

Ultra Cloud Core 5G Session Management Function, Release 2025.02 - CLI Command Reference

First Published: 2025-04-30

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

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

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

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

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

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

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

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

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

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

© 2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

About this Guide xxxv

Conventions Used xxxv

CHAPTER 1

Configuration Command Reference 1

aaa 23

active-charging service 24

active-charging service bandwidth-policy 24

active-charging service bandwidth-policy flow limit-for-bandwidth id 25

active-charging service bandwidth-policy group-id 25

active-charging service bandwidth-policy group-id direction downlink grpPeakBwp 26

active-charging service bandwidth-policy group-id direction uplink grpPeakBwp 27

active-charging service buffering-limit 29

active-charging service charging-action 29

active-charging service charging-action allocation-retention-priority 30

active-charging service charging-action billing-action 31

active-charging service charging-action cca charging credit 32

active-charging service charging-action flow action 32

active-charging service charging-action flow action discard 33

active-charging service charging-action flow action readdress 33

active-charging service charging-action flow limit-for-bandwidth 34

active-charging service charging-action flow limit-for-bandwidth direction downlink peak-data-rate 34

active-charging service charging-action flow limit-for-bandwidth direction uplink peak-data-rate 35

active-charging service charging-action tft packet-filter 37

active-charging service charging-action tos af11 37

active-charging service charging-action tos af12 38

active-charging service charging-action tos af13 38

active-charging service charging-action tos af21 38
active-charging service charging-action tos af22 39
active-charging service charging-action tos af23 39
active-charging service charging-action tos af31 40
active-charging service charging-action tos af32 40
active-charging service charging-action tos af33 40
active-charging service charging-action tos af41 41
active-charging service charging-action tos af42 41
active-charging service charging-action tos af43 42
active-charging service charging-action tos be 42
active-charging service charging-action tos ef 42
active-charging service charging-action tos lower-bits 43
active-charging service content-filtering category policy-id 43
active-charging service content-filtering category policy-id analyze priority 44
active-charging service content-filtering category policy-id analyze priority all 44
active-charging service content-filtering category policy-id analyze priority category 45
active-charging service content-filtering category policy-id analyze priority x-category 47
active-charging service credit-control group 48
active-charging service credit-control group associate 48
active-charging service credit-control group diameter 49
active-charging service credit-control group diameter origin 49
active-charging service credit-control group diameter service-context-id 50
active-charging service credit-control group diameter session 50
active-charging service credit-control group failure-handling initial-request continue 50
active-charging service credit-control group failure-handling initial-request retry-and-terminate 51
active-charging service credit-control group failure-handling initial-request terminate 51
active-charging service credit-control group failure-handling terminate-request continue 52
active-charging service credit-control group failure-handling terminate-request retry-and-terminate 52
active-charging service credit-control group failure-handling terminate-request terminate 53
active-charging service credit-control group failure-handling update-request continue 53
active-charging service credit-control group failure-handling update-request retry-and-terminate 54
active-charging service credit-control group failure-handling update-request terminate 54
active-charging service credit-control group pending-traffic-treatment forced-reauth 55
active-charging service credit-control group pending-traffic-treatment noquota 55

active-charging service credit-control group pending-traffic-treatment noquota limited-pass 56
active-charging service credit-control group pending-traffic-treatment quota-exhausted 56
active-charging service credit-control group pending-traffic-treatment trigger 57
active-charging service credit-control group pending-traffic-treatment validity-expired 57
active-charging service credit-control group quota holding-time 58
active-charging service credit-control group quota request-trigger 58
active-charging service credit-control group timestamp-rounding 58
active-charging service credit-control group usage-reporting quotas-to-report based-on-grant 59
active-charging service group-of-ruledefs 59
active-charging service group-of-ruledefs add-ruledef priority 60
active-charging service p2p-detection attribute ssl-renegotiation 60
active-charging service p2p-detection ecs-analysis 61
active-charging service p2p-detection protocol 62
active-charging service packet-filter 62
active-charging service packet-filter ip local-port operator 63
active-charging service packet-filter ip local-port range 64
active-charging service packet-filter ip protocol 64
active-charging service packet-filter ip remote-address 65
active-charging service packet-filter ip remote-port operator 66
active-charging service packet-filter ip remote-port range 66
active-charging service packet-filter ip tos-traffic-class 67
active-charging service rulebase 67
active-charