed if the HNB-id follows the format: '1<OUI>-<SerialNumber>@<realm>'.

**Usage Guidelines**

Use this command to configure and allow modification to the HNB ID before it is sent to the AAA server for authentication in HNB-GW service instance.

**Examples**

The following command configures the discarding of leading character of HNB-id if it contains Organizationally Unique Identifier:

```plaintext
hnb-identity oui discard-leading-char
```
ip iu-qos-dscp

Enables or disables the DSCP marking parameter for data packets carried over an IuCS/IuPS interface towards MSC/SGSN. By default this command is Disabled.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbgw-service)#

**Syntax Description**

ip iu-qos-dscp protocol udp payload { gtpu | rtcp | rtp } dscp_code

{ default | no } ip iu-qos-dscp protocol udp payload { gtpu | rtcp | rtp }

no

Use this keyword to place the configuration in pass-through mode (no marking of DSCP). Use of this keyword is allowed even when there is no previous DSCP parameter set.

---

**Important**

In this configuration the **no** keyword does not disable or remove a previous configuration.

**default**

Enables the DSCP marking on HNB-GW and set/restores the QoS parameters to their default setting.

**udp payload { gtpu | rtcp | rtp } dscp_code**

Specifies the QoS traffic pattern towards MSC/SGSN in SCTP protocol association over IuCS/IuPS interface. By this keyword the Traffic classes specified by a user based on UDP protocol and GTPU, RTCP, and RTP type of payload identified based on the transport level port numbers.

Default DSCP code in UDP traffic are:

- GTP-U: cs1
- RTCP: ef
- RTP: af41
**dscp_code**

Specifies the QoS DSCP codes supported for SCTP and UDP traffic and its payloads towards MSC/SGSN over IuCS/IuPS interface.

The following type of DSCP codes `dscp_code` are supported over IuH interface:

- **af11**: Marks traffic as Assured Forwarding 11 PHB (high throughput data)
- **af12**: Marks traffic as Assured Forwarding 12 PHB (high throughput data)
- **af13**: Marks traffic as Assured Forwarding 13 PHB (high throughput data)
- **af21**: Marks traffic as Assured Forwarding 21 PHB (low latency data)
- **af22**: Marks traffic as Assured Forwarding 22 PHB (low latency data)
- **af23**: Marks traffic as Assured Forwarding 23 PHB (low latency data)
- **af31**: Marks traffic as Assured Forwarding 31 PHB (multimedia streaming)
- **af32**: Marks traffic as Assured Forwarding 32 PHB (multimedia streaming)
- **af33**: Marks traffic as Assured Forwarding 33 PHB (multimedia streaming)
- **af41**: Marks traffic as Assured Forwarding 41 PHB (multimedia conferencing). This is the default DSCP code for RTP payloads in UDP protocol.
- **af42**: Marks traffic as Assured Forwarding 42 PHB (multimedia conferencing)
- **af43**: Marks traffic as Assured Forwarding 43 PHB (multimedia conferencing)
- **cs1**: Marks traffic with Class Selector 1 (low priority data). This is the default DSCP code for GTP-U payloads in UDP protocol.
- **cs2**: Marks traffic with Class Selector 2 (OAM)
- **cs3**: Marks traffic with Class Selector 3 (broadcast video)
- **cs4**: Marks traffic with Class Selector 4 (real-time interactive)
- **cs5**: Marks traffic with Class Selector 5 (signaling). This is the default DSCP code for all SCTP payloads.
- **cs6**: Marks traffic with Class Selector 6 (network control)
- **df**: Marks traffic as Default Forwarding (best effort: DSCP = 0)
- **ef**: Marks traffic as Expedited Forwarding PHB (telephony). This is the default DSCP code for RTCP payloads in UDP protocol.

**Usage Guidelines**

Use this command to enable/disable the DSCP marking for data packets over IuCS/PS interface. This command assigns the DSCP levels to specific traffic patterns in order to ensure that the packets are delivered according to the precedence with which they are tagged. The Diffserv markings are applied to the IP header of every subscriber data packet transmitted over IuCS/IuPs interface(s) towards MSC/SGSN.

This command adds DSCP marking on egress traffic going towards CN (CS/PS). To make the configuration **pass-through** mode or not marking DSCP at all in the packets, `no` variant of command is used. Use of `no` is allowed even when there is no previous DSCP configuration done.
By default this command is Disabled.

When DSCP configuration is not specified, the system works in pass-through mode and DSCP values in the ingress (from CN) and egress (to HNB) data packets remain unchanged. Multiple traffic classes can share the same code point value.

Following type shown in following tables respectively:

**Table 7: Supported DSCP Codes and Service Class**

<table>
<thead>
<tr>
<th>Service Class</th>
<th>DSCP Code</th>
<th>Service Class</th>
<th>DSCP Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>high throughput data</td>
<td>af11</td>
<td>low priority data</td>
<td>cs1</td>
</tr>
<tr>
<td></td>
<td>af12</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>af13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>low latency data</td>
<td>af21</td>
<td>OAM</td>
<td>cs2</td>
</tr>
<tr>
<td></td>
<td>af22</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>af23</td>
<td></td>
<td></td>
</tr>
<tr>
<td>multimedia streaming</td>
<td>af31</td>
<td>broadcast video</td>
<td>cs3</td>
</tr>
<tr>
<td></td>
<td>af32</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>af33</td>
<td></td>
<td></td>
</tr>
<tr>
<td>multimedia conferencing</td>
<td>af41</td>
<td>real-time interactive</td>
<td>cs4</td>
</tr>
<tr>
<td></td>
<td>af42</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>af43</td>
<td></td>
<td></td>
</tr>
<tr>
<td>best effort/ default forwarding, value zero</td>
<td>df</td>
<td>Signaling</td>
<td>cs5</td>
</tr>
<tr>
<td>telephony</td>
<td>ef</td>
<td>network control</td>
<td>cs6</td>
</tr>
</tbody>
</table>

The DSCP level can be configured for multiple traffic patterns within a single instance of this command.

**Examples**

The following command configures the DSCP code for the SCTP IuCS/IuPS streaming traffic pattern for all payloads to be ef:

```
ip iu-qos-dscp protocol sctp payload all ef
```
ip iuh-qos-dscp

Enables or disables the DSCP marking parameter for control and data packets transmitted over an IuH interface towards HNB. By default this command is Disabled.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbgw-service)#

Syntax Description

```
ip iuh-qos-dscp protocol { sctp payload all | udp payload { gtpu | rtcp | rtp } } dscp_code
{ default | no } ip iuh-qos-dscp protocol { sctp payload all | udp payload { gtpu | rtcp | rtp } }
```

`no`

Use this keyword to set the configuration in pass-through mode. Use of this keyword is allowed even when there is no previous DSCP parameter set.

Important

In this configuration the no keyword does not disable/remove a previous configuration.

`default`

Enables the DSCP marking on HNB-GW and set/restores the QoS parameters to its default setting.

```
sctp payload all dscp_code
```

Specifies the QOS traffic pattern towards HNB in SCTP protocol association over IuH interface.

By this keyword the Traffic classes specified by a user based on SCTP protocol and all type of payload identified based on the transport level port numbers.

By default DSCP codes cs5 is supported for all payloads in SCTP protocol.

```
udp payload { gtpu | rtcp | rtp } dscp_code
```

Specifies the QOS traffic pattern towards HNB in SCTP protocol association over IuH interface.

---

[Command Line Interface Reference, Modes G - H, StarOS Release 19]
By this keyword the Traffic classes specified by a user based on UDP protocol and GTPU, RTCP, and RTP type of payload identified based on the transport level port numbers.

Default DSCP code in UDP traffic are:

- **GTP-U**: cs1
- **RTCP**: ef
- **RTP**: af41

### dscp_code

Specifies the QOS DSCP codes supported for SCTP and UDP traffic and its payloads towards HNB over IuH interface.

Following type of DSCP codes `dscp_code` are supported over IuH interface:

- **af11**: Marks traffic as Assured Forwarding 11 PHB (high throughput data)
- **af12**: Marks traffic as Assured Forwarding 12 PHB (high throughput data)
- **af13**: Marks traffic as Assured Forwarding 13 PHB (high throughput data)
- **af21**: Marks traffic as Assured Forwarding 21 PHB (low latency data)
- **af22**: Marks traffic as Assured Forwarding 22 PHB (low latency data)
- **af23**: Marks traffic as Assured Forwarding 23 PHB (low latency data)
- **af31**: Marks traffic as Assured Forwarding 31 PHB (multimedia streaming)
- **af32**: Marks traffic as Assured Forwarding 32 PHB (multimedia streaming)
- **af33**: Marks traffic as Assured Forwarding 33 PHB (multimedia streaming)
- **af41**: Marks traffic as Assured Forwarding 41 PHB (multimedia conferencing). This is the default DSCP code for RTP payloads in UDP protocol.
- **af42**: Marks traffic as Assured Forwarding 42 PHB (multimedia conferencing)
- **af43**: Marks traffic as Assured Forwarding 43 PHB (multimedia conferencing)
- **cs1**: Marks traffic with Class Selector 1 (low priority data). This is the default DSCP code for GTP-U payloads in UDP protocol.
- **cs2**: Marks traffic with Class Selector 2 (OAM)
- **cs3**: Marks traffic with Class Selector 3 (broadcast video)
- **cs4**: Marks traffic with Class Selector 4 (real-time interactive)
- **cs5**: Marks traffic with Class Selector 5 (signaling). This is the default DSCP code for all SCTP payloads.
- **cs6**: Marks traffic with Class Selector 6 (network control)
- **df**: Marks traffic as Default Forwarding (best effort: DSCP = 0)
- **ef**: Marks traffic as Expedited Forwarding PHB (telephony). This is the default DSCP code for RTCP payloads in UDP protocol.
Usage Guidelines

Use this command to enable/disable the DSCP marking for control and data packets carried by the IP protocols and their payloads on IuH. This command assigns the DSCP levels to specific traffic patterns in order to ensure that the packets are delivered according to the precedence with which they are tagged. The Diffserv markings are applied to the IP header of every subscriber data packet transmitted over IuH interface(s) towards HNB.

This command adds DSCP marking on egress traffic going towards HNB. To make the configuration pass-through mode or not marking DSCP at all in the packets, no variant of command is used. Use of no is allowed even when there is no previous DSCP configuration done.

---

**Important**

By default this command is **Disabled**.

---

**Important**

When DSCP configuration is not specified, system works in pass-through mode and DSCP value in the ingress (from CN) and egress (to HNB) control and data packets remain unchanged. Multiple traffic classes can share the same code point value.

---

Following type shown in following tables respectively:

### Table 8: Supported DSCP Codes and Service Class 140

<table>
<thead>
<tr>
<th>Service Class</th>
<th>DSCP Code</th>
<th>Service Class</th>
<th>DSCP Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>high throughput data</td>
<td>af11</td>
<td>low priority data</td>
<td>cs1</td>
</tr>
<tr>
<td></td>
<td>af12</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>af13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>low latency data</td>
<td>af21</td>
<td>OAM</td>
<td>cs2</td>
</tr>
<tr>
<td></td>
<td>af22</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>af23</td>
<td></td>
<td></td>
</tr>
<tr>
<td>multimedia streaming</td>
<td>af31</td>
<td>broadcast video</td>
<td>cs3</td>
</tr>
<tr>
<td></td>
<td>af32</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>af33</td>
<td></td>
<td></td>
</tr>
<tr>
<td>multimedia conferencing</td>
<td>af41</td>
<td>real-time interactive</td>
<td>cs4</td>
</tr>
<tr>
<td></td>
<td>af42</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>af43</td>
<td></td>
<td></td>
</tr>
<tr>
<td>best effort/ default forwarding, value zero</td>
<td>df</td>
<td>Signaling</td>
<td>cs5</td>
</tr>
<tr>
<td>telephony</td>
<td>ef</td>
<td>network control</td>
<td>cs6</td>
</tr>
</tbody>
</table>
The DSCP level can be configured for multiple traffic patterns within a single instance of this command.

**Examples**

The following command configures the DSCP code for the SCTP IuH streaming traffic pattern for all payloads to be ef:

```
ip iuh-qos-dscp protocol sctp payload all ef
```
ipsec connection-timeout

This command allows to configure IPSEC tunnel idle time out in hours. Default is 4 hours.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbw-service service_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-hnbw-service)#

Syntax Description
{ default | no } ipsec connection-timeout  ipsec_connection_timeout

default
Sets the default value of idle time out as 4 hours.

no
Disbles IPSEC idle time out.

ipsec_connection_timeout
IPSEC tunnel idle time out in hours between 1 and 48. Default is 4 hours.

Usage Guidelines
Use this command to configure IPSEC tunnel idle timeout in a specific HNB-GW service.

Examples
The following command sets IPSEC tunnel idle time out to 3 hours:

ipsec connection-timeout  3
iurh-handoff

This command enables or disables the Femto To Femto Handover in a specific HNB-GW service.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-hnbgw-service)#

Syntax Description

| no | default | iurh-handoff

default

Sets the default behavior of the Femto To Femto Handover in a specific HNB-GW service. By default, it is disabled.

no

Disables the Femto To Femto Handover option in a specific HNB-GW service.

Usage Guidelines

Use this command to enable or disable the Femto To Femto Handover in a specific HNB-GW service.

Examples

The following command sets the default value of Femto To Femto Handover in a specific HNB-GW service:

default iurh-handoff
This command is used to configure the IURH Relocation Guard Timer in a specific HNB-GW service. If F2F handover does not happen within the guard time, the procedure is aborted.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration
configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

**Syntax Description**

```
| default | iurh-handoff-guard-timer  timer_seconds
```

**default**
Sets the default value of IURH Relocation Guard Timer. By default, the IURH Relocation Guard Timer value is 15 seconds.

```
timer_seconds
```

*timer_seconds* is the number of seconds, an integer ranging from 10 to 30.

**Usage Guidelines**
Use this command to configure the IURH Relocation Guard Timer in a specific HNB-GW service.

**Examples**
The following command sets the default value of the IURH Relocation Guard Timer in a specific HNB-GW service:
```
default iurh-handoff-guard-timer 20
```
**mocn-max-reroute-attempts**

This command configures the maximum number of operators who can be attempted in the reroute procedure.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

```configure > context context_name > hnbgw-service service_name```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-hnbgw-service)#
```  

**Syntax Description**

```mocn-max-reroute-attempts  max_attempts```

- **default mocn-max-reroute-attempts**

  - **default**
    
    Sets / Restores default value assigned for maximum number of operators who can be attempted in the reroute procedure. The default value is 4.

  - **max_attempts**
    
    `max_attempts` is an integer ranging from 1 through 8.

**Usage Guidelines**

Use this command to configure the maximum number of operators who can be attempted in the reroute procedure.

**Examples**

The following command configures the maximum number of operators who can be attempted in the reroute procedure as 5:

```mocn-max-reroute-attempts 5```
mocn-reroute-timeout

This command configures the timeout for the individual reroute procedure with one operator.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

`configure > context context_name > hnbgw-service service_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-hnbgw-service)#
```

**Syntax Description**

```
mocn-reroute-timeout  timeout_value
default mocn-reroute-timeout
```

**default**
Sets / Restores default timeout value for the individual reroute procedure with one operator. The default value is 5.

**timeout_value**

`timeout_value` is an integer ranging from 1 through 5.

**Usage Guidelines**
Use this command to configure the timeout for the individual reroute procedure with one operator.

**Examples**
The following command configures the timeout for the individual reroute procedure with one operator. 4:

```
mocn-reroute-timeout 4
```
paging cs-domain

Configures paging optimization parameters for CS domain in the HNB-GW service instance.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

```
configure > context context_name > hnbgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

**Syntax Description**

```
paging cs-domain { handle-unknown-imsi { use-cn-paging-area | use-whitelist } } | phase1 page-last-known-hnb timeout timeout_val1 | phase2 paging-grid-fan-out timeout timeout_val2 | phase3 paging-area-fan-out timeout timeout_val3 }
no paging cs-domain { handle-unknown-imsi { use-cn-paging-area | use-whitelist } } | phase1 page-last-known-hnb | phase2 paging-grid-fan-out | phase3 paging-area-fan-out 
default paging cs-domain { handle-unknown-imsi { use-cn-paging-area | use-whitelist } } | phase1 page-last-known-hnb timeout | phase2 paging-grid-fan-out timeout | phase3 paging-area-fan-out timeout }
```

default

Sets the default behavior of paging optimization configuration for the a specific HNB-GW service.

no

Removes paging optimization configuration for an appended option in a specific HNB-GW service.

**handle-unknown-imsi**
Handles Unknown IMSIs Options.

**use-cn-paging-area**
Uses paging area provided by Core Network for forwarding the Page Req to all open/hybrid HNBs.

**use-whitelist**
Uses whitelist of HNBs for forwarding the Page req to all closed/hybrid HNBs.
phase 1
Paging Phase 1 Configuration - Forwards Page Req to last-known-hnb.

page-last-known-hnb
Page the last known HNB for the call.

timeout `timeout_val1`
Sets the timeout value in seconds for the last-known-hnb paging configuration. It is an integer value ranging from 1 to 30.

phase 2
Paging Phase 2 Configuration - Forwards Page Req to all HNBs in the Grid of last-known-hnb.

paging-grid-fan-out
Pages the last known paging grid.

timeout `timeout_val2`
Sets the timeout value in seconds for the grid fan-out paging configuration. It is an integer value ranging from 1 to 30.

phase 3
Paging Phase 3 Configuration - Forwards Page Req to all HNBs in the LAI of last-known-hnb.

paging-area-fan-out
Pages the last known paging area.

timeout `timeout_val3`
Sets the timeout value in seconds for the area fan-out paging configuration. It is an integer value ranging from 1 to 30.

Usage Guidelines
Use this command to configure the CS domain paging optimization parameters for a specific HNB-GW service instance.

Examples
The following command configures the CS domain paging optimization for grid fan-out timeout as 15 seconds for a specific HNB-GW service:
paging cs-domain phase2 paging-grid-fan-out timeout 15
paging imsi-purge-timer

Configures paging optimization based on the timer for purging the unregistered IMSIs in the HNB-GW service instance.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbgw-service)#

**Syntax Description**

paging imsi-purge-timer timeout timeout_val1
default paging imsi-purge-timer timeout
default

Sets the default value for the IMSI purge timer as 3 hours.

timeout_val1

Sets the timeout value for the IMSI purge timer in hours. It is an integer ranging 1 to 12.

**Usage Guidelines**

Use this command to configure the timer value for purging the unknown IMSIs for paging optimization configuration in a specific HNB-GW service instance.

**Examples**

The following command configures the IMSI purge timer as 4 hours for a specific HNB-GW service instance:

paging imsi-purge-timer timeout 4
**paging ps-domain**

Configures paging optimization parameters for PS domain in the HNB-GW service instance.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbgw-service)#

**Syntax Description**

paging ps-domain { handle-unknown-imsi { use-cn-paging-area | use-whitelist } | phase1 page-last-known-hnb timeout timeout_val1 | phase2 paging-grid-fan-out timeout timeout_val2 | phase3 paging-area-fan-out timeout timeout_val3 }

no paging ps-domain { handle-unknown-imsi { use-cn-paging-area | use-whitelist } | phase1 page-last-known-hnb | phase2 paging-grid-fan-out | phase3 paging-area-fan-out }

default paging ps-domain { handle-unknown-imsi { use-cn-paging-area | use-whitelist } | phase1 page-last-known-hnb timeout | phase2 paging-grid-fan-out timeout | phase3 paging-area-fan-out timeout }

default

Sets the default behavior of paging optimization configuration for the a specific HNB-GW service.

no

Removes paging optimization configuration for an appended option in a specific HNB-GW service.

handle-unknown-imsi

Handles Unknown IMSIs Options.

use-cn-paging-area

Uses paging area provided by Core Network for forwarding the Page Req to all open/hybrid HNBs.

use-whitelist

Uses whitelist of HNBs for forwarding the Page req to all closed/hybrid HNBs.
 phase1
Paging Phase1 Configuration - Forwards Page Req to last-known-hnb.

page-last-known-hnb
Page the last known HNB for the call.

timeout timeout_val1
Sets the timeout value in seconds for the last-known-hnb paging configuration. It is an integer value ranging from 1 to 30.

 phase2
Paging Phase2 Configuration - Forwards Page Req to all HNBs in the Grid of last-known-hnb.

paging-grid-fan-out
Pages the last known paging grid.

timeout_val2
Sets the timeout value in seconds for the grid fan-out paging configuration. It is an integer value ranging from 1 to 30.

 phase3
Paging Phase3 Configuration - Forwards Page Req to all HNBs in the LAI of last-known-hnb.

paging-area-fan-out
Pages the last known paging area.

timeout_val3
Sets the timeout value in seconds for the area fan-out paging configuration. It is an integer value ranging from 1 to 30.

Usage Guidelines
Use this command to configure the PS domain paging optimization parameters for a specific HNB-GW service instance.

Examples
The following command configures the PS domain paging optimization grid fan-out timeout as 20 seconds for a specific HNB-GW service:

  paging ps-domain phase2 paging-grid-fan-out timeout 15
paging open-hnb

Configures paging optimization parameters for open HNBs connected through Open Access mode in the HNB-GW service instance. In this release it is used to configure paging optimization for Open Access mode support only. This command is deprecated release 15.0 onwards. Paging optimization can be configured using other paging commands available in this chapter.

Important

From Release 14.0 and onward this command is part of HNB-Global Configuration Mode.

Important

From Release 16 and later, this command has been deprecated.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-hnbgw-service)#

Syntax Description

paging open-hnb [hnb-where-ue-registered fallback | {always | never | only-if-with-paging-area}]
default paging open-hnb

default

Sets the default behavior of paging optimization configuration for an open HNB while using Open Access mode support.

By default the HNB-GW pages open HNBs only if paging-area IE is received in the paging message.

{always | never | only-if-with-paging-area}

Sets the HNB-GW service instance to page open HNB for a paging message.

always: Sets the system to ALWAYS page the open HNBs irrespective of paging-area IE is received in paging messages.

never: Sets the system to NEVER page any open HNB.
**only-if-with-paging-area**: Sets the system to page the open HNBs only when **paging-area** IE is received in paging messages.

**hnb-where-ue-registered fallback** {always | never | only-if-with-paging-area}
Sets the HNB-GW service instance to page open HNB from where the UE is registered.

**always**: Sets the system to ALWAYS page the open HNBs from where the UE is registered. If the UE is not registered then it pages the open HNBs irrespective of **paging-area** IE is received in paging messages.

**never**: Sets the system to page the open HNBs from where the UE is registered. If the UE is not registered then it NEVER pages any open HNB.

**only-if-with-paging-area**: Sets the system to ALWAYS page the open HNBs from where the UE is registered. If the UE is not registered then it pages the open HNBs only when **paging-area** IE is received in paging messages.

**Usage Guidelines**
Use this command to configure the paging optimization parameters for open HNBs connected through Open Access mode in HNB-GW service instance.

**Examples**
The following command configures the HNB-GW service instance to page an open HNB from where the UE is connected and paging-area IE is received in paging message:

```
paging open-hnb hnb-where-ue-registered fallback only-if-with-paging-area
```
radio-network-plmn

Creates, remove and enters the HNB-RN-PLMN Configuration mode. In this mode you can configure various parameters for radio network public mobile land networks (PLMNs). A maximum of 16 radio PLMN-IDs can be configured in an HNB-GW service.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbgw-service)#

Syntax Description

radio-network-plmn mcc mcc_num mnc mnc_num [ -noconfirm ]

no radio-network-plmn mcc mcc_num mnc mnc_num

no

Removes the configured radio network PLMN identifier for an HNB-GW service.

Caution

Removing the PLMN-ID is a disruptive operation; the HNB-GW service will be re-started.

mcc mcc_num

Specifies the mobile country code (MCC) part of radio network PLMN identifier as an integer value from 101 through 998.

mnc mnc_num

Specifies the mobile network code (MNC) part of radio network PLMN identifier as a 2- or 3-digit integer from 01 through 998.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.
Usage Guidelines

Use this command to configure the radio network PLMN identifier for an HNB-GW service. This command also creates a configuration mode to configure various parameters for defined radio network PLMN identifier in HNB-GW service.

⚠️ Caution

Changing or removing the PLMN-ID is a disruptive operation; the HNB-GW service will be re-started.

Entering this command results in the following prompt:

```
{context_name}@hostname(config-radio-network-plmn)#
```

A maximum of 16 radio network PLMN identifiers are supported for an HNB-GW service.

Examples

The following command configures the radio network PLMN identifier with MCC value as 102 and MNC value as 20 for an HNB-GW service:

```
radio-network-plmn mmc 102 mnc 20
```
**ranap reset**

Configures various Radio Access Network (RAN) Application Part reset procedure parameters in an HNB access network.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

```plaintext
configure > context context_name > hnbgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-hnbgw-service)#
```

**Syntax Description**

```plaintext
ranap reset {ack-timeout timer_value | guard-timeout g_timer | hnbgw-initiated | max-retransmissions retries}
default ranap reset {ack-timeout | guard-timeout | hnbgw-initiated | max-retransmissions }
no ranap hnbgw-initiated
default
```

**default**

Resets the RANAP RESET parameters on HNB-GW service instance.

**no**

Disables the RANAP RESET procedure related parameters in an HNB-GW service instance.

**ack-timeout timer_value**

Sets the timer value (in seconds) to wait for Reset Acknowledge from SGSN/MSC. This is used during HNB-GW initiated RANAP RESET procedure in HNB-GW service instance.

*timer_value* is an integer value from 5 through 10. Default: 10

**guard-timeout g_timer_value**

Sets the timer value (in seconds) to send Reset Acknowledge to SGSN/MSC. After this duration the HNB-GW sends RESET-ACK to SGSN/MSC. This is used during SGSN/MSC initiated RANAP RESET procedure in HNB-GW service instance.

*g_timer_value* is an integer value from 5 through 10. Default: 10
hnbgw-initiated
Enables the HNB-GW Initiated RANAP RESET procedures. Default: Disabled

max-retransmission retries
Sets the maximum number of retries allowed for transmission of RESET-ACK message to SGSN/MSC. This is used during RANAP RESET procedure in HNB-GW service instance.

retries is an integer value from 0 through 2. When 0 is used retransmission is disabled. Default: 1

Usage Guidelines
Use this command to configure the RANAP RESET procedure related parameters in HNB-GW service.

Examples
The following command configures the HNB-GW initiated RANAP RESET Procedure for an HNB-GW service:

`ranap reset hnbgw-initiated`
rtcp report

Enables or disables the generation of RTP Control Protocol (RTCP) packet/report types on a per HNB-GW service instance basis. It also sets the time interval in seconds between two consecutive RTCP reports.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-hnbgw-service)#

Syntax Description
rtcp report interval dur
{ no | default } rtcp report interval

no
Disables the RTCP report generation on HNB-GW service. When RTP configuration is not explicitly mentioned, this is the default behavior.

default
Restores the report interval value to its default value of 5 seconds.

interval dur
Sets the time interval (in seconds) between two consecutive RTCP reports as an integer from 5 through 30. Default: 5

Usage Guidelines
Use this command to configure the enabling or disabling of the generation of RTCP packet/report types on a per HNB-GW service instance basis and sets the specified time interval in seconds between two consecutive RTCP reports.

RTCP enables the receiver to detect if there is any packet loss and needs to compensate for any delay jitter. RTP and RTCP protocols work independently of the underlying Transport layer and Network layer protocols.

Whenever this command is disabled, RTCP report generation stops from the next expiry of the previously configured interval and after enabling, reports are generated only for the calls that established as new calls in the future. For existing calls reports generated as per configuration in place.
RTP reports are generated for each RAB for RTP received from and sent to IuH interface.

- **Important**
  The same interval is applicable for all kinds of RTCP packets/reports across all sessions on an HNB-GW service.

**Examples**

The following command configures the RTCP report generation interval to 15 seconds on an HNB-GW service for RTP stream:

```
rtp report interval 15
```
**rtp address**

Configures the Real Time Protocol (RTP) address on HNB-GW used to map RTP streams while HNB-GW connects to MSC/VLR through an IuCSoIP (IuCS-over-IP) tunnel. This command is used for RTP stream management on HNB-GW.

This command is obsolete. Use **ip pool** or **ipv6 pool** command in Context Configuration mode for IP pool configuration for RTP stream management.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

```
configure > context context_name > hnbgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

**Syntax Description**

- **rtp address address**
- **no rtp address**

- **no**
  
  Removes the RTP IP address association to be used for communication between HNB and HNB-GW while communicating with MSC/VLR-GW through IuCS over IP tunnel.

- **address address**

  Specifies the IP address of HNB-GW to use as an end point by HNB and HNB maps the RTP streams with this IP address and HNB-GW communicates with MSC/VLR through IuCS-over-IP Tunnel.

  *address* is the same IP address as assigned to HNB-GW to communicate with HNB and must be an IP address in IPv4 or IPv6 notation.

**Important**

This command cannot be entered more than once. Only one RTP IP address can be configured for one HNB-GW service.


**Usage Guidelines**

Use this command to enable the HNB-GW IP address as RTP IP address and send the same to HNB to map RTP streams while HNB-GW communicates with MSC/VLR through IuCS-over-IP tunnel.

This command is used for RTP stream management on HNB-GW.

**Examples**

The following command sets the RTP IP address 10.2.3.4 on HNB-GW to communicate with HNB while using IuCS-over-IP tunnel with CS network:

```
rtp address 10.2.3.4
```
rtp port

Configures the Real Time Protocol (RTP) port range to listen from HNB while connecting to MSC/VLR through an IuCSoIP (IuCS-over-IP) interface. This command is used for RTP stream management on HNB-GW. This command is obsolete. Use **ip pool** or **ipv6 pool** command in Context Configuration mode for IP pool configuration for RTP stream management.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

```
configure > context context_name > hnbgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-hnbgw-service) #
```

**Syntax Description**

```
rtp port range port_start to port_end
default rtp port range
```

**default**
Sets the RTP port range to default range from 16384 to 65535.

```
port range range_start to range_end
```

Specifies the port number range to be used by HNB to map the RTP streams and HNB-GW listen on these ports while communicating with MSC/VLR through IuCS-over-IP tunnel.

- `range_start` must be an integer between 16384 through 65535 and should be less than `range_end`.
- `range_end` must be an integer between 16384 through 65535 and should be more than `range_start`.

Default: port 16384 through 65535

**Important**

This command cannot be entered more than once. Only one range of RTP port can be configured for one HNB-GW service.
Usage Guidelines

Caution
This command is NOT active now.

Use this command to assign the RTP port range to be used by HNB to map RTP streams and HNB-GW listen these ports for RTP streams while communicating with MSC/VLR through IuCS-over-IP tunnel.
This command is used for RTP stream management on HNB-GW.

Examples
The following command sets the RTP port number 20000 to 21000 on HNB-GW to listen from HNB for RTP streams while connecting with MSC/VLR using IuCS-over-IP tunnel.
rtp port range 20000 to 21000
**rtp mux**

Configures the HNB-GW service to allow an Home-NodeB to multiplex multiple RTP streams in one IP packet. This support is provided for RTP stream management feature on HNB-GW.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbgw-service)#

**Syntax Description**

`[no | default] rtp mux`

**default**

Sets the multiplexing option to default state of "disabled".

**no**

Removes the configured option to multiplex multiple RTP stream in one packet by Home-NodeB in HNB-GW configuration.

**Usage Guidelines**

Use this command to allow an Home-NodeB to multiplex multiple RTP streams in one IP packet. This configuration support is provided for RTP stream management feature on HNB-GW and it is disabled by default.

**Examples**

The following command sets the HNB-GW to allow HNB to multiplex multiple RTP stream in one packet:

`rtp mux`
sctp bind

Configures the SCTP IP address and port that is used for binding the SCTP socket to communicate with the Home-NodeB over an Iuh interface within an HNB-GW service.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration
configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-hnbgw-service)#
```

**Syntax Description**

```
sctp bind { address IPv4_address | port port_num }
no sctp bind { address | port }
```

no
Removes the SCTP binding.

**address IPv4_address**

Specifies the IP address of the HNB-GW Iuh interface in IPv4 dotted-decimal.

**port port_num**

Specifies the SCTP port number to communicate with the Home-NodeBs using Iuh interface as an integer form 1 through 65535.

**Usage Guidelines**

Use this command to assign the SCTP IP address and port with SCTP socket on HNB-GW to communicate with the Home-NodeB using Iuh interface. This SCTP configuration provides the IP-address and listen port where HNB-GW service shall bind to listen for incoming SCTP associations from HNB.

**Examples**

The following command sets the SCTP port number 999 on HNB-GW to listen from Home-NodeB over Iuh interface:

```
sctp bind port 999
```
The following command sets the SCTP address 10.2.3.4 of HNB-GW to use with Home-NodeB over Iuh interface:

sctp bind address 10.2.3.4
**sctp checksum-type**

Configures SCTP checksum-type.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Syntax Description**

`sctp checksum-type { adler32 | crc32 }

default sctp checksum-type

default
Sets the SCTP checksum-type.

`adler32`
 Specifies the SCTP checksum-type ADLER32.

`crc32`
 Specifies the SCTP checksum-type CRC32.

**Usage Guidelines**

Use this command to configure SCTP checksum-type.

**Examples**

The following command sets the SCTP checksum-type to adler32 on HNB-GW:

`sctp checksum-type adler32`
sctp connection-timeout

Configures the SCTP connection timeout duration to explicitly remove the SCTP association with a non-responsive HNB in an HNB-GW service.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

```
configure > context context_name > hnbgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

**Syntax Description**

```
sctp connection-timeout dur
{ default | no } sctp connection-timeout

no

Disables the connection time out configuration on HNB-GW service.

default

Restores the connection timeout duration value to its default value of 10 seconds.

```

dur

Sets the connection timeout duration (in seconds) after which the association is explicitly removed. In case of an HNB de-registration scenario, the HNB-GW waits for configured amount time before initiating the procedure to clear the SCTP association.

```

dur is an integer from 5 through 30. Default: 10
```

**Usage Guidelines**

Use this command to configure the minimum duration value before removing the SCTP association between a non-responding HNB and HNB-GW. If HNB registration not happened within the configured period after the SCTP association is established then the SCTP association is explicitly removed. In a scenario where an HNB de-registered due to any reason, the HNB-GW waits for the configured amount of time before initiating the procedure to clear the SCTP association.
Examples

The following command sets the SCTP connection timeout duration to 15 second on HNB-GW after expiry of which the SCTP association is removed:

```
sctp connection-timeout 15
```
**sctp cookie-life**

Configures the SCTP valid cookie-life, Min 5000ms and Max 120000ms with granularity of 100ms.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

```
configure > context context_name > hnbw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbw-service)#
```

**Syntax Description**
```
sctp cookie-life dur
default sctp cookie-life
```

- **default**
  Restores the SCTP cookie-life value.

- **dur**
  Sets the SCTP cookie-life (in seconds).
  - *dur* is an integer from 50 through 1200.

**Usage Guidelines**
Use this command to configure the SCTP valid cookie-life.

**Examples**
The following command sets the SCTP cookie-life value to 55 on HNB-GW:
```
sctp cookie-life 55
```
**sctp heart-beat-timeout**

Configures the SCTP heartbeat timer parameters for SCTP connection over an IuH interface in an HNB-GW service instance.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

`configure > context context_name > hnbgw-service service_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-hnbgw-service)#
```

**Syntax Description**

```
sctp heart-beat-timeout dur
{ default | no } sctp heart-beat-timeout
```

**no**
Disables the heartbeat timer configuration for SCTP over IuH in HNB-GW service instance.

**default**
Restores the default time out value for heartbeat timer to 30 seconds.

**dur**
Sets the heartbeat timer timeout duration (in seconds) after which the next heartbeat command is sent to HNB from HNB-GW in SCTP over an IuH interface. In an HNB de-registration scenario, the HNB-GW waits for configured amount time before initiating the procedure to clear the SCTP association.

`dur` is an integer from 1 through 300. Default: 30

**Usage Guidelines**

Use this command to configure the minimum duration value before retransmitting the HEARTBEAT chunk to HNB from HNB-GW in SCTP transmission. By default HNB-GW monitors the reachability of the idle HNBs by sending a HEARTBEAT chunk periodically to the HNB address.

Each time the HEARTBEAT timer expires on any address, or when a HEARTBEAT sent to an idle address is not acknowledged within a Retransmission Timeout duration, the error counter of that HNB incremented.
When the value in the error counter exceeds the protocol parameter for maximum retransmission for that destination address, the HNB-GW mark the destination HNB as inactive and a notification is sent to the upper layer.

**Examples**

The following command sets the SCTP HEARTBEAT timeout duration to 15 second on HNB-GW after expiry of which the HNB-GW retransmits the HEARTBAT chunk to HNB over SCTP association:

```
sctp heart-beat-timeout 15
```
**sctp mtu-size**

This command configures SCTP mtu-size, Min 508 bytes and Max is 65535 bytes with granularity of 1 byte.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local] host_name (config-hnbgw-service) #

**Syntax Description**

sctp mtu-size { max | min | start } size

default sctp mtu-size { max | min | start }

default

Sets the SCTP mtu-size to its default value.

size

size is an integer from 508 through 65535.

**Usage Guidelines**

Use this command to configure the SCTP mtu-size.

**Examples**

The following command configures the SCTP mtu-size max value to 555 on HNB-GW:

sctp mtu-size max 555
**sctp rto**

This command sets the SCTP Retransmission Timeout value.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

`configure > context context_name > hnbgw-service service_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

**Syntax Description**

```
sctp rto { initial initial_value | max max_value | min min_value }
default sctp rto { initial | max | min }
```

**default**

Sets the SCTP Retransmission Timeout value to default.

**initial_value**

`initial_value` is SCTP Retransmission Timeout initial value, which is an integer from 1 through 1200.

**max_value**

`max_value` is SCTP Retransmission Timeout max value (Min 500 ms and max 120000 ms with granularity of 100 ms), which is an integer from 5 through 1200.

**min_value**

`min_value` is SCTP Retransmission Timeout max value (Min 100 ms and max 5000 ms with granularity of 100 ms), which is an integer from 1 through 50.

**Usage Guidelines**

Use this command to set the SCTP Retransmission Timeout value.

**Examples**

The following command sets the SCTP max Retransmission Timeout value to 555 on HNB-GW:

```
sctp rto max 555
```
sctp sack-frequency

This command configures the SCTP Selective Ack Frequency.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-hnbgw-service)#

**Syntax Description**

sctp sack-frequency value
default sctp sack-frequency

**default**

Sets the SCTP sack-frequency value to default.

**value**

Min value is 1 and Max value is 5.

**Usage Guidelines**

Use this command to configure the SCTP Selective Ack Frequency.

**Examples**

The following command configure the SCTP Selective Ack Frequency to 5 on HNB-GW:

sctp sack-frequency 5
**sctp sack-period**

This command is used to configure SCTP Selective Ack Period in Seconds.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

```
configure > context context_name > hnbgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-hnbgw-service)#
```

**Syntax Description**

```
sctp sack-period value
default sctp sack-period
```

**default**

Sets the SCTP sack-period value to default.

**value**

Min 0 ms and Max is 500ms with granularity of 100ms.

**value** is an integer from 0 through 5.

**Usage Guidelines**

Use this command to configure the SCTP Selective Ack Period in Seconds.

**Examples**

The following command configures the SCTP Selective Ack Period in Seconds to 5 on HNB-GW:

```
sctp sack-period 5
```
security-gateway bind

Binds the SeGW in an HNB-GW service to a logical IP interface serving as an Iuh interface and associates an IPsec IKEv2 crypto-map template.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

```
configure > context context_name > hnbgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-hnbgw-service)#
```

**Syntax Description**

- `security-gateway bind address IPv4_address crypto-template cryp_name [ context ctxt_name]`
- `no security-gateway bind`

**no**

Removes a previously configured IPSec IP address use for binding the IKEv2 IPSec tunnel (local bind address) to communicate with the Home-NodeBs using Iuh interface.

- `bind address IPv4_address`

Specifies the IP address for the Iuh interface for the IPSec tunnel. This is the IP address where the HNB-GW service is bound and that is provided to the Home-NodeB during HNB-GW discovery.

The IP address is expressed in IPv4 dotted-decimal.

- `crypto-template cryp_name`

Specifies the Crypto-map template to be used for IPsec IKEv2 tunneling for the interface configured as an Iuh.

`cryp_name` specifies the name of the pre-configured Crypto-map template which is configured in Crypto-Map Template Configuration mode and associated with the HNB-GW service to create an IPSec tunnel with a Home-NodeB during HNB-GW discovery procedure over an Iuh interface.

- `context ctxt_name`

Specifies the name of the pre-configured context in which the Security Gateway service is configured. By default this command uses the HNB-GW service context for the security Gateway configuration.
Usage Guidelines

Use this command to associate or tie the HNB-GW service to a specific logical IP address that is used for binding the Iuh socket to communicate with the Home-NodeB using IPSec tunnel. A maximum of one IP address can be configured with this command for one HNB-GW service.

The HNB-GW passes the IP address during setting up the HNB-GW discovery procedure with the Home-NodeB.

⚠️ Caution

This is a critical configuration. The HNB-GW service cannot be started without this configuration. Any change to this configuration would lead to restarting the HNB-GW service and removing or disabling this configuration stops the HNB-GW service.

Examples

The following command binds the logical IP interface with the address of 10.2.3.4 to the HNB-GW service using existing IPsec Crypto-Map template crypto1 to establish IPSec tunnel with Home-NodeB:

```
security-gateway bind address 10.2.3.4 crypto-template crypto1
```

The following command disables a binding that was previously configured:

```
security-gateway bind address 12.34.44.56
```
**sessmgr-to-cbsmgr-pacing-timer**

This command configures pacing timer value for SABP messages being sent from Sessmgr to CBSmgr. Default value is 100ms.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration
configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-hnbgw-service)#
```

**Syntax Description**

`sessmgr-to-cbsmgr-pacing-timer milli_seconds`

`milli_seconds`

Pacing timer value in milliseconds which is an integer from 10 through 500.

**Usage Guidelines**

Use this command to configure pacing timer value for SABP messages being sent from Sessmgr to CBSmgr.

**Examples**

The following command sets pacing timer value for SABP messages being sent from Sessmgr to CBSmgr to 50:

`sessmgr-to-cbsmgr-pacing-timer 50`
tnnsf-timer

Configures the NAS Node Selection Function (NNSF) timer (T-NNSF) which is used by the HNB-GW to store the IMSI and the relevant Global-CN-ID in the short term after Paging. This timer is used for Iu-Flex feature support.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

```
configure > context context_name > hnbgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

**Syntax Description**

```
{ no | default } tnsf-timer
```

- **no**
  Disables/removes the configured timer value of NNSF timer (T-NNSF) from HNB-GW service instance.

- **default**
  Sets the timer value of NNSF timer (T-NNSF) for HNB-GW service instance to default value of 30 seconds.

```
tnsf-timer dur
```

Configures the NNSF timer (in seconds) which is used by the HNB-GW to store the IMSI and the relevant Global-CN-ID as an integer from 10 through 60. Default: 30

**Usage Guidelines**

Use this command to configure the NNSF timer value in seconds for Iu-Flex support.

Whenever the MSC sends the paging request with IMSI, the HNB-GW stores the Global_CN_ID of the node which issued the paging request message for the given IMSI and HNB-GW starts the `tnnsf-timer`. HNB-GW stores the mapping of IMSI to Global_CN_ID until the `tnnsf-timer` expires.

**Examples**
The following command sets the NNSF timer value to 30 seconds in an HNB-GW service instance:

```
default tnsf-timer
```
**ue registration-timeout**

Configures the UE registration timeout duration to de-register the connected UE from an HNB-GW service.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbgw-service)#

**Syntax Description**

`ue registration-timeout dur`

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>{ default</td>
<td>no }</td>
</tr>
<tr>
<td><code>default</code></td>
<td>Restores the UE registration timeout duration value to its default value of 120 seconds.</td>
</tr>
<tr>
<td><code>dur</code></td>
<td>Sets the UE registration timeout duration (in seconds) after which the UE is de-registered from HNB-GW. In a scenario when all Iu connections are released for a subscriber, the HNB-GW service de-registers the UE after the configured duration only.</td>
</tr>
</tbody>
</table>

**dur**

is an integer from 60 through 300. Default: 120

**Usage Guidelines**

Use this command to configure the minimum duration value before de-registering the UE when subscriber fails to establish the Iu connection. If subscriber's Iu session does not established before configured period then UE is de-registered. Also in a scenario where all Iu connections are released for a subscriber, the HNB-GW service waits for configured period before starting UE deregistration procedure.

**Examples**

The following command sets the UE registration timeout duration to 150 second on HNB-GW after expiry of which the UE is de-registered:

`ue registration-timeout 150`
HNB-CS Network Configuration Mode Commands

The HNB-CS Network configuration mode provides the commands to create, provide, and manage the circuit switched (CS) network instance allowing the Home Evolved NodeB Gateway (HNB-GW) access with the CS core network in a 3G UMTS network.

**Command Modes**  
**Exec > Global Configuration > HNB-CS Network Configuration**

**configure > cs-network cs_instance**

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-cs-network-instance_id)#
```

**Important**

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

- associate aclap-service, page 1485
- associate rtp pool, page 1487
- associate sccp-network, page 1489
- end, page 1491
- exit, page 1492
- global-rnc-id, page 1493
- iu-rtcp-interval, page 1495
- map core-network-id, page 1496
- map idnns, page 1498
- map lac, page 1500
- map nri, page 1502
- msc deadtime, page 1504
- msc point-code, page 1506
- nri length, page 1508
- null-nri, page 1510
- offload-msc, page 1512
- ranap reset, page 1514
- sccp, page 1516
associate alcap-service

Associates a previously defined Access Link Control Application Part (ALCAP) service with the CS network instance for multiplexing of different users onto one AAL2 transmission path using channel IDs (CIDs). This configuration is provided to support IuCS-over-ATM functionality.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > HNB-CS Network Configuration

configure > cs-network cs_instance

Entering the above command sequence results in the following prompt:

[local] host_name(config-cs-network-instance_id)#

Syntax Description

associate alcap-service svc_name context ctx_name

no associate alcap-service

no
Removes the associated ALCAP service from this HNB-CS network instance configuration.

svc_name
Identifies the name of the ALCAP service preconfigured in Context configuration mode to associate with an HNB-CS network instance for multiplexing of different users onto one AAL2 transmission path using channel IDs (CIDs).

svc_name must be a preconfigured ALCAP service.

Only one instance of this command can be configured.

⚠️ Caution
If this CLI is not configured any RAB-ASST-REQ requesting AAL2 connection setup shall be rejected with an appropriate cause.

cxtextsctx_name

Specifies the name of the context in which ALCAP service is configured.

cxctx_name must be an existing context name in which this ALCAP service is configured.
Usage Guidelines

Use this command to configure IuCS-over-ATM support. This association of ALCAP protocol service configuration in HNB-CS network instance provides multiplexing of different users onto one AAL2 transmission path using channel IDs (CIDs).

⚠️ Caution

If this CLI is not configured any RAB-ASST-REQ message requesting AAL2 connection setup shall be rejected with an appropriate cause.

⚠️ Important

This command must not be used more than once to configure IuCS-over-ATM support.

Examples

Following command associates ALCAP service alcap_svc1 configured in context named Ctx_alcap1 with specific HNB-CS network instance:

```
associate alcap-service alcap_svc1 context ctx_alcap1
```
associate rtp pool

Associates a previously defined RTP pool (IP pool) with the CS network instance to be used for assignment of IP address/port as RTP streams end point address over IuCS interface. This configuration support is provided for RTP stream management feature in an HNB-GW service.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > HNB-CS Network Configuration

configure > cs-network cs_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-cs-network-instance_id)#

Syntax Description

associate rtp pool pool_name context ctx_name

no associate rtp pool

no

Removes the associated RTP pool (IP pool) from this HNB-CS network instance configuration.

pool_name

Identifies the name of the RTP IP pool preconfigured in Context configuration mode to associate with an HNB-CS network instance to be used for assignment of IP address/port over the IuCS interface RTP streams. pool_name must be an existing IP pool name configured in Context configuration mode.

Important
For IP pool (RTP pool) configuration, refer Context Configuration Commands Mode chapter.

cntxtctx_name

Specifies the name of the context in which RTP pool (IP pool) is configured.

cntx_name must be an existing context name in which this IP pool is configured.
Usage Guidelines

Use this command to associate RTP pool (IP Pool) with an HNB-CS network instance for allotment of IP address/port over IuCS interface for RTP streams across all sessions. A fixed range of RTP ports from 5000 through 65000 shall be used to allocate to RTP stream.

Important
This command must be used to provide IP address/port for RTP streams end point address over IuCS interface.

Important
This configuration support is provided for RTP stream management feature on an HNB-GW service.

Examples

Following command associates RTP pool named rtp_1 with specific HNB-CS network instance:
associate rtp pool rtp_1
associate sccp-network

Associates a predefined Signaling Connection Control Part (SCCP) network ID with the CS network instance in order to route the messages towards MSC/VLR over IuCS interface.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > HNB-CS Network Configuration

configure > cs-network cs_instance

Entering the above command sequence results in the following prompt:

[local] host_name(config-cs-network-instance_id)#

Syntax Description
associate-sccp-network sccp_net_id
no associate-sccp-network

no

Removes the associated SCCP network ID from this HNB-CS network instance configuration.

sccp_network_id

Identifies the predefined SCCP network ID to associate with an HNB-CS network instance over IuCS/IuFlex interface to enable connection with MSC/VLR(s). 

sccp_network_id must be a predefined SCCP network ID in Global configuration mode.

Usage Guidelines
Use this command to associate a preconfigured SCCP network ID over IuCS interface in HNB-GW service to connect with CS network elements; i.e. MSC.

Important
The SCCP network ID must be defined in Global Configuration mode before using it with this command.

Important
A single SCCP network configuration instance can not be shared with multiple HNB-CS network instances.
Examples

Following command associates SCCP network 2 with specific HNB-CS network instance:

```
associate-sccp-network 2
```
end

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

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

der

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.
global-rnc-id

Configures the Radio Network Concentrator (RNC) identifier in a Radio Network PLMN associated with HNB-CS network configuration instance. The RNC identifier is provided to the HNB during HNB-REGISTRATION.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > HNB-CS Network Configuration

```
configure > cs-network cs_instance
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-cs-network-instance_id)#
```

**Syntax Description**

```
[ no ] global-rnc-id mcc mcc_num mnc mnc_num id rnc_id | common-plmn mcc mcc_num mnc mnc_num
```

- **no**
  Deletes the RNC, MMC, and MNC information from the HNB-CS Network configuration instance.

- **mcc mcc_num**
  Specifies the mobile country code (MCC) part of radio network PLMN identifier as an integer value from 100 through 999.

- **mnc mnc_num**
  Specifies the mobile network code (MNC) part of radio network PLMN identifier as a 2- or 3-digit integer from 00 through 999.

- **common-plmn mcc mcc_num mnc mnc_num**
  Configures the Common PLMN for this CS Network.

  - **mcc mcc_num** specifies mobile country code (MCC) part of Common PLMN for this CS Network as an integer value from 100 through 999.
  - **mnc mnc_num** specifies the mobile network code (MNC) part of Common PLMN for this CS Network as an integer value from 00 through 999.
**Usage Guidelines**

Use this command to configure RNC id to associate Radio Network PLMN which will be sent to HNBs from HNB-GW during HNB-REGISTRATION procedure. Depending upon the requirement the RNC Identifier can be provided at the desired granularity.

**Examples**

The following command configures the HNB-GW service to return an RNC identifier as 102 when an HNB-REGISTRATION request is received with LAC 1, and RAC 2:

```
global rnc-id mcc 102 mnc 02 id 2
```
**iu-rtcp-interval**

This command configures RTCP reporting interval for HNBGW Service on Iu Interface.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > HNB-CS Network Configuration

`configure > cs-network cs_instance`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-cs-network-instance_id)#
```

**Syntax Description**

`iu-rtcp-interval report_generation_interval`

`{ default | no } iu-rtcp-interval`

**default**

Sets the default value assigned for reporting interval for HNBGW Service on Iu Interface.

**no**

Disables RTCP reporting interval for HNBGW Service on Iu Interface.

**report_generation_interval**

Specifies the RTCP report generation interval as an integer from 5 through 30.

**Usage Guidelines**

Use this command to configure RTCP reporting interval for HNBGW Service on Iu Interface.

**Examples**

The following command configures RTCP reporting interval for HNBGW Service as 10 seconds:

```
iu-rtcp-interval 10
```
map core-network-id

Maps/associates the CS core network id to a default Mobile Switching Center (MSC) in network using MSC point code in HNB-CS network to allow HNBs to access UMTS network.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > HNB-CS Network Configuration

configure > cs-network cs_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-cs-network-instance_id) #

**Syntax Description**

map core-network-id cn_id point-code msc_point_code

no map core-network-id cn_id

no

Removes the mapping of a CS core network id with particular MSC point code.

**cn_id**

Specifies the core network identifier configured to represent a UMTS CS core network as an integer from 0 through 4095.

Multiple instance of this command can be mapped with different MSC point code.

**point-code msc_point_code**

Specifies the SS7 address of the default MSC in the CS network in point code value to a configured HNB-CS network instance.

**point_code** is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ####### format.

Only one instance of this MSC point code can be mapped with one CS core network id.

**Usage Guidelines**

Use this command to map a UMTS CS core network identifier with a particular MSC point code.

This command can be entered multiple times with same MSC point code to map with one or more CS core network Id, but a particular core network identifier can be mapped to one MSC only.
This command is instrumental in Iu-Flex functionality, whenever HNB-GW receives RESET/RESET-RES messages from MSC with Global CN-ID information element, the response from HNB-GW is sent to the node configured for that particular Global CN-ID.

If the RESET/RESET-RES messages do not have Global CN-ID IE, then the response of those messages is directed to the default MSC which is configured using `msc point-code` command in this mode.

**Examples**

The following command configures the CS core network identifier 101 with an MSC point code 1.2.3:

```
map core-network-id 101 point-code 1.2.3
```

The following command configures the CS core network identifier 102 with the same MSC point code 1.2.3:

```
map core-network-id 102 point-code 1.2.3
```
map idnns

Configures the mapping of Intra-Domain NAS Node Selector (IDNNS) IE received from UE in RUA connect message towards HNB-GW to MSC point code. This is an important configuration for CS network resource sharing over Iu-Flex interface.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > HNB-CS Network Configuration

`configure > cs-network cs_instance`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-cs-network-instance_id)#
```

**Syntax Description**

```
map idnns range idnns_start to idnns_end point-code msc_point_code [ backup point-code bkup_msc_point_code ]
no map idnns range idnns_start to idnns_end
```

**no**

Removes the entries of mapping of range of IDNNS received from UE with particular MSC point code.

**range idnns_start to idnns_end**

Specifies the range of IDNNS received from the UE to map with a particular MSC point code during initial CS core network node selection.

- `idnns_start` is an integer from 0 through 1023 that should be less than `idnns_end`.
- `idnns_end` must be an integer from 0 through 1023 that should be more than `idnns_start`.

The command can be entered more than once to map multiple IDNNS ranges to the same MSC, but overlapping and mapping of the same range to different MSC point codes is not allowed.

**point-code msc_point_code**

Specifies the SS7 address of the MSC in the CS network to map with a range of IDNNS values.

- `msc_point_code` is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ######## format.
**backup point-code bkup_msc_point_code**

Specifies the SS7 address of the MSC to be used as a backup in the CS network to map with a range of IDNNS values.

*bkup_msc_point_code* is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ####### format.

**Usage Guidelines**

Use this command to map a NRI received from UE during initial CS network node selection to MSC point code through NRI range mapping over Iu-Flex interface.

The IDNNS refers to the information element in RUA connect message from UE towards RAN (HNB-GW). In IDNNS IE, if the choice of routing mentioned is other than local P-TMSI, then the value it provides is used against this configuration to map the MSC point code.

If backup MSC point-code is specified, then specified MSC works as backup for the IDNS range configured. This Backup MSC is selected if the mapped MSC for a given IDNNS range is going for offloading using *offload-msc point-code* command.

The command can be entered more than once to map multiple IDNNS ranges to same MSC point code, but overlapping and mapping of same range to different MSC point code is not allowed.

**Examples**

The following command maps the IDNNS range from 101 to 201 with MSC point code 1.2.3 and point code 7.8.9 as backup MSC point code:

```bash
map nri range 101 to 201 point-code 1.2.3 backup point-code 7.8.9
```

The following command removes all IDNNS range matching entries between 301 to 399 from the configuration:

```bash
no map idnns range 301 to 399
```
map lac

Configures the mapping of the Location Area Code (LAC) received from UE to an MSC point code. This is an important configuration for CS network resource sharing without Iu-Flex interface configuration.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > HNB-CS Network Configuration
configure > cs-network cs_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-cs-network-instance_id)#

Syntax Description

map lac range lac_start to lac_end point-code msc_point_code
no map lac range lac_start to lac_end

no

Removes the entries of mapping of range of LACs received from UE with particular MSC point code.

range lac_start to lac_end

Specifies the range of LACs received from UE to map with particular MSC point code during initial CS core network node selection.

lac_start is an integer from 0 through 65535 that should be less than lac_end.
lac_end is an integer from 0 through 65535 that should be more than lac_start.

The command can be entered more than once to map multiple LAC ranges to same MSC, but overlapping is not allowed.

point-code msc_point_code

Specifies the SS7 address of the MSC in the CS network to map with a range of LAC values.

point_code is an SS7 point code in dotted-decimal ####.####.#### or 8-digit decimal ####### format.

Usage Guidelines

Use this command to map a LAC, received from UE during HNB registration, for MSC selection over IuCS interface through LAC range mapping with MSC point code.
This configuration is used during initial CS core network node selection when the LAC from the UE is available. This configuration is used when the core network is not using Iu-Flex interface for MSC selection. The command can be entered more than once to map multiple LAC ranges to same MSC point code.

**Important**

This command can be used together with Iu-Flex configuration, but MSC selection based on LAC takes place only if Iu-Flex is not configured. If both Iu-Flex and LAC are configured then selection of MSC is based on Iu-Flex configuration only.

**Examples**

The following command maps the LAC range from 20 to 50 with MSC point code 1.2.3:

```
map lac range 20 to 50 point-code 1.2.3
```

The following command removes all LAC range matching entries between 20 to 50 from the configuration:

```
no map lac range 20 to 50
```
map nri

Configures the mapping of Network Resource Identifier (NRI) sent from UE to the MSC point code. This is an important configuration for CS network resource sharing over Iu-Flex interface.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > HNB-CS Network Configuration
configure > cs-network cs_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-cs-network-instance_id)#

Syntax Description

map nri range nri_start to nri_end point-code msc_point_code
no map nri range nri_start to nri_end

no

Removes the entries of mapping of range of NRIs received from UE with particular MSC point code.

range nri_start to nri_end

Specifies the range of NRIs received from UE to map with particular MSC point code during initial CS core network node selection.

nri_start is an integer from 0 through 1023 that should be less than nri_end.
nri_end is an integer from 0 through 1023 that should be more than nri_start.

The command can be entered more than once to map multiple NRI ranges to same MSC, but overlapping is not allowed.

point-code msc_point_code

Specifies the SS7 address of the MSC in the CS network to map with a range of NRI values.

point_code is an SS7 point code in dotted-decimal ####.####.#### or 8-digit decimal ####### format.

Usage Guidelines

Use this command to map a NRI received from UE during initial CS network node selection to MSC point code through NRI range mapping over Iu-Flex interface.
This configuration is used during initial CS core network node selection when the network resource identifier (NRI) from the UE is available. The NRI range is mapped to MSC point code. This configuration is used when the core network uses Iu-Flex interface.

The command can be entered more than once to map multiple NRI ranges to same MSC point code.

It is possible to configure multiple ranges to more than one MSC however this configuration is required only when the CS core network is configured as Multi-Operator Core Network (MOCN).

When the CS core network is not MOCN and one range is mapped to more than one MSC then MSC is selected randomly in a non-predictable manner.

**Examples**

The following command maps the NRI range from 101 to 201 with MSC point code 1.2.3:

```
map nri range 101 to 201 point-code 1.2.3
```

The following command maps the NRI range from 301 to 399 with MSC point code 1.2.3:

```
map nri range 301 to 399 point-code 1.2.3
```

The following command removes all NRI range matching entries between 301 to 399 from the configuration:

```
no map nri range 301 to 399
```
**msc deadtime**

Configures a timer on the HNB-GW to manage MSC availability in a CS core network on receiving of a PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from an SCCP instance.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > HNB-CS Network Configuration

configure > cs-network cs_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-cs-network-instance_id)#

**Syntax Description**

`msc deadtime { immediate | dur }`

| no | default | msc deadtime |

- **no**
  
  Marks the peer node (MSC) as always available; it can never be marked down for a specific HNB-CS network instance.

- **default**
  
  Sets the default action for HNB-GW and provisions it as such that the peer node (MSC) is marked down as soon as HNB-GW receives PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP in a specific HNB-CS network instance. Default: Enabled

- **immediate**
  
  Sets the HNB-GW to mark the peer node (MSC) down immediately and clears all Iu-CS connections towards the MSC. Default: Disabled

- **dur**
  
  Sets the duration (in seconds) for a timer that starts when the HNB-GW receives a PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP for a peer MSC. On expiry of this timer the peer MSC is marked as dead and all Iu-CS connections towards that MSC are released.

  `dur` is an integer from 1 through 30.

  Only one instance of this command can be configured.
Usage Guidelines

This command is used to configure a timer on HNB-GW to manage MSC availability in a CS core network on receiving of PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP. This configuration plays important role during RANAP reset procedure as well.

Timer value sets the duration in seconds for a timer which started once HNB-GW receives PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP for a peer MSC. On expiry of this timer the peer MSC is marked as dead and all Iu-CS connections towards that MSC shall be released.

Important

This command can be entered only once. Reentering this command overwrites the previous parameters.

Examples

The following command configures the deadtime timer value for 10 seconds on HNB-GW. Once HNB-GW receives PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP for a peer MSC the HNB-GW waits for configured period and on expiry of timer it marks the specific MSC as dead:

```
msc deadtime 10
```
**msc point-code**

Configures the default MSC point-code within an HNB-CS network instance. This command is used when HNB-GW is to be connected to only one MSC with in a CS network or as default MSC for all HNBs connected through specific HNB-CS network instance.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > HNB-CS Network Configuration

```
configure > cs-network cs_instance
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-cs-network-instance_id)#
```

**Syntax Description**

```
[ no ] msc point-code point_code
```

- **no**
  
  Removes the configured default MSC point code from a specific HNB-CS network instance.

**Caution**

Removing the MSC point code is a disruptive operation and affects all HNB sessions which are connected to particular MSC through an HNB-CS network instance.

**Usage Guidelines**

Use this command to configure a default MSC to which HNB connects for CS network access through HNB-GW service.

Point-code is an SS7 address for an element in the SS7 network. Point-codes must be defined in dotted-decimal format in a string of 1 to 11 digits. Format options include:

- 0.0.1 to 7.255.7 for point-code in the ITU range.
• 0.0.1 to 255.255.255 for point-code in the ANSI range.
• 0.0.1 to 15.31.255 for point-code in the TTC Range.
• a string of 1 to 11 digits in dotted-decimal to represent a point-code in a different range.

**Important**

This command can be entered only once. If entered again the previous value shall be overwritten.

**Examples**

The following command configures a default MSC with point code 101.201.101 for HNBs to access CS network through HNB-GW service in this HNB-CS network instance:

```plaintext
msc point-code 101.201.101
```
nri length

Configures the network resource identifier (NRI) length in bits to identify a specific MSC serving in a pooled area. At least one NRI value has to be assigned to an MSC serving in a pool. The NRI is coded inside of the temporary mobile subscriber identity (TMSI), located within bits 14 to 23 with an variable length between 0 and 10 bits. Operator needs to set this NRI length to indicates the number of bits that shall be used for the NRI field to set the parameters for Iu-Flex (MSC pooling) functionality.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > HNB-CS Network Configuration

configure > cs-network cs_instance

Entering the above command sequence results in the following prompt:
[local]host_name(config-cs-network-instance_id)#

Syntax Description
nri length nri_value
default nri length

default
Sets the NRI length to the default value of 0 and disables the Iu-Flex (MSC pooling) functionality.

nri length nri_value
Default: 0
Specifies the number of bits to be used in the P-TMSI (bits 23 to 18) to define the network resource identifier (NRI). The NRI length configuration also sets the maximum size of the pool. If not configured, the NRI length is of zero length.

length is an integer from 1 to 10 that identifies the number of bits. When a non-zero value is configured the CS network is considered to be a pool.

Usage Guidelines
Use this command to enable the Iu-Flex functionality on HNB-GW. This command identifies a unique MSC serving a pooled area for Iu-Flex functionality and at least one NRI value has to assigned to an MSC serving in a pool. It performs MSC pooling/offloading scenario over Iu-Flex interface. The NRI is stored in the bits 14 to 23 of TMSI. The HNB-GW uses a portion of this NRI to set the parameters for Iu-Flex (MSC pooling) functionality.
If more than one NRI is configured, the HNB-GW service does round-robin between the available NRIs when new subscriber(s) (re)connect.

This command must be used in conjunction with null nri command to configured MSC pooling/offloading over Iu-Flex interface.

**Examples**

The following command sets the HNB-GW to a bit length of 6 to derive the values from the NRI field (stored in bits 14 to 23 of TMSI) to set the parameters for Iu-Flex (MSC pooling) functionality:

```
nri length 6
```
**null-nri**

Configures the null NRI for load redistribution in support of Iu-Flex functionality. The NRI value defined with this command must be unique across the pool areas. This null-NRI is used by HNB-GW for load redistribution during MSC offloading.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > HNB-CS Network Configuration

configure > cs-network cs_instance

Entering the above command sequence results in the following prompt:

\[\text{[local]} \text{host_name(config-cs-network}\text{-instance_id)] \#\]

**Syntax Description**

- **null-nri**  
  - **null_nri_value**
  - **no null-nri**  
    - **null_nri_value**

**null_nri_value**

Specifies the null-NRI value to be used by HNB-GW for load redistribution during MSC offloading as an integer from 0 through 1023.

Without MOCN configuration this value can be entered only once.

For MOCN a unique null-NRI must be assigned to each MOCN operator identified by its PLMN-ID (MCC+MNC).

A 0 (zero) value configured as a null-NRI indicates the keyword is not to be used. There is no default value for this parameter.

**Usage Guidelines**

Use this command to identify the MSC to be used by HNB-GW for load redistribution during MSC offloading over an Iu-Flex interface.

There is one unique null-NRI in a PLMN supporting pool functionality.

Without MOCN configuration this command can be entered only once. For MOCN a unique null-NRI must be assigned to each MOCN operator identified by its PLMN-ID (MCC+MNC).
Examples

The following command sets the null-NRI as 1001 to be used by HNB-GW for load redistribution during MSC offloading:

```
null-nri 1001
```
offload-msc

Provisions the HNB-GW to enable or disable the exclusion of a particular primary MSC node during an NAS Node Selection Function (NNSF) procedure when it needs to be offloaded while using Iu-Flex functionality on the HNB-GW.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > HNB-CS Network Configuration
configure > cs-network cs_instance

Entering the above command sequence results in the following prompt:

> [local]host_name(config-cs-network-instance_id)#

**Syntax Description**

```
[ no ] offload-msc point-code msc_point_code
```

- **no**
  Removes the specified primary MSC point code from the exclusion list for NNSF function on HNB-GW and re-enables the inclusion of the primary MSC to be considered by HNB-GW.

- **point-code msc_point_code**
  Specifies the SS7 address of the primary MSC in the CS network to be excluded for NNSF function on HNB-GW when it needs to be offloaded via Iu-Flex functionality.
  
  *point_code* is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ####### format.
  
  Only one instance of this primary MSC point code can be mapped with one CS core network id.

**Usage Guidelines**

Use this command to provision the HNB-GW to enable or disable the exclusion of the primary MSC node when it needs to be offloaded.

When this command is enabled for exclusion of primary MSC node during NNSF function in HNB-GW, the HNB-GW excludes the particular node from being considered.

User can re-enable the inclusion of the primary MSC node to be considered for NNSF functionality by **no offload-msc point-code** command.
Important

Offload check is only for the primary point code and NOT for the backup point code. This command can be used for planned maintenance as well.

Examples

The following command configures the HNB-GW to exclude the primary MSC point code 1.2.3 from being considered in NSSF function for Iu-Flex support:

```
offload-msc point-code 1.2.3
```

The following command re-enables the inclusion of MSC point code 1.2.3 from being considered in NSSF function for Iu-Flex support:

```
no offload-msc point-code 1.2.3
```
**ranap reset**

Configures various Radio Access Network (RAN) Application Part reset procedure parameters for CS network association in an HNB access network.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > HNB-CS Network Configuration

*configure > cs-network cs_instance*

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-cs-network-instance_id)#
```

**Syntax Description**

```
ranap reset { ack-timeout timer_value | guard-timeout g_timer | hnbgw-initiated | max-retransmissions retries | use-actual-plmn }

default  ranap reset { ack-timeout | guard-timeout | hnbgw-initiated | max-retransmissions | use-actual-plmn }

no  ranap { hnbgw-initiated | use-actual-plmn }
```

**default**

Resets the RANAP RESET parameters in HNB-CS Network configuration instance.

**no**

Disables the RANAP RESET procedure related parameters in an HNB-CS Network configuration instance.

**ack-timeout timer_value**

Sets the timer value (in seconds) to wait for Reset Acknowledge from MSC. This is used during HNB-GW initiated RANAP RESET procedure in HNB-CS Network configuration instance.

*timer_value* is an integer value from 5 through 10. Default: 10

**guard-timeout g_timer_value**

Sets the timer value (in seconds) to send Reset Acknowledge to MSC. After this duration the HNB-GW sends RESET-ACK to MSC. This is used during MSC initiated RANAP RESET procedure in HNB-CS Network configuration instance.

*g_timer_value* is an integer value from 5 through 10. Default: 10
**hnbgw-initiated**
Enables the HNB-GW Initiated RANAP RESET procedures. Default: Disabled

**max-retransmission retries**
Sets the maximum number of retries allowed for transmission of RESET-ACK message to MSC. This is used during RANAP RESET procedure in HNB-CS Network configuration instance.

_retries_ is an integer value from 0 through 2. When 0 is used retransmission is disabled. Default: 1

**use-actual-plmn**
Actual PLMN will be sent in RANAP Reset/Reset Resource. By default, Common PLMN will be sent.

**Usage Guidelines**
Use this command to configure the RANAP RESET procedure related parameters in HNB-CS Network configuration for multiple HNB-GW service support.

**Examples**
The following command configures the HNB-GW initiated RANAP RESET Procedure for an HNB-CS Network configuration instance:

`ranap reset hnbgw-initiated`
**sccp**

Configures Signaling Connection Control Part (SCCP) related parameters for HNB-GW on the circuit switched (CS) network.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > HNB-CS Network Configuration

`configure > cs-network cs_instance`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-cs-network-instance_id)#
```

**Syntax Description**

```
| default | no | sccp calling-party-address
```

`default`

Restores the configuration to its default setting. By default, the calling party address is not included in the outgoing SCCP CR message.

`no`

If previously enabled, removes the configuration and restores the default setting.

`calling-party-address`

Specifies to include the optional calling-party-address IE in the outgoing SCCP CR message.

**Usage Guidelines**

Use this command to enable HNB-GW to include the optional calling party address in the outgoing Signaling Connection Control Part (SCCP) Connection Request (CR) message on the circuit switched network.

**Examples**

The following command enables the calling party address to be sent in the SCCP CR message:

```
sccp calling-party-address
```
HNB-PS Network Configuration Mode Commands

The HNB-PS Network Configuration Mode is used to manage the packet switched (PS) network instance on HNB-GW service to provide HNB access with the PS core network in a 3G UMTS network.

Command Modes

Exec > Global Configuration > HNB-PS Network Configuration
configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:

[local] host_name(config-ps-network-instance_id)#

Important

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

- associate gtpu-service, page 1519
- associate-sccp-network, page 1521
- end, page 1522
- exit, page 1523
- global-rnc-id, page 1524
- map core-network-id, page 1526
- map idnns range, page 1528
- map nri range, page 1530
- nri length, page 1532
- null-nri, page 1534
- offload-sgsn, page 1536
- ranap reset, page 1538
- sgsn deadtime, page 1540
• sgsn point-code, page 1542
• sccp, page 1544
### associate gtpu-service

 Associates a previously configured GTP-U service to provide a GTP-U tunnel with an SGSN towards the core network side. A GTP-U service must be configured in Context Configuration mode before using this configuration.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > HNB-PS Network Configuration

```plaintext
configure > ps-network ps_instance
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-ps-network-instance_id)#
```

**Syntax Description**

- `associate gtpu-service svc_name context ctx_name`
- `no associate gtpu-service`

- `no`
  
  Removes the associated GTP-U service from this HNB-GW service configuration.

- `svc_name`
  
  Specifies the name of the preconfigured GTP-U service.

- `context ctx_name`
  
  Specifies the name of the context in which the GTP-U service is configured.

**Usage Guidelines**

Use this command to configure GTP-U data plan tunnel between HNB-GW service and GSNs in core network. The service defined for GTP-U tunnel must be configured in Context configuration mode.

**Important**

Another GTP-U service can be used to bind the HNB-GW service to GTP-U tunnel with HNB in HNB access network and can be configured in HNB-GW Service Configuration mode. For more information on GTP-U service configuration, refer to *GTP-U Service Configuration Mode Commands* chapter.
Examples

The following command associates GTP-U service `gtpu_svc1` configured in context named `Ctx_gtpu1` with specific HNB-PS network instance for GTP-U tunnel towards GSN in core network:

```
associate gtpu-service gtpu_svc1 context Ctx_gtpu1
```
associate-sccp-network

Associates a previously defined Signaling Connection Control Part (SCCP) network identifier with the PS network instance in order to route the messages towards the SGSN via the IuPS interface.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > HNB-PS Network Configuration
configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:
[local]host_name(config-ps-network-instance_id)#

Syntax Description
associate-sccp-network sccp_net_id
no associate-sccp-network

no
Removes the associated SCCP network configuration instance from this HNB-PS network instance configuration.

sccp_net_id
Specifies a predefined SCCP network identifier.

Usage Guidelines
Use this command to associate a predefined SCCP network ID with the IuPS interface in HNB-GW service to connect with PS network elements; i.e. SGSN.

Important
The SCCP network ID must be defined in Global Configuration mode before using it with this command.

Important
A single SCCP network ID can not be shared with multiple HNB-PS network instances.

Examples
The following command associates SCCP network ID 2 with specific HNB-PS network instance:
associate-sccp-network 2
end

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

Product
All

Privilege
Security Administrator, Administrator

Syntax Description
end

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

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

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax Description**
exit

**Usage Guidelines**
Use this command to return to the parent configuration mode.
global-rnc-id

Configures the Radio Network Concentrator (RNC) identifier in a Radio Network PLMN associated with HNB-PS network configuration instance. The RNC identifier is provided to the HNB during HNB-REGISTRATION.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > HNB-PS Network Configuration

configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:

[local] host_name(config-ps-network-instance_id)#

Syntax Description

[ no ] global-rnc-id mcc mcc_num mnc mnc_num id rnc_id [ common-plmn mcc mcc_num mnc mnc_num ]

no

Deletes the RNC, MMC, and MNC information from the HNB-PS Network configuration instance.

mcc mcc_num

Specifies the mobile country code (MCC) part of radio network PLMN identifier as an integer value from 100 through 999.

mnc mnc_num

Specifies the mobile network code (MNC) part of radio network PLMN identifier as a 2- or 3-digit integer from 00 through 999.

id rnc_id

Specifies the RNC identifier as an integer from 0 through 4095.

common-plmn mcc mcc_num mnc mnc_num

Configures the Common PLMN for this PS Network.

mcc mcc_num configures the MCC of Common PLMN for this PS Network as an integer value from 100 through 999.
**mnc mnc_num** configures the MNC of Common PLMN for this PS Network as a 2- or 3-digit integer from 00 through 999.

**Usage Guidelines**

Use this command to configure RNC id to associate Radio Network PLMN which will be sent to HNBs from HNB-GW during HNB-REGISTRATION procedure. Depending upon the requirement the RNC Identifier can be provided at the desired granularity.

**Examples**

The following command configures the HNB-GW service to return an RNC identifier as 102 when an HNB-REGISTRATION request is received with LAC 1, and RAC 2:

```
global rnc-id mcc 102 mnc 02 id 2
```
map core-network-id

Maps/associates the PS core network identifier to a default SGSN in the network using an SGSN point code to allow HNBs to access the UMTS network.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > HNB-PS Network Configuration
configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:

[local] host_name(config-ps-network-instance_id)#

Syntax Description
map core-network-id cn_id point-code sgsn_point_code
no map core-network-id cn_id

no
Removes the mapping of a PS core network id with particular SGSN point code.

cn_id
Specifies the core network identifier configured to represent a UMTS PS core network as an integer from 0 through 4095.
Multiple instance of this command can be mapped with different SGSN point codes.

point-code sgsn_point_code
Specifies the SS7 address of the default SGSN in the PS network.
point_code is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ####### format.
Only one instance of this SGSN point code can be mapped with one PS core network identifier.

Usage Guidelines
Use this command to map a UMTS PS core network identifier with a particular SGSN point code.
This command can be entered multiple times with same SGSN point code to map with one or more PS core network Id, but a particular core network identifier can be mapped to one SGSN only.
This command is instrumental in Iu-Flex functionality, whenever HNB-GW receives RESET/RESET-RES messages from SGSN with Global CN-ID information element, the response from HNB-GW is sent to the node configured for that particular Global CN-ID.

If the RESET/RESET-RES messages do not have Global CN-ID IE, then the response of those messages is directed to the default SGSN which is configured using `sgsn point-code` command in this mode.

**Examples**

The following command configures the PS core network identifier `101` with an SGSN point code `1.2.3`:

```
map core-network-id 101 point-code 1.2.3
```

The following command configures the PS core network identifier `102` with the same SGSN point code `1.2.3`:

```
map core-network-id 102 point-code 1.2.3
```
**map idnns range**

Configures the mapping of an Intra-Domain NAS Node Selector (IDNNS) IE received from UE in an RUA connect message towards HNB-GW. This is an important configuration for PS network resource sharing over an Iu-Flex interface.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > HNB-PS Network Configuration

configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-ps-network-instance_id) #
```

**Syntax Description**

```
map idnns range idnns_start to idnns_end point-code sgsn_point_code {backup point-code bkup_sgsn_point_code}
no map idnns range idnns_start to idnns_end
```

**range idnns_start to idnns_end**

Specifies the range of IDNNSs received from UE to map with particular SGSN point codes during the initial PS core network node selection.

*idnns_start* is an integer from 0 through 1023 that should be less than *idnns_end*.

*idnns_end* is an integer from 0 through 1023 that should be more than *idnns_start*.

The command can be entered more than once to map multiple IDNNS ranges to the same SGSN. However, overlapping and mapping of the same range to different SGSN point codes is not allowed.

**point-code sgsn_point_code**

Specifies the SS7 address of the SGSN in the PS network.

*sgsn_point_code* is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ####### format.

**backup point-code bkup_sgsn_point_code**

Specifies the SS7 address of the SGSN to be used as the backup in the PS network.
bkup_sgsn_point_code is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ####### format.

Usage Guidelines

Use this command to map a NRI received from UE during initial PS network node selection to SGSN point code through NRI range mapping over Iu-Flex interface.

The IDNNS refers to the information element in RUA connect message from UE towards RAN (HNB-GW). In IDNNS IE, if the choice of routing mentioned is other than local P-TMSI, then the value it provides is used against this configuration to map the SGSN point code.

If backup SGSN point-code is specified, then specified SGSN works as backup for the IDNS range configured. This Backup SGSN is selected if the mapped SGSN for a given IDNNS range is going for offloading using offload-sgsn point-code command.

The command can be entered more than once to map multiple IDNNS ranges to same SGSN point code, but overlapping and mapping of same range to different SGSN point code is not allowed.

Examples

The following command maps the IDNNS range from 101 to 201 with SGSN point code 1.2.3 and point code 7.8.9 as backup SGSN point code:

map nri range 101 to 201 point-code 1.2.3 backup point-code 7.8.9

The following command removes all IDNNS range matching entries between 301 to 399 from the configuration:

no map idnns range 301 to 399
**map nri range**

Configures the mapping of the Network Resource Identifier (NRI) received from UE to an SGSN point code. This is an important configuration for PS network resource sharing over Iu-Flex interface.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > HNB-PS Network Configuration
configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:
[local]host_name(config-ps-network-instance_id)#

**Syntax Description**
- **map nri range nri_start to nri_end point-code sgsn_point_code**
- **no map nri range nri_start to nri_end**

**no**
Removes the entries of mapping of range of NRIs received from UE with a particular SGSN point code.

**range nri_start to nri_end**
Specifies the range of NRIs received from UE to map with a particular SGSN point code during initial PS core network node selection.

**nri_start** is an integer from 0 through 1023 that should be less than **nri_end**.

**nri_end** is an integer from 0 through 1023 that should be more than **nri_start**.

The command can be entered more than once to map multiple NRI ranges to the same SGSN, but overlapping is not allowed.

**point-code sgsn_point_code**
Specifies the SS7 address of the SGSN in the PS network to map with range of NRI values.

**point_code** is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ######## format.

**Usage Guidelines**
Use this command to map a NRI received from UE during initial PS network node selection to SGSN point code through NRI range mapping over Iu-Flex interface.
This configuration is used during initial PS core network node selection when the network resource identifier (NRI) from the UE is available. The NRI range is mapped to SGSN point code. This configuration is used when the core network uses Iu-Flex interface.

The command can be entered more than once to map multiple NRI ranges to same SGSN point code.

It is possible to configure multiple ranges to more than one SGSN however this configuration is required only when the PS core network is configured as Multi-Operator Core Network (MOCN).

When the PS core network is not MOCN and one range is mapped to more than one SGSN then SGSN is selected randomly in a non-predictable manner.

**Examples**

The following command maps the NRI range from 101 to 201 with SGSN point code 1.2.3:

```
map nri range 101 to 201 point-code 1.2.3
```

The following command maps the NRI range from 301 to 399 with SGSN point code 1.2.3:

```
map nri range 301 to 399 point-code 1.2.3
```

The following command removes all NRI range matching entries between 301 to 399 from the configuration:

```
no map nri range 301 to 399
```
**nri length**

Configures the network resource identifier (NRI) length in bits to identify a specific SGSN serving in a pooled area. At least one NRI value must be assigned to an SGSN serving in a pool. The NRI is coded inside of the temporary mobile subscriber identity (TMSI), located within bits 14 to 23 with a variable length between 0 and 10 bits. The operator must set this NRI length to indicates the number of bits that shall be used for the NRI field to set the parameters for Iu-Flex (SGSN pooling) functionality.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > HNB-PS Network Configuration

`configure > ps-network ps_instance`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-ps-network-instance_id)#
```

**Syntax Description**

`nri length nri_value`

`default nri length`

- **default**

  Sets the NRI length to default value of 0 and disables the Iu-Flex (SGSN pooling) functionality.

- **nri length nri_length**

  Default: 0

  Specifies the number of bits to be used in the P-TMS (bits 23 to 18) to define the network resource identifier (NRI). The NRI length configuration also sets the maximum size of the pool. If not configured, the NRI length is set to zero length.

  `length` is an integer from 1 to 10. When a non-zero value is configured the PS network is considered to be a pool. Default: 0

**Usage Guidelines**

Use this command to enable the Iu-Flex functionality on HNB-GW. This command identifies a unique SGSN serving a pooled area for Iu-Flex functionality and at least one NRI value has to assigned to an SGSN serving in a pool. It performs SGSN pooling/offloading scenario over Iu-Flex interface. The NRI is stored in the bits 14 to 23 of TMSI. The HNB-GW uses a portion of this NRI to set the parameters for Iu-Flex (SGSN pooling) functionality.
If more than one NRI is configured, the HNB-GW service does round-robin between the available NRIs when new subscriber(s) (re)connect.

This command must be used in conjunction with null nri command to configured SGSN pooling/offloading over Iu-Flex interface.

**Examples**

The following command sets the HNB-GW to use bit length as 6 to derive the values from the NRI field (stored in the bits 14 to 23 of TMSI) to set the parameters for Iu-Flex (SGSN pooling) functionality:

```
nri length 6
```
null-nri

Configures the null network resource identifier (NRI) for load redistribution in support of Iu-Flex functionality. The NRI value defined with this command must be unique across the pool areas. This null-NRI is used by HNB-GW for load redistribution during SGSN offloading.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > HNB-PS Network Configuration

configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-ps-network-instance_id)#

Syntax Description

null-nri null_nri_value

no null-nri null_nri_value

no

Disables/removes the configured null-NRI value used for SGSN offloading procedure.

null_nri_value

Indicates the null-NRI value to be used by HNB-GW for load re-distribution during SGSN offloading as an integer from 0 through 1023.

Without MOCN configuration this value can be entered only once. For MOCN a unique null-NRI must be assigned to each MOCN operator identify by its PLMN-ID (MCC+MNC).

A 0 (zero) value configured as null-NRI indicates the keyword is not to be used. There is no default value for this parameter.

Usage Guidelines

Use this command to identify the SGSN by HNB-GW to be used for load redistribution during SGSN offloading over Iu-Flex interface.

There is one unique null-NRI in a PLMN supporting pool functionality.

Without MOCN configuration this command can be entered only once. In case of MOCN a unique null-NRI must be assigned to each MOCN operator identify by its PLMN-id (MCC+MNC).
Examples

The following command sets the null-NRI as **1001** to be used by HNB-GW for load redistribution during SGSN offloading:

```
null-nri 1001
```
**offload-sgsn**

Enables or disables the exclusion of a specified primary SGSN node during the NAS Node Selection Function (NNSF) procedure when it needs to be offloaded using Iu-Flex functionality.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > HNB-PS Network Configuration
configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-ps-network-instance_id)#
```

**Syntax Description**

```
| no | offload-sgsn point-code sgsn_point_code
```

**no**

Removes the specified primary SGSN point code from the exclusion list for NNSF function on HNB-GW and re-enables the inclusion of the primary SGSN node to be considered by HNB-GW.

**point-code sgsn_point_code**

Specifies SS7 address of primary SGSN in PS network having specific point code value to be excluded for NNSF function on HNB-GW when it needs to be offloaded in Iu-Flex functionality.

*point_code* is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ######## format.

Only one instance of this primary SGSN point code can be mapped with one PS core network id.

**Usage Guidelines**

Use this command to provision the HNB-GW to enable or disable the exclusion of the SGSN node when it needs to be offloaded.

When this command is enabled for exclusion of SGSN node during NNSF function in HNB-GW, the HNB-GW excludes the particular node from being considered.

User can re-enable the inclusion of the SGSN node to be considered for NNSF functionality by **no offload-sgsn point-code** command.

---

**Important**

The offload check is only for the primary point code and NOT for the backup point code.
This command can be used for planned maintenance as well.

Examples

The following command configure the HNB-GW to exclude the primary SGSN point code 1.2.3 from being considered in NSSF function for Iu-Flex support:

```
offload-sgsn point-code 1.2.3
```

The following command re-enables the inclusion of SGSN point code 1.2.3 from being considered in NSSF function for Iu-Flex support:

```
no offload-sgsn point-code 1.2.3
```
ranap reset

Configures various Radio Access Network (RAN) Application Part reset procedure parameters for PS network association in an HNB access network.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > HNB-PS Network Configuration

configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:

\[local\]host_name(config-ps-network-instance_id)#

Syntax Description

`ranap reset { ack-timeout timer_value | guard-timeout g_timer | hnbgw-initiated | max-retransmissions retries | use-actual-plmn }`

default `ranap reset { ack-timeout | guard-timeout | hnbgw-initiated | max-retransmissions | use-actual-plmn }

no `ranap { hnbgw-initiated | use-actual-plmn }

default

Resets the RANAP RESET parameters in HNB-PS Network configuration instance.

no

Disables the RANAP RESET procedure related parameters in an HNB-PS Network configuration instance.

`ack-timeout timer_value`

Sets the timer value (in seconds) to wait for Reset Acknowledge from SGSN. This is used during HNB-GW initiated RANAP RESET procedure in HNB-PS Network configuration instance.

`timer_value` is an integer value from 5 through 10. Default: 10

`guard-timeout g_timer_value`

Sets the timer value (in seconds) to send Reset Acknowledge to SGSN. After this duration the HNB-GW sends RESET-ACK to SGSN. This is used during SGSN initiated RANAP RESET procedure in HNB-PS Network configuration instance.

`g_timer_value` is an integer value from 5 through 10. Default: 10
**HNB-GW Initiated**
Enables the HNB-GW Initiated RANAP RESET procedures. Default: Disabled

**max-retransmission retries**
Sets the maximum number of retries allowed for transmission of RESET-ACK message to SGSN. This is used during RANAP RESET procedure in HNB-PS Network configuration instance.

*retries* is an integer value from 0 through 2. When 0 is used retransmission is disabled. Default: 1

**use-actual-plmn**
Actual PLMN will be sent in RANAP Reset/Reset Resource. By default, Common PLMN will be sent.

**Usage Guidelines**
Use this command to configure the RANAP RESET procedure related parameters in HNB-PS Network configuration for multiple HNB-GW service support.

**Examples**
The following command configures the HNB-GW initiated RANAP RESET Procedure for an HNB-PS Network configuration instance:

```
ranap reset hnbgw-initiated
```
**sgsn deadtime**

Configures a timer on HNB-GW to manage SGSN availability in a PS core network on receiving of a PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > HNB-PS Network Configuration
configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ps-network-instance_id)#
```

**Syntax Description**

```
sgsn deadtime { immediate | dur }
[ no | default ] sgsn deadtime
```

- **no**
  Makes the peer node (SGSN) always available for all HNB-PS network instances.

- **default**
  Sets the default action for HNB-GW such that the peer node (SGSN) is marked down as soon as HNB-GW receives a PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP in a specific HNB-PS network instance. Default: Enabled

- **immediate**
  Sets the HNB-GW to mark the peer node (SGSN) down immediately and clears all Iu-PS connections towards the SGSN. Default: Disabled

- **dur**
  Sets the duration (in seconds) for a timer which starts once HNB-GW receives a PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP for a peer SGSN. On expiry of this timer the peer SGSN is marked as dead and all Iu-PS connections towards that SGSN are released.
  
  - **dur** is an integer from 1 through 30.
  - Only one instance of this command can be configured.
Usage Guidelines

This command is used to configure a timer on HNB-GW to manage SGSN availability in a PS core network on receiving of PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP.

Timer value sets the duration in seconds for a timer which started once HNB-GW receives PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP for a peer SGSN. On expiry of this timer the peer SGSN is marked as dead and all Iu-PS connections towards that SGSN shall be released.

Important

This command can be entered only once. Reentering this command overwrites the previous parameters.

Examples

The following command configures the deadtime timer value for 10 seconds on HNB-GW. Once HNB-GW receives PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP for a peer SGSN the HNB-GW waits for configured period and on expiry of timer it marks the specific SGSN as dead:

```
sgsn deadtime 10
```
sgsn point-code

Configures the default SGSN point-code with the HNB-PS network instance. This command is used when HNB-GW is to be connected to only one SGSN with in a PS network or as the default SGSN for all HNBs connected through specific HNB-PS network instance.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > HNB-PS Network Configuration

       configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:

   [local]host_name(config-ps-network-instance_id)#

Syntax Description

[ no ] sgsn point-code point_code

no

Removes the configured default SGSN point code from specific HNB-PS network instance.

Caution

Removing the SGSN point code is a disruptive operation and affects all HNB sessions which are connected to particular SGSN through an HNB-PS network instance.

point_code

Specifies the SS7 address of the default SGSN in a PS network.

point_code is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ####### format.

Only one instance of this command can be configured.

Usage Guidelines

Use this command to configure a default SGSN to which HNB connects for PS network access through the HNB-GW service.

Point-code is an SS7 address for an element in the SS7 network. Point-codes must be defined in dotted-decimal format in a string of 1 to 11 digits. Format options include:

- 0.0.1 to 7.255.7 for point-code in the ITU range.
• 0.0.1 to 255.255.255 for point-code in the ANSI range.
• 0.0.1 to 15.31.255 for point-code in the TTC Range.
• a string of 1 to 11 digits in dotted-decimal to represent a point-code in a different range.

**Important**
This command can be entered only once. If entered again the previous value shall be overwritten.

**Examples**
The following command configures a default SGSN with point code **101.201.101** for HNBs to access PS network through HNB-GW service in this HNB-PS network instance:

SGSN point-code 101.201.101
**sccp**

Configures Signaling Connection Control Part (SCCP) related parameters for HNBGW on the packet switched (PS) network.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > HNB-PS Network Configuration

configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:

\[\text{[local]} host_name (config-ps-network-instance_id)\]#

**Syntax Description**

| default | no | sccp calling-party-address |

**default**

Restores the configuration to its default setting. By default, the calling party address is not included in the outgoing SCCP CR message.

**no**

If previously enabled, removes the configuration and restores the default setting.

**calling-party-address**

Specifies to include the optional calling-party-address IE in the outgoing SCCP CR message.

**Usage Guidelines**

Use this command to enable HNBGW to include the optional calling party address in the outgoing Signaling Connection Control Part (SCCP) Connection Request (CR) message on the packet switched (PS) network.

**Examples**

The following command enables the calling party address to be sent in the SCCP CR message:

sccp calling-party-address
HNB-RN PLMN Configuration Mode Commands

This HNB Radio Network PLMN configuration mode defines the radio network PLMN parameters related to the HNB-GW connection with a UMTS Femto radio network.

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration > HNB-RN PLMN Configuration

configure > context context_name > hnb-gw-service service_name > radio-network-plmn mcc mcc_number mnc mnc_number

Entering the above command sequence results in the following prompt:

`{context_name}@host_name(config-hnbw-radio-plmn)#`

---

**Important**

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

- associate cs-network, page 1546
- associate ps-network, page 1547
- authorised-macro-lai, page 1548
- end, page 1550
- exit, page 1551
- rnc-id, page 1552
associate cs-network

From StarOS Release 14.0 onward this command is deprecated.
associate ps-network

From StarOS Release 14.0 onward this command is deprecated.
authorised-macro-lai

Configures the macro LAI based authorization parameters for this HNB-GW service.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration > HNB-RN PLMN Configuration

```
configure > context context_name > hnbgw-service service_name > radio-network-plmn mcc mcc_number mnc mnc_number
```

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-hnbgw-radio-plmn)#
```

**Syntax Description**

```
authorised-macro-lai { macro-info-ie-absent-action { accept | reject } | mcc mcc_id mnc mnc_id lac range range_from to range_to }
default authorised-macro-lai macro-info-ie-absent-action
no authorised-macro-lai mcc mcc_id mnc mnc_id lac range range_from to range_to

default
```

Configures the default parameters for macro LAI based authorization for the system configuration. Default action is to reject HNB if IE is absent.

```
no
```

Deletes the macro LAI based authorization parameters from the system configuration.

```
mcc-id
```

Specifies the MCC of pre-configured macro lai range for HNB authorization as a number, ranging from 100..999

```
mnc-id
```

Specifies the MNC of pre-configured macro lai range for HNB authorization, ranging from 00..999

```
lac range
```

Specifies the LAC of pre-configured macro LAI range for HNB authorization.
range_from

Specifies the LAC range minimum value, which is an integer from 0..65535.

range_to

Specifies the LAC range maximum value, which is also an integer from 0..65535.

Usage Guidelines

Use this command to configure the macro LAI based authorization parameters for an existing HNB-GW service.

Examples

The following command configures the default action for macro LAI based authorization for an existing HNB-GW service.

default authorised-macro-lai macro-info-ie-absent-action
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.
**rnc-id**

Configures the Radio Network Concentrator (RNC) identifier in a Radio Network PLMN associated with HNB-GW service. The RNC identifier is provided to the HNB during HNB-REGISTRATION.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration > HNB-RN PLMN Configuration

```
configure > context context_name > hnbgw-service service_name > radio-network-plmn mcc mcc_number mnc mnc_number
```

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-hnbgw-radio-plmn) #
```

**Syntax Description**

| no | rnc-id rnc_id |

**no**

Deletes the RNC id from the system configuration.

**rnc-id**

Specifies the RNC identifier as an integer from 0 through 4095.

**Usage Guidelines**

Use this command to configure RNC id for Radio Network PLMN which will be sent to HNBs from HNB-GW during HNB-REGISTRATION procedure. Depending upon the requirement the RNC Identifier can be provided at the desired granularity.

**Examples**

The following command configures the HNB-GW service to return an RNC identifier as *102* when an HNB-REGISTRATION request is received:

```
global rnc-id 102
```
HSGW Service Configuration Mode Commands

The HSGW Service Configuration Mode is used to create and manage a configuration allowing the HRPD Serving Gateway (HSGW) to communicate, send and receive call data, and session flows to/from an evolved Access Network/evolved Packet Control Function (eAN/ePCF) in an eHRPD network.

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name (config-hsgw-service) #

Important

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

- a11-signalling-packets, page 1555
- associate, page 1556
- bind address, page 1557
- context-retention-timer, page 1559
- data-available-indicator, page 1560
- data-over-signaling, page 1561
- dns-pgw, page 1562
- end, page 1564
- exit, page 1565
- fqdn, page 1566
- fragment, page 1568
- gre, page 1569
- ip, page 1572
• lifetime, page 1575
• max-retransmissions, page 1576
• mobile-access-gateway, page 1577
• network-initiated-qos, page 1578
• plmn id, page 1579
• policy overload, page 1580
• profile-id-qci-mapping, page 1582
• registration-deny, page 1583
• retransmission-timeout, page 1585
• rsvp, page 1586
• setup-timeout, page 1588
• spi remote-address, page 1589
• ue-initiated-qos, page 1592
• unauthorized-flows, page 1593
**a11-signalling-packets**

Enables the DSCP marking feature for IP headers carrying outgoing A11-signalling A11 packets (such as RRP, RU, SU).

**Product**
HSGW

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HSGW Service Configuration

```plaintext
configure > context context_name > hsgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

**Syntax Description**

```plaintext
a11-signalling-packets ip-header-dscp value
[ default | no ] a11-signalling-packets ip-header-dscp
```

**default**
Restores the specified parameter to its default setting of 0x0.

**no**
Disables the specified functionality.

```plaintext
ip-header-dscp value
```

Configures the QoS Differentiated Services Code Point (DSCP) marking for IP header encapsulation.

**value**: Represents the DSCP setting as the first six most-significant bits of the ToS field. It can be configured to any hex value from 0x0 through 0x3F. Default is 0x0.

**Usage Guidelines**
Use this command to enable or disable the DSCP marking feature for IP headers carrying outgoing A11-signalling A11 packets. DSCP marking is disabled by default.

**Examples**
The following command configures the HSGW service to support DSCP marking for IP headers on A11 packets in outgoing A11-signalling traffic:

```
a11-signalling-packets ip-header-dscp 0x21
```
**associate**

 Associates accounting policies and QCI-QoS mapping parameters with this HSGW service.

**Product**

HSGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-hsgw-service)#

**Syntax Description**

`associate { accounting-policy name | qci-qos-mapping name }`

`no associate { accounting-policy | name } | qci-qos-mapping }`

- **no**
  
  Removes the specified associated policy or mapping from the service.

- **accounting-policy name**
  
  Specifies an existing accounting policy to associate with the HSGW service as an alphanumeric string of 1 through 63 characters.

- **qci-qos-mapping name**
  
  Specifies an existing QCI-QoS mapping configuration as an alphanumeric string of 1 through 63 characters. QCI-QoS mapping is configured through the **qci-qos-mapping** command in the Global Configuration Mode.

**Usage Guidelines**

Use this command to associate an accounting policy with the HSGW service.

**Examples**

The following command associates an accounting policy named *acct2* to the HSGW service:

`associate accounting-policy acct2`
bind address

Binds the service to a logical IP interface serving as the A10 interface and specifies the maximum number of subscribers that can access this service over the configured interface.

Product
HSGW

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > HSGW Service Configuration
configure > context context_name > hsgw-service service_name

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

Syntax Description
bind address ip_address [ max-subscribers num ]
no bind address

no
Removes the interface binding from this service.

divide ip_address
Specifies the IP address of the A10/A11 interface in IPv4 dotted-decimal notation.

max-subscribers num
Specifies the maximum number of subscribers that can access this service on this interface as an integer from 0 through 2500000. Default: 2500000

Important
The maximum number of subscribers supported is dependant on the license key installed and the number of active PSCs in the system. A fully loaded system with 13 active PSCs can support 3,000,000 total subscribers. Refer to the license key command and the Usage section (below) for additional information.

Usage Guidelines
Associate the HSGW service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an A10/A11 interface that provides the session connectivity to/from an eAN/PCF. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.
This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.

When configuring the **max-subscribers** option, be sure to consider the following:

- The total number of A10/A11 interfaces you will configure
- The total number of subscriber sessions that all of the configured interfaces may handle during peak busy hours
- An average bandwidth per session multiplied by the total number of sessions
- The type of physical port (10/100Base-T or 1000Base-Tx) that these interfaces will be bound to

Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.

**Examples**

The following command would bind the logical IP interface with the address of 112.334.556.778 to the HSGW service and specifies that a maximum of 200,000 simultaneous subscriber sessions can be facilitated by the interface/service at any given time:

```
bind address 112.334.556.778 max-subscribers 200000
```
context-retention-timer

Configures the maximum number of consecutive seconds that a UE session context (which includes the LCP, authentication and A10 session context for a given UE) is maintained by the HSGW before it is torn down.

**Product**
HSGW

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HSGW Service Configuration

`configure > context context_name > hsgw-service service_name`

Entering the above command sequence results in the following prompt:

`{context_name}@host_name(config-hsgw-service)#`

**Syntax Description**
`context-retention-timer timeout [ sec ]
[ default | no ] context-retention-timer timeout`

- **default**
  Disables the timer.

- **no**
  Disables the timer.

- **timeout [ sec ]**
  Specifies the amount of time (in seconds) that the session context is maintained before it is disassembled as an integer from 1 through 3600. Default: 60.
  In Release 15.0 and later, the maximum value has been increased to 86400 seconds (24 hours).

**Usage Guidelines**
Use this command to configure a timer to retain session contexts for a specified amount of time before disassembling it.

**Examples**
The following command allows the HSGW to maintain session contexts for 120 seconds before tearing them down:
`context-retention-timer timeout 120`
**data-available-indicator**

Enables sending the Data Available Indicator extension in A10/A11 Registration Reply messages.

**Product**

HSGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-hsgw-service)#
```

**Syntax Description**

data-available-indicator

**Usage Guidelines**

Use this command to enable the sending of the Data Available Indicator extension in A10/A11 Registration Reply messages.
data-over-signaling

Enables the data-over-signaling marking feature for A10 packets.

Product HSGW

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-hsgw-service)#

Syntax Description [ default | no ] data-over-signaling

default

Enables the data-over-signaling feature for A10 packets.

no

Disables the data-over-signaling feature for A10 packets.

Usage Guidelines Use this command to enable or disable the data-over-signaling feature for A10 packets.
**dns-pgw**

Identifies the location of the DNS client to the HSGW service and enables/disables P-GW load balancing using DNS SRV lookup.

**Product**

HSGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

`configure > context context_name > hsgw-service service_name`

Entering the above command sequence results in the following prompt:

`(context_name)host_name(config-hsgw-service)#`

**Syntax Description**

`dns-pgw { context_name | selection { topology [weight] | weight } }`

`[default | no] dns-pgw { context | selection { topology [weight] | weight } }`

**default**

Returns the command to its default setting of the current context.

By default, topology will be enabled and weight will be disabled.

**no**

Removes the configured DNS client context name or P-GW DNS selection criteria from this service.

**context name**

Specifies an existing context in which the DNS client is configured as an alphanumeric string of 1 through 79 characters.

**selection { topology [weight] | weight }**

Specifies P-GW DNS selection criteria.

- **topology**: Enables topology selection, which selects a P-GW topologically closer to the HSGW.
- **topology weight**: Enables topology selection with weight.
- **weight**: Enables selection with weight only when both preference values are the same; disables topology selection.
Usage Guidelines

Use this command to identify to the HSGW service the context where the DNS client is configured. The DNS client is used to identify an FQDN for the peer P-GW. This command defaults to the same context as the HSGW service.

In addition, this command enables and disables P-GW load balancing using DNS SRV lookup by defining P-GW DNS selection criteria.

Examples

The following command identifies the context where the DNS client is configured as isp3:

dns-pgw context isp3

The following command enables P-GW DNS topology selection with weight:

dns-pgw selection topology weight
end

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

<table>
<thead>
<tr>
<th>Product</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
<tr>
<td>Syntax Description</td>
<td>end</td>
</tr>
<tr>
<td>Usage Guidelines</td>
<td>Use this command to return to the Exec mode.</td>
</tr>
</tbody>
</table>
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.
fqdn

Configures the Fully Qualified Domain Name (FQDN) for this HSGW service.

**Product**
HSGW

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HSGW Service Configuration

```
configure > context context_name > hsgw-service service_name
```

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

**Syntax Description**

```
fqdn domain_name
[ default | no ] fqdn
```

- **default**
  Returns the command to the default setting of "null".

- **no**
  Removes the configured FQDN name from this service.

- **domain_name**
  Specifies an FQDN for the HSGW service as an alphanumeric string of 1 through 256 characters.

**Important**
In order to properly interact with other nodes in the network, the FQDN should be 96 alpha and/or numeric characters or less.

**Usage Guidelines**

Use this command to configure an FQDN for this HSGW service. The FQDN is used when matching a P-GW with an HSGW.

**Topology Matching**

You may specify which P-GW you wish an HSGW interface to connect with by enabling topology matching within the FQDNs for both the HSGW service and P-GW service. Topology matching selects geographically closer nodes and reduces backhaul traffic for a specified interface.
The following optional keywords enable or disable topology matching when added to the beginning of an FQDN:

- **topon.**<interface_name>.
  
  Beginning an FQDN with `topon` initiates topology matching with available P-GWs in the network. Once this feature is enabled, the rest of the FQDN is processed from right to left until a matching regional designator is found on a corresponding P-GW FQDN.

- **topoff.**<interface_name>.
  
  By default, topology matching is disabled. If you enable topology matching for any interfaces within a node, however, all interfaces not using this feature should be designated with `topoff`.

**Examples**

The following command configures this HSGW service with an FQDN of `abc123.com`:

```
fqdn abc123.com
```

The following command configures this HSGW service with an FQDN that enables topology matching:

```
fqdn topon. <interface_name>.hsgw01.bos.ma.node.epc.mnc<value>.mcc<value>.3gppnetwork.org
```

The associated P-GW service must have a corresponding FQDN similar to the following:

```
topon. <interface_name>.pgw01.bos.ma.node.epc.mnc<value>.mcc<value>.3gppnetwork.org
```
fragment

Enables or disables Point-to-Point Protocol (PPP) payload fragmentation.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-hsgw-service)#

Syntax Description

| default | no | fragment ppp-data

default

Returns the command to its default setting of enabled.

no

Disables PPP payload fragmentation.

Usage Guidelines

Use this command to enable or disable PPP payload fragmentation.
**gre**

Configures Generic Routing Encapsulation (GRE) parameters for the A10 protocol within the HSGW service.

**Product**

HSGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

```
configure > context context_name > hsgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

**Syntax Description**

```
gre { checksum | checksum-verify | flow-control { action { disconnect-session | resume-session } } || timeout msecs } + | ip-header-dscp value { all-control-packets | setup-packets-only } | reorder-timeout msecs | segmentation | sequence-mode { none | reorder } | sequence-numbers | threegppp2-ext-headers qos-marking }
default gre { checksum | checksum-verify | flow-control | ip-header-dscp | reorder-timeout | sequence-mode | sequence-numbers | threegppp2-ext-headers qos-marking }
no gre { checksum | checksum-verify | flow-control | ip-header-dscp | segmentation | sequence-numbers | threegppp2-ext-headers qos-marking }
```

**default**

Restores the specified parameter to its default setting.

**no**

Disables the specified functionality.

**checksum**

Enables the introduction of the checksum field in outgoing GRE packets. Default: disabled

**checksum-verify**

Enables verification of the GRE checksum (if present) in incoming GRE packets. Default: disabled

**flow-control [ action { disconnect-session | resume-session } ] [ timeout msecs ] +**

Default: no GRE flow-control
Enables 3GPP2 GRE flow control which causes the HSGW to send flow control enabled Normal Vendor Specific Extensions (NVSE) in A11 RRPs.

**action** { disconnect-session | resume-session }:

Default: disconnect-session

Specifies the action to be taken when timeout is reached:

- **disconnect-session**: Ends the session and releases the call.
- **resume-session**: Switches flow control to XON and resumes delivery of packets to the RAN.

**timeout msecs**

Specifies the amount of time (in milliseconds) to wait for an XON indicator from the RAN (after receiving an XOFF). Also sets the action to be taken if the timeout limit is reached.

*msecs* is an integer from 1 through 1000000. Default: 1000

**ip-header-dscp value** { all-control-packets | setup-packets-only }

Default: Disabled

Configures QoS Differentiated Services Code Point (DSCP) marking for GRE packets.

- **value**: Represents the DSCP setting as the first six most-significant bits of the ToS field. It can be configured to any hexadecimal value from 0x0 through 0x3F.
- **all-control-packets**: Dictates that the DSCP marking is to be provided in all GRE control packets.
- **setup-packets-only**: Dictates that the DSCP marking is to be provided only in GRE setup packets.

**reorder-timeout msecs**

Configures the maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets as an integer from 0 through 5000. Default: 100

**segmentation**

Enables GRE Segmentation for the HSGW service. Default: disabled

**sequence-mode** { none | reorder }

Default: none

Configures handling of incoming out-of-sequence GRE packets.

- **none**: Specifies that sequence numbers in packets are ignored and all arriving packets are processed in the order they arrive.
- **reorder**: Specifies that out of sequence packets are stored in a sequencing queue until one of the conditions is met:
  
  - The reorder timeout occurs: All queued packets are sent for processing and the accepted sequence number is updated to the highest number in the queue.
  
  - The queue is full (five packets): All packets in the queue are sent for processing, the reorder timer is stopped and the accepted sequence number is updated to the highest number in the queue.
- An arriving packet has a sequence number such that the difference between this and the packet at the head of the queue is greater than five. All the packets in the queue are sent for processing, the reorder timer is stopped and the accepted sequence number is updated to the highest number that arrived.

- A packet arrives that fills a gap in the sequenced numbers stored in the queue and creates a subset of packets whose sequence numbers are continuous with the current accepted sequence number. This subset of packets in the queue is sent for processing. The reorder timer continues to run and the accepted sequence number is updated to the highest number in the subset delivered.

**sequence-numbers**

Enables insertion of GRE sequence numbers in data that is about to be transmitted over the A10 interface. Data coming into the system containing sequence numbers but that is out of sequence is not re-sequenced.

**threegppp2-ext-headers qos-marking**

When threegppp2-ext-headers qos-marking is enabled and the PCF negotiates capability in the A11 RRQ, the HSGW will include the QoS optional data attribute in the GRE 3gpp2 extension header.

The **no** keyword, enables qos-marking in the GRE header based on the tos value in the header.

**Usage Guidelines**

Use this command to set GRE parameters for the A10 protocol within the HSGW service.

**Examples**

The following command configures the HSGW service to support the inclusion of GRE sequence numbers in outgoing traffic:

```
gre sequence-numbers
```
ip

Enables the use of Robust Header Compression (RoHC) and enters the HSGW Service ROHC Configuration Mode where RoHC parameters are configured for the service.

Configures the local User Datagram Protocol (UDP) port for the A10/A11 interface IP socket.

Sets the parameters for IP source validation. Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network. Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-hsgw-service)#

Syntax Description

ip { header-compression rohc | local-port number | source-violation { clear-on-valid-packet | drop-limit num | period secs | reneg-limit num } }

default ip { header-compression rohc | local-port | source-violation { drop-limit | period | reneg-limit } }

no ip { header-compression rohc | source-violation clear-on-valid-packet }

default

Resets the keyword to its default value.

no

header-compression rohc: Removes the RoHC configuration from this service.

ip source-violation clear-on-valid-packet: Disables the ability of the service to reset the reneg-limit and drop-limit counters after receipt of a properly addressed packet.

header-compression rohc

Specifies that Robust Header Compression will be applied to sessions using this service and enters the HSGW Service RoHC Configuration Mode where RoHC parameters are configured.
local-port number
Specifies the UDP port number as an integer from 1 through 65535. Default: 699

source-violation { clear-on-valid-packet | drop-limit num | period secs | reneg-limit num }

clear-on-valid-packet
Configures the service to reset the reneg-limit and drop-limit counters after receipt of a properly addressed packet. Default: disabled

drop-limit num
Specifies the number of allowed source violations within a detection period before forcing a call disconnect as an integer from 1 through 1000000. If num is not specified, the value is set to the default. Default: 10

period secs
Specifies the length of time (in seconds) for a source violation detection period to last; drop-limit and reneg-limit counters are decremented each time this value is reached.

The counters are decremented in this manner: reneg-limit counter is reduced by one (1) each time the period value is reached until the counter is zero (0); drop-limit counter is halved each time the period value is reached until the counter is zero (0). If secs is not specified, the value is set to the default.

secs is an integer from 1 through1000000. Default: 120

reneg-limit num
Sets the number of allowed source violations within a detection period before forcing a PPP renegotiation. If num is not specified, the value is set to the default.

num is an integer from 1 through 1000000. Default: 5

Usage Guidelines

Header Compression RoHC: Use this command to specify that sessions using this service will have Robust Header Compression applied and configure parameters supporting RoHC.

Entering this command results in the following prompt:

{context_name}@hostname(config-ip-header-compression-rohc)#

HSGW Service RoHC Configuration Mode commands are defined in the HSGW Service RoHC Configuration Mode Commands chapter.

Local Port: Specify the UDP port that should be used for communications between the Packet Control Function (PCF) and the HSGW.

Important
The UDP port setting on the PCF must match the local-port setting for the HSGW service on the system in order for the two devices to communicate.

Source Violation: This function is intended to allow the operator to configure a network to prevent problems such as when a user gets handed back and forth between two HSGWs a number of times during a handoff scenario.

This function operates in the following manner:

When a subscriber packet is received with a source address violation, the system increments both the IP source-violation reneg-limit and drop-limit counters and starts the timer for the IP-source violation period. Every subsequent packet received with a bad source address during the IP-source violation period causes the reneg-limit and drop-limit counters to increment.
For example, if reneg-limit is set to 5, then the system allows 5 packets with a bad source address (source violations), but on the 5th packet, it re-negotiates PPP.

If the drop-limit is set to 10, the above process of receiving 5 source violations and renegotiating PPP occurs only once. After the second 5 source violations, the call is dropped. The period timer continues to count throughout this process.

If the configured source-violation period is exceeded at any time before the call is dropped, the reneg-limit counter is checked. If the reneg-limit counter is greater than zero (0), the reneg-limit is decremented by 1. If the reneg-limit counter equals zero, the drop-limit is decremented by half.

**Examples**

The following command specifies a UDP port of 3950 for the HSGW service to use to communicate with the PCF on the A10/A11 interface:

```
ip local-port 3950
```

The following command sets the drop limit to 15 and leaves the other values at their defaults:

```
ip source-violation drop-limit 15
```
lifetime

Specifies how long an A10 connection can exist before its registration is considered expired.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

cconfigure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-hsgw-service)#

Syntax Description

lifetime time

[ default | no ] lifetime

default

Resets the lifetime value to the default setting of 1800 seconds.

no

Specifies that an A10 connection can exist for an infinite amount of time.

time

Specifies the time (in seconds) that an A10 connection can exist before its registration is considered expired as an integer from 1 through 65534. Default: 1800

Usage Guidelines

Use this command to set a limit to the amount of time that a subscriber session can remain up whether or not the session is active or dormant. If the lifetime timer expires before the subscriber terminates the session, the connection is terminated automatically.

Examples

The following command specifies a time of 3600 seconds (1 hour) for subscriber sessions on this HSGW service:

lifetime 3600
**max-retransmissions**

Configures the maximum number of times the HSGW service will attempt to communicate with an eAN/PCF before it marks it as unreachable.

**Product**

HSGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

cfg

cfg

Entering the above command sequence results in the following prompt:

```
(config-hsgw-service)
```

**Syntax Description**

- `max-retransmissions count`
- `default max-retransmissions`

**default**

Resets the maximum number of allowed retransmissions to the default value of 5.

**count**

Specifies the maximum number of times the HSGW service will attempt to communicate with an eAN/PCF before it marks it as unreachable.

`count` is an integer from 1 through 1000000. Default: 5

**Usage Guidelines**

Use this command to limit the number of retransmissions to an eAN/PCF before marking it as unreachable. If the value configured is reached, the call is dropped.

**Examples**

The following command configures the maximum number of retransmissions for the HSGW service to 3:

```
max-retransmissions 3
```
mobile-access-gateway

Identifies the mobile access gateway (MAG) context through which MIPv6 calls are to be routed.

Product  HSGW

Privilege  Administrator

Command Modes  Exec > Global Configuration > Context Configuration > HSGW Service Configuration

```configure > context context_name > hsgw-service service_name```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

Syntax Description

- `mobile-access-gateway context context_name [mag-service service_name]`
- `no mobile-access-gateway context`

The `no` command removes the configured MAG context route from this service.

- `context context_name [mag-service service_name]`

Specifies the name of the context and, optionally, the service through which MIPv6 sessions are to be routed. The `context_name` is an existing context expressed as an alphanumeric string of 1 through 79 characters. The `service_name` is an existing MAG service expressed as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to specify where MIPv6 sessions are routed through this service.

Examples

The following command identifies the MAG context MAG1 as the context through which MIPv6 sessions are to be routed and further narrows the route by specifying the service name (mag_serv3):

```
mobile-access-gateway context MAG1 mag-service mag_serv3
```
network-initiated-qos

Enables the use of network initiated QoS functionality.

**Product**
HSGW

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HSGW Service Configuration
configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-hsgw-service)#

**Syntax Description**
| default | no | network-initiated-qos |

**default**
Returns the command to its default setting of enabled.

**no**
Disables the ability to use network initiated QoS functionality.

**Usage Guidelines**
Use this command to enable or disable support for network initiated QoS functionality. Network initiated QoS is enabled by default.

When network initiated QoS functionality is enabled, if the vendor specific network control protocol (VSNCP) protocol configuration options (PCO) arrive from the UE with the BCM set, the HSGW CCR-I includes the Network-Request-Support AVP. If the PCRF behavior returns a BCM of MS+NW when this AVP is received, then flows originating from the network (RSVP Resv) would be triggered upon a PCC-Rule install.
plmn id

Configures Public Land Mobile Network identifiers used to determine if a mobile station is visiting, roaming or belongs to this network.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

{context_name}@host_name(config-hsgw-service)#

Syntax Description

plmn id mcc number mnc number

mcc number mnc number

mcc number: Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999.

mnc number: Specifies the mobile network code (MNC) portion of the PLMN identifier as a 2- or 3-digit integer from 00 through 999.

Usage Guidelines

The PLMN identifier is used to aid the HSGW service in the determination of whether or not a mobile station is visiting, roaming, or home. Multiple P-GW services can be configured with the same PLMN identifier. Up to five PLMN IDs can be configured for each P-GW Service. The configured IDs are used in Diameter-EAP-Request messages (as a Visited-Network-Identifier AVP).

Examples

The following command configures the PLMN identifier with an MCC of 462 and MNC of 2:

plmn id mcc 462 mnc 02
policy overload

Specifies how an HSGW service should handle overload conditions.

Product HSGW

Privilege Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-hsgw-service)#

Syntax Description

policy overload { redirect address | weight weight_num | address2 | weight weight_num | ... address16 | weight weight_num | } | reject | use reject-code { admin-prohibite | insufficient-resources } }

default policy overload

no policy overload { redirect address | address2 | ... | address16 }

default

Returns the command to its default setting of "reject" with the "admin-prohibited" code.

no

Removes a specified "redirect address" from this service.

redirect address | weight weight_num | address2 | weight weight_num | ... address16 | weight weight_num |

This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the HSGW service rejects new sessions with an A11 Registration Reply Code of 88H (unknown HSGW address) and provides the IP address of an alternate HSGW. This command can be issued multiple times.

address: The IP address of an alternate HSGW expressed in IPv4 dotted decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.

weight weight_num: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified, the entry is automatically assigned a weight of 1 (default). weight_num must be an integer value from 1 through 10.
reject [ use reject-code { admin-prohibite | insufficient-resources } ]

This option will cause any overload traffic to be rejected. The HSGW sends an A11 Registration Reply Code of 82H (insufficient resources).

use-reject-code admin-prohibited: When this keyword is specified and traffic is rejected, the error code admin prohibited is returned instead of the error code "insufficient resources". This is the default behavior.

use-reject-code insufficient-resources: When this keyword is specified and traffic is rejected, the error code "insufficient resources" is returned instead of the error code admin prohibited.

Usage Guidelines

Policies can be implemented to dictate HSGW service behavior for overload conditions.

The system invokes the overload policy if the number of calls currently being processed exceeds the licensed limit for the maximum number of sessions supported by the system.

The system automatically invokes the overload policy when an on-line software upgrade is started.

Use the no policy overload command to delete a previously configured policy. If after deleting the policy setting you desire to return the policy parameter to its default setting, use the default policy command.

The chassis is shipped from the factory with the policy options overload disabled

Examples

The following command configures the HSGW service to redirect overload traffic to two IPv4 addresses, one priority weighted 1 and the other priority weighted 5:

policy overload redirect 10.2.3.4 weight 1 10.2.3.5 weight 5
profile-id-qci-mapping

Associates a configured mapping table for RP QoS Profile ID to LTE QoS Class Index (QCI) mapping with this service.

**Product**

HSGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

`configure > context context_name > hsgw-service service_name`

Entering the above command sequence results in the following prompt:

```
(context_name)host_name(config-hsgw-service)#
```

**Syntax Description**

```
profile-id-qci-mapping name
no profile-id-qci-mapping [ name ]
```

- **no**
  
  Removes all profile maps or a specific profile map from this service.

- **name**
  
  Specifies the name of an existing Profile ID - QCI Mapping table to be associated with this service as an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to associate the HSGW service with a configured Profile ID - QCI Mapping table. The table is configured in the Global Configuration Mode using the `profile-id-qci-mapping-table` command.

**Examples**

The following command associates a Profile ID - QCI Mapping table named `table3` with this service:

```
profile-id-qci-mapping table3
```
registration-deny

Configures parameters related to registration rejection.

Product
HSGW

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

/context_name/host_name(config-hsgw-service)#

Syntax Description

registration-deny { handoff connection-setup-record-absent | newcall connection-setup-record-absent } [ use-deny-code { poorly-formed-request | reason-unspecified } ]
[ default | no ] registration-deny { handoff connection-setup-record-absent | newcall connection-setup-record-absent }

default | no
Returns the command to its default settings.

handoff connection-setup-record-absent
When enabled, the HSGW denies or discards handoff R-P sessions that do not have an A11 Connection Setup record in the A11 Registration Request.
Default is disabled. Default HSGW behavior is to accept such requests.

newcall connection-setup-record-absent
When enabled, the HSGW denies or discards new R-P sessions that do not have the A11 Connection Setup record in the A11 Registration Request.
Default is disabled. Default HSGW behavior is to accept such requests.

use-deny-code { poorly-formed-request | reason-unspecified }
Sets the specified Registration Deny Code when denying a new call or handoff because of a missing connection setup record.
Usage Guidelines
Use this command to configure parameters relating to the rejection of registration requests.

Examples
The following command denies registration for registration requests missing the connection setup record and replies with a use deny code of "poorly formed request":

```
registration-deny handoff connection-setup-record-absent use-deny-code poorly-formed-request
```
retransmission-timeout

Configures the maximum allowable time for the HSGW service to wait for a response from the eAN/PCF before it attempts to communicate with the eAN/PCF again (if the system is configured to retry the PCF), or marks the eAN/PCF as unreachable.

**Product**
HSGW

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

(context_name)host_name(config-hsgw-service)#

**Syntax Description**

retransmission-timeout **time**

| default | no | retransmission-timeout |

**default**

Resets the timeout setting to the default value of 3.

**no**

Deletes a previously configured timeout value.

**time**

Specifies the maximum allowable time (in seconds) for the HSGW service to wait for a response from the eAN/PCF before it: a) attempts to communicate with the eAN/PCF again (if the system is configured to retry the PCF), or b) marks the eAN/PCF as unreachable.

**Usage Guidelines**

Use the retransmission timeout command in conjunction with the **max-retransmissions** command in order to configure the HSGW service's behavior when it does not receive a response from a particular PCF.

**Examples**

The following command configures a retransmission timeout value of 5 seconds:

retransmission-timeout 5
**rsvp**

Configures resource reservation protocol (RSVP) parameters for this HSGW service in support of the network initiated QoS feature.

**Product**

HSGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

**Syntax Description**

```
rsvp { max-retransmissions count | retransmission-timeout seconds }
| default | no | rsvp { max-retransmissions | retransmission-timeout }
```

**default**

Resets the maximum number of allowed retransmissions to the default value of 5 or the timeout setting to the default value of 3.

**no**

Disables the feature.

**max-retransmissions count**

Specifies the maximum retransmission count of RP control packets as an integer from 1 through 1000000. Default: 5

**retransmission-timeout seconds**

Specifies the maximum amount of time (in seconds) to allow for retransmission of RP control packets as an integer from 1 through 1000000. Default: 3

**Usage Guidelines**

Use this command to set RSVP parameters for this HSGW service in support of the network initiated QoS feature.
Examples

The following command configures the maximum number of retransmissions to 3:

```
rsvp max-retransmissions 3
```
**setup-timeout**

Specifies the maximum amount of time allowed for session setup.

**Product**
HSGW

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HSGW Service Configuration
configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-hsgw-service)#
```

**Syntax Description**

```
setup-timeout seconds
default| no | setup-timeout
```

- **default**
  
  Resets the command to the default value of enabled with a timeout of 60 seconds.

- **no**
  
  Disables the feature.

- **seconds**
  
  Specifies the maximum amount of time (in seconds) to allow for setup of a session in this service as an integer from 1 though 1000000. Default: 60

**Usage Guidelines**

Use this command to set the maximum amount of time allowed for setting up a session.

**Examples**

The following command sets the maximum time allowed for setting up a session to 5 minutes (300 seconds):

```
setup-timeout 300
```
**spi remote-address**

Configures the security parameter index (SPI) between the HSGW service and the evolved Access Network/evolved Packet Control Function (eAN/ePCF). This command also configures the redirection of calls based on the PCF zone.

**Product**

HSGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

`configure > context context_name > hsgw-service service_name`

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-hsgw-service)#
```

**Syntax Description**

```
spi remote-address { pcf_ip_address | ip_addr_mask_combo } spi-number number { encrypted secret enc_secret | secret secret } | description string | [ hash-algorithm { md5 | rfc2002-md5 } | | replay-protection { nonce | timestamp } | | timestamp-tolerance tolerance | | zone zone_id | ]
no spi remote-address pcf_ip_address spi-number number
```

**pcf_ip_address | ip_addr_mask_combo**

*pcf_ip_address*: Specifies the IP address of the ePCF. *pcf_ip_address* is an IP address expressed in IPv4 dotted decimal notation or IPv6 colon separated notation.

*ip_addr_mask_combo*: Specifies the IP address and mask bits of the PCF. *ip_addr_mask_combo* must be specified using the form "IP Address/Mask Bits" where the IP address must in IPv4 dotted-decimal or IPv6 colon-separated notation, and the mask bits are a numeric value corresponding to the number of bits in the subnet mask.

**spi-number number**

Specifies the SPI which indicates a security context between the PCF and the HSGW as an integer from 256 through 4294967295.

**encrypted secret enc_secret | secret secret**

Configures the shared-secret between the HSGW service and the PCF. The secret can be either encrypted or non-encrypted.

**encrypted secret enc_secret**: Specifies the encrypted shared key (*enc_secret*) between the PCF and the HSGW service. *enc_secret* must be between 1 and 236 alpha and/or numeric characters and is case sensitive.
**secret** secret: Specifies the shared key (secret) between the PCF and the HSGW services. **secret** must be between 1 and 127 alpha and/or numeric characters and is case sensitive.

The **encrypted** keyword is intended only for use by the chassis while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **secret** keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.

**description string**

This is a description for the SPI expressed as an alphanumeric string of 1 through 31 characters.

**hash-algorithm** { md5 | rfc2002-md5 }

Specifies the hash-algorithm used between the HSGW service and the PCF. Default: md5

- **md5**: Configures the hash-algorithm to implement MD5.
- **rfc2002-md5**: Configures the hash-algorithm to implement keyed-MD5.

**replay-protection** { nonce | timestamp }

Specifies the replay-protection scheme that should be implemented by the HSGW service. Default: timestamp

- **nonce**: Configures replay protection to be implemented using NONCE (Number ONCE).
- **timestamp**: Configures replay protection to be implemented using timestamps.

**timestamp-tolerance**

Specifies the allowable difference (in seconds) between timestamps as an integer from 0 through 65535. If the difference is exceeded, the session will be rejected. If set to 0, timestamp tolerance checking is disabled at the receiving end. Default: 60

**zone zone_id**

Specifies the different PCF zones to configure in HSGW service. Mapping of a zone-number to a set of HSGWs can be done per HSGW service basis.

- **zone_id** is an integer value from 1 through 32. A maximum of 32 PCF zones can be configured for a HSGW service.

**Usage Guidelines**

An SPI is a security mechanism configured and shared by the PCF and the HSGW service. Please refer to **IETF RFC 2002: IP Mobility Support** for additional information.

Multiple SPIs can be configured if the HSGW service is communicating with multiple eAN/ePCFs.

**Important**

The SPI configuration on the PCF must match the SPI configuration for the HSGW service on the system in order for the two devices to communicate properly.

This command used with the **zone** keyword redirects all calls on the basis of PCF zone to the specific HSGW on the basis of parameters configured using the **policy pcf-zone-match** command.
Examples

The following command configures the HSGW service to use an SPI of 256 when communicating with a PCF with the IP address 192.168.0.2. The key that would be shared between the PCF and the HSGW service is q397F65.

```
spi remote-address 192.168.0.2 spi-number 256 secret q397F65
```

The following command creates the configured SPI of 400 for an PCF with an IP address of 172.100.3.200 and zone id as 11:

```
spi remote-address 172.100.3.200 spi-number 400 zone 11
```
ue-initiated-qos

Configures the HSGW behavior for UE initiated QoS requests.

Product

HSGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration
configure > context context_name > hsgw-service service_name

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

Syntax Description

| default | no | ue-initiated-qos |

default

Returns the HSGW to the default behavior, where UE initiated QoS requests are accepted and forwarded to the PCRF via Gx interface.

no

Enables rejection of UE initiated QoS request for dedicated bearer in HSGW service. HSGW does not forward the request to the PCRF over Gxa and instead rejects the UE initiated QoS immediately.

Usage Guidelines

Use this command to enable or disable support for UE initiated QoS functionality.

By default, UE initiated QoS requests are accepted and forwarded to the PCRF via Gx interface. If PCRF rejects the UE initiated QoS, UE request is rejected.

This command allows rejection of UE initiated QoS request for dedicated bearer in HSGW service. HSGW does not forward the request to the PCRF over Gxa and instead rejects the UE initiated QoS immediately.

Examples

The following command rejects UE-initiated QoS request for dedicated bearer in HSGW service:

no ue-initiated-qos
unauthorized-flows

Configures the service to wait a specified number of seconds before triggering a QoS update to downgrade an unauthorized flow.

**Product**
HSGW

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HSGW Service Configuration
configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

**Syntax Description**

```
unauthorized-flows qos-update wait-timeout seconds
[ default | no ] unauthorized-flows qos-update wait-timeout

default
Returns the command to its default setting.

no
Removes the configure wait-timeout setting for this service.

qos-update wait-timeout seconds
Specifies the number of seconds to wait before triggering the QoS update to downgrade the unauthorized flow as an integer from 1 through 65534.
```

**Usage Guidelines**

Use this command to specify a wait timeout trigger for flows that are unauthorized by policy rules received via the Gxa interface from the PCRF. When the wit timer expires, the HSGW triggers a QoS update to downgrade the unauthorized flow.

**Examples**

The following command configures the HSGW service to apply the wait time of 30 seconds after receiving an flow unauthorized by the PCRF:

```
unauthorized-flow qos-update wait-timeout 30
```
unauthorized-flows
HSGW Service RoHC Configuration Mode Commands

The HSGW Service RoHC Configuration Mode is used to configure Robust Header Compression (RoHC) parameters for the service.

**Command Modes**

Exec > Global Configuration > Context Configuration > HSGW Service Configuration > HSGW Service RoHC Configuration

```
configure > context context_name > hsgw-service service_name > ip header-compression rohc
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-ip-header-compression-rohc)#
```

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

- cid-mode, page 1596
- end, page 1598
- exit, page 1599
- mrru, page 1600
- profile, page 1601
### cid-mode

This mode allows you to configure options that apply during RoHC compression for the service.

**Product**

HSGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HSGW Service Configuration > HSGW Service RoHC Configuration

`configure > context context_name > hsgw-service service_name > ip header-compression rohc`

Entering the above command sequence results in the following prompt:

`{context_name}@host_name(config-ip-header-compression-rohc)#`

**Syntax Description**

```plaintext
cid-mode { large | small } max-cid integer

default cid-mode

default
Reset all options in the RoHC Profile Compression Configuration mode to their default values.

large
Use large packets with optional information for RoHC

small
This is the default packet size.
Use small RoHC packets.

max-cid integer
Specifies the highest context ID number to be used by the compressor as an integer from 0 through 15 when small packet size is selected, and 0 through 31 when large packet size is selected. Default: 15
```

**Usage Guidelines**

Use this command to set the RoHC packet size and define the maximum

**Examples**

The following command sets large RoHC packet size and sets the maximum CID to 28:

`cid-mode large max-cid 28`
The following command sets the cid-mode to the default settings of small packets and max-cid 0:

```
default cid-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.
**mrru**

Specifies the size of the largest reconstructed reception unit that the decompressor is expected to reassemble from segments. The size includes the CRC. If maximum received reconstructed unit (MRRU) is negotiated to be 0, no segment headers are allowed on the channel.

**Product**

HSGW

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HSGW Service Configuration > HSGW Service RoHC Configuration

`configure > context context_name > hsgw-service service_name > ip header-compression rohc`

Entering the above command sequence results in the following prompt:

`(context_name)host_name(config-ip-header-compression-rohc)#`

**Syntax Description**

```
mrru num_octets

default mrru
```

default

Resets the value of this command to its default setting of 0.

`num_octets`

Specifies the number of allowed octets for the MRRU as an integer from 0 through 65535. Default: 0

**Usage Guidelines**

Use this command to set the size, in octets, of the largest reconstructed reception unit that the decompressor is expected to reassemble from segments.

**Examples**

The following command sets the largest reconstructed reception unit to 1024 octets:

```
mrru 1024
```

The following command resets the MRRU size to its default of 0 octets:

```
default mrru
```
profile

Specifies the header compression profiles to use. A header compression profile is a specification of how to compress the headers of a specific kind of packet stream over a specific kind of link. At least one profile must be specified.

Product
HSGW

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > HSGW Service Configuration > HSGW Service RoHC Configuration

configure > context context_name > hsgw-service service_name > ip header-compression rohc

Entering the above command sequence results in the following prompt:

{context_name} host_name(config-ip-header-compression-rohc)#

Syntax Description

profile { | esp-ip | | rtp-udp | | udp-ip | | uncompressed-ip | }

default profile
default
Default: esp-ip rtp-udp udp-ip uncompressed-ip
Returns the RoHC profile configuration to its default setting.

esp-ip
Enables RoHC Profile 0x0003 which is for ESP/IP compression, compression of the header chain up to and including the first ESP header, but not subsequent subheaders.

rtp-udp
Enables RoHC Profile 0x0001 which is for RTP/UDP/IP compression

udp-ip
Enables RoHC Profile 0x0002 which is for UDP/IP compression; compression of the first 12 octets of the UDP payload is not attempted.

uncompressed-ip
Enables RoHC Profile 0x0000 which is for sending uncompressed IP packets.
Usage Guidelines
Use this command to specify the RoHC header compression profiles.

Examples
The following command sets the profiles to use as esp-ip and rtp-udp:
profile esp-ip rtp-udp
HSS Peer Service Configuration Mode Commands

The HSS Peer Service Configuration Mode is used to create and manage the Home Subscriber Server (HSS) Peer Service.

**Command Modes**

Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

configure > context context_name > hss-peer-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hss-peer-service)#
```

**Important**

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

- auth-request, page 1604
- diameter hss-dictionary, page 1606
- diameter hss-endpoint, page 1608
- diameter suppress, page 1610
- diameter update-dictionary-avps, page 1611
- dynamic-destination-realm, page 1613
- end, page 1614
- exit, page 1615
- failure-handling, page 1616
- request timeout, page 1619
- zone-code-format, page 1620
### auth-request

Configures the number of authentication vectors the MME/SGSN requests in an Authentication-Information-Request (AIR) message to the HSS for each UE requiring authentication.

#### Product
- MME
- SGSN

#### Privilege
Administrator

#### Command Modes
Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

```bash
configure > context context_name > hss-peer-service service_name
```

Entering the above command sequence results in the following prompt:

```bash
<context_name>@host_name(config-hss-peer-service)#
```

#### Syntax Description

```bash
auth-request num-auth-vectors num
default auth-request num-auth-vectors
```

- `num-auth-vectors num`
  Specifies the number of vectors the MME/SGSN is requesting from the HSS as an integer.
  - `num` prior to Release 16, the valid range is 1 through 3. Default = 1.
  - `num` beginning with Release 16, the valid range is 1 through 5. Default = 1.

#### Usage Guidelines
Use this command to configure the number of authentication vectors the MME/SGSN requests in an Authentication-Information-Request (AIR) message to the HSS for each UE requiring authentication.

Receiving multiple vectors from the HSS for a given UE helps reduce the number of messages across the diameter connection plus provides the MME/SGSN with additional vectors for the UE in the event that the connection or the HSS id disabled.

**Related Commands:**

- To view the current number of requested vectors, execute the `show hss-peer-service service name <name>` command in the Exec mode.
- To set the minimum number (low watermark) of vectors to be maintained at all times, execute `min-unused-auth-vector min_num` command from the call control profile configuration mode. (SGSN only)
• For troubleshooting, check the number of free, used, or in-use vectors displayed in the output of the
  `show subscribers [gprs-only | sgsn-only] full` command. (SGSN only).

**Examples**

The following command sets the number of requested vectors to 2:

```
auth-request num-auth-vectors 2
```
diameter hss-dictionary

Specifies the Diameter Credit Control dictionary for the HSS peer service.

<table>
<thead>
<tr>
<th>Product</th>
<th>MME</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SGSN</td>
</tr>
</tbody>
</table>

| Privilege | Administrator |

| Command Modes | Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration
|               | configure > context context_name > hss-peer-service service_name |

Entering the above command sequence results in the following prompt:

```
{context_name} host_name {config-hss-peer-service} #
```

**Syntax Description**

diameter hss-dictionary { custom1 | standard | standard-r9 } { eir-dictionary { custom1 | standard | standard-r9 } } 

default diameter hss-dictionary 

default

Sets the dictionary to default standard-r9 for HSS peer service.

custom1

Sets the Diameter dictionary to a customer-specific HSS Diameter dictionary. Default: Disabled

standard

Sets the Diameter dictionary to the standard (3GPP release 8) HSS peer dictionary. Default: Disabled

standard-r9

Sets the Diameter dictionary to the standard HSS peer dictionary for 3GPP release 9. Default: Enabled

eir-dictionary { custom1 | standard | standard-r9 }

Specifies that an Equipment Identity Register (EIR) dictionary is to be used in conjunction with the HSS Diameter dictionary.

custom1: Sets the EIR Diameter dictionary to a customer-specific EIR Diameter dictionary.

standard: Sets the EIR Diameter dictionary to the standard HSS peer dictionary.
**standard-r9**: Sets the EIR Diameter dictionary to the standard HSS peer dictionary for release 9.

**Usage Guidelines**

Use this command to select the Diameter dictionary and, optionally, the EIR end-point dictionary, for the HSS peer service.

**Examples**

The following command sets the Diameter dictionary to IETF RFC 4006 specific:

```
diameter hss-dictionary standard
```

The following command sets the special 'custom2' dictionary as the EIR dictionary:

```
diameter hss-dictionary standard eir-dictionary custom2
```
diameter hss-endpoint

Associates a preconfigured Diameter origin endpoint with this HSS peer service.

Product
MME
SGSN

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

configure > context context_name > hss-peer-service service_name

Entering the above command sequence results in the following prompt:

{context_name}host_name(config-hss-peer-service)#

Syntax Description

\[\text{diameter hss-endpoint} endpoint_name [\text{eir-endpoint} eir_endpoint_name] [\text{auc-endpoint} auc_endpoint_name] \]

\[\text{no} \text{diameter hss-endpoint}\]

no

Removes previously associated Diameter origin endpoint from this HSS peer service.

endpoint_name

Identifies a preconfigured Diameter endpoint specific to the HSS interface. The endpoint must be present in all Diameter messages and is the endpoint that originates the Diameter message.

endpoint_name is a preconfigured Diameter endpoint name expressed as an alphanumeric string of 1 through 63 characters.

eir-endpoint eir_endpoint_name

Identifies a preconfigured Diameter endpoint specific to the S13 or S13’ Equipment Identity Register (EIR) interface.

eir_endpoint_name must be an existing Diameter endpoint expressed as an alphanumeric string of 1 through 63 characters.
**auc-endpoint auc_endpoint_name**

**auc-endpoint** Including this keyword option enables routing to an authentication center (AuC) as the endpoint in place of the hss-endpoint. If configured, all AIR messages are routed to this AuC-endpoint. If not configured, all AIR messages are sent to the configured HSS endpoint.

**auc_endpoint_name** Identifies the AuC endpoint and must be a unique endpoint name comprised of a string of 1 to 63 alphanumeric characters.

**Usage Guidelines**

Use this command to associate a Diameter origin endpoint to create a Diameter-based S6a or S6d (SGSN) interface association in this HSS peer service to provide AAA functionality to the EPS bearer context.

Optionally, use this command to associate a Diameter origin endpoint to create a Diameter-based S13 or S13' (SGSN) interface association in this HSS peer service to provide IMEI query capability between the MME and an EIR.

A second option, the **auc-endpoint** keyword, enables you to use this command to define an authentication center (AuC) as the routing endpoint in place of the hss-endpoint. If configured, all AIR messages are routed to this AuC endpoint. If not configured, all AIR messages are sent to the configured HSS endpoint.

**Important**

The configuration of all endpoints is only valid when all necessary endpoint configuration has been completed. All endpoint listed above must also be defined as valid endpoints using the commands in the Diameter Endpoint configuration mode (refer to the Diameter Endpoint Configuration Mode Commands chapter in the Command Line Interface Reference manual) for more information on Diameter endpoint configuration parameters.

**Examples**

The following command associates the preconfigured Diameter endpoint **hss_1** with this HSS peer service for HSS interface support.

```
diameter hss-endpoint hss_1
```

The following command enables use of an authentication center (AuC1) in place of an HSS server (HSS1) as an endpoint for Diameter originated messages:

```
diameter hss-endpoint HSS1 auc-endpoint AuC1
```
diameter suppress

Configures the MME to restrict the sending of the Notify-Request-Message to the HSS. By default, the Notify-Request-Message is sent to the HSS.

**Product**
MME

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

**Syntax Description**

| no | diameter suppress notify-request |

  **Usage Guidelines**
Use this command to restrict the MME from sending the Notify-Request-Message to the HSS. This can be used to control whether handover to non-3GPP access can occur.
diameter update-dictionary-avps

Specifies which release of 3GPP TS 29.272 is to be used for the HSS peer service.

**Product**
- MME
- SGSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

configure > context context_name > hss-peer-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name] host_name (config-hss-peer-service)#
```

**Syntax Description**

```
diameter update-dictionary-avps { 3gpp-r10 | 3gpp-r11 | 3gpp-r9 }
no diameter update-dictionary-avps
```

- **no**
  Sets the command to the default value where Release 8 ('standard') dictionary is used for backward compatibility of previous releases.

- **3gpp-r10**
  Configures the MME/SGSN to signal additional AVPs to HSS in support of Release 10 of 3GPP 29.272.

- **3gpp-r11**
  Configures the MME/SGSN to signal additional AVPs to HSS in support of Release 11 of 3GPP 29.272.
  Using this keyword is necessary to enable the MME to fully support inclusion of the Additional Mobile Station ISDN (A-MSISDN) flag of the Feature List AVP in Update Location Request (ULR) messages sent over the S6a interface to the HSS at the time a UE Attaches. For more information about supporting A-MSISDN, refer to the information for the a-msisdn command in the Call-Control Profile configuration mode.

- **3gpp-r9**
  Configures the MME/SGSN to signal Release 9 AVPs to HSS.

**Usage Guidelines**

Use this command to configure the 3GPP release that should be supported for this HSS peer service.
This command is only applicable for the 'standard' diameter dictionary as defined in the **diameter hss-dictionary** command.

**Examples**

After a command is issued to support the AVPs as defined by the various releases of the 3GPP 29.272 spec, use the following command to disable the support:

```
no diameter update-dictionary-avps
```
**dynamic-destination-realm**

Enables the MME to construct the destination realm using the MCC and MNC of foreign subscribers.

**Product**
MME

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

configure > context context_name > hss-peer-service service_name

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-hss-peer-service)#`

**Syntax Description**

<table>
<thead>
<tr>
<th>default</th>
<th>no</th>
<th>dynamic-destination-realm</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Returns the configuration to the default setting, where the MME uses the configured peer realm as the destination realm.

| no |    |                           |
|    |    |                           |

Disables the dynamic destination realm configuration. This provides the same behavior as the `default` keyword.

**Usage Guidelines**

This command configures the MME to derive the EPC Home Network Realm/Domain based on the user's IMSI (MNC and MCC values) and use it as the Destination Realm in all diameter messages.

For a foreign subscriber, the MME does not know the HSS nodes in all the foreign PLMNs. In this case the MME routes S6a/S6d requests directed to foreign PLMNs via a Diameter Routing Agent (DRA) using only the destination realm. The DRA in turn routes the request to the correct HSS based on the destination realm. In order to accomplish this, the MME needs to dynamically construct requests to the DRA/HSS with a Destination Realm representing the foreign PLMN of the UE.

Refer to Configuring Dynamic Destination Realm Construction for Foreign Subscribers in Chapter 2 of the MME Administration Guide for more information about configuring this feature.

**Examples**

The following command configures the MME to derive the destination realm for foreign subscribers based on the user's IMSI (MNC/MCC).

`dynamic-destination-realm`
**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

Configures failure handling behavior in the event of a failure with the HSS peer service. It also defines the action on various error codes on the Diameter interface during authentication or session activities.

**Product**

MME

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

`configure > context context_name > hss-peer-service service_name`

Entering the above command sequence results in the following prompt:

`(context_name)host_name(config-hss-peer-service)#`

**Syntax Description**

failure-handling { authentication-information-request | check-identity-request | notify-request | purge-ue-request | update-location-request } { diameter-result-code start_error_code [ to end_error_code ] | request-timeout } action { continue | retry-and-terminate | terminate }

no failure-handling { authentication-information-request | check-identity-request | notify-request | purge-ue-request | update-location-request } diameter-result-code start_error_code [ to end_error_code ]

default failure-handling { authentication-information-request | check-identity-request | notify-request | purge-ue-request | update-location-request } request-timeout

no

Removes the preconfigured failure handling procedures for calls in an HSS peer service.

default

Sets the default action for failure handling procedure for calls in an HSS peer service.

For default actions on Diameter result/error codes see the Usage section below.

**authentication-information-request**

Configures the MME-HSS service to handle the failures in an Auth-Information-Request message.

Configures the SGSN-HSS service to handle the failures in an Auth-Information-Request message.
check-identity-request
Configures the MME-HSS service to handle the failures in a Check-Identity-Information-Request message.
Configures the SGSN-HSS service to handle the failures in a Check-Identity-Information-Request message.

notify-request
Configures the MME-HSS service to handle the failures in a Notify-Request message.
This option is not supported on SGSN.

purge-ue-request
Configures the MME-HSS service to handle the failures in a Purge-UE-Request message.
Configures the SGSN-HSS service to handle the failures in a Purge-UE-Request message.

update-location-request
Configures the HSS peer service to handle the failures in an Update-Location-Request message.

diameter-result-code start_error_code [to end_error_code]
Configures the HSS peer service to handle the failures for various request messages having specific single or range of Diameter result codes in a request message.

start_error_code specifies an individual error code for Diameter protocol as an integer from 3000 through 5999. This will be the starting of code if a range of error codes is specified with the optional keyword to end_error_code.

to end_error_code is used to specify a range of error codes to handle by this command. end_error_code specifies the end error code for Diameter protocol as an integer from 3000 through 5999.

request-timeout
Configures the HSS peer service to handle the failures for various request messages if response to that message is not received before timeout duration exhausted.

action { continue | retry-and-terminate | terminate }
Specifies the action to be taken on failure of any message as a policy for failure handling.

• continue: This option works differently for each system.

  For the SGSN: On receipt of any error for MICR session request, the SGSN allows the HSS peer service to continue with the session procedure without any interruption. For all other request/message types, the SGSN behaves as it would if configured for the retry-and-terminate option.

  For the MME: The MME does not support this option and if continue is included in the command, the MME behaves as it would if configured for the retry-and-terminate option.

  For 12.0 and earlier releases the continue option in failure handling on SGSN for IMEI procedures has the same behavior as that of the retry-and-terminate option.
For releases after 14.0, the **continue** option for IMEI procedure on SGSN can be configured in case of timeout and error responses requests from HSS so that the requests will be re-tried on a second peer (if configured) and the call is continued. The configuration of **continue** option for IMEI procedure is as follows:

```plaintext
configure context <name>
   hss-peer-service <name>
      failure-handling check-identity-request request-timeout action continue
      failure-handling check-identity-request diameter-result-code <range1> to <range2> action continue
      failure-handling check-identity-request diameter-result-code <range1> action continue
      exit
      exit
      exit

- **retry-and-terminate**: On receipt of any error, once the configured condition (either the request timeout or receipt of the specified result code) occurs, the system retries sending the request (AIR/ULR/NOR/PUR/MICR) to another peer that is configured in the same endpoint. If no response is received for AIR or ULR from the second peer, then the system allows the HSS peer service to terminate the session.

- **terminate**: On receipt of any error, once the configured condition (either the request timeout or receipt of the specified result code) is met, the system allows the HSS peer service to immediately terminate the session (AIR/ULR/MICR) without any further action.

**Usage Guidelines**

Use this command to configure the failure handling behavior in the event of a communication failure with the HSS peer service.

The following are the default actions 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.

- 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 will allow HSS peer service to continue if any failure in Auth-Information-Request message occurred with Diameter error code 3050:

```plaintext
failure-handling authentication-information-request diameter-result-code 3050 action continue
```
request timeout

Configures the application request timeout between the HSS peer service and HSS node. The MME/SGSN waits for this duration before retransmitting the request to corresponding HSS node.

**Product**

MME  
SGSN

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration  
`configure > context context_name > hss-peer-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hss-peer-service)#
```

**Syntax Description**

```
request timeout `dur`
[ no | default ] request timeout
```

- **no**
  Disables the configured application request timeout value.

- **default**
  Sets the application request time out duration to default value of 300 seconds.

- **dur**
  Specifies the application request timeout duration (in seconds) as an integer from 1 through 300. The MME/SGSN will wait for this duration before retrying the request with corresponding HSS. Default: 20

**Usage Guidelines**

Use this command to set the waiting period for HSS peer service in seconds after which the request is deemed to have failed or system will resend the request.

**Examples**

The following example configures the application request timeout duration to 20 seconds:

```
default request timeout
```
zone-code-format

Configures how the MME must interpret the received zone-code values from the HSS.

Product
MME

Privilege
Administrator

Command Modes
Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration
configure > context context_name > hss-peer-service service_name

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

Syntax Description
zone-code-format { ascii-string }
| default | zone-code-format

default
Returns the command to the default setting, where the MME interprets the zone-code as an octet string.

ascii-string
Configures the MME to interpret the zone-code as an ascii string. This option is provided to maintain backward compatibility.

When configured as ascii-string, the MME interprets the received zone-code as an ASCII string (coded in hexadecimal representation) and converts it byte by byte to an integer value. For example, if the HSS sends the zone-code value as 3032, the MME converts this to 02 (ASCII value of 0 in Hex is 0x30, ASCII value of 2 in Hex is 0x32). With this configuration, the MME accepted zone-codes only within the range of 0 to 99.

Usage Guidelines
This new command specifies the format of the zone-code value received from HSS to MME. The MME uses this configuration to interpret and convert the received zone-code value to an integer value and validate it against the list of allowed zone-code configured for the zone-code restriction feature.

By default, the MME interprets the received zone-code value from HSS as a octet-string (2 bytes) which is coded in full hexadecimal representation. The MME converts the entire 2 byte octet string coded in hexadecimal to integer value and it uses the same for validation for zone-code restriction feature. For example, if the HSS sends the zone-code value as 3032, MME converts this to 12338 (which is the equivalent of 0x3032).
Examples

The following command configures the HSS Peer Service to interpret the zone-code received from the HSS as an ASCII string.

`zone-code-format ascii-string`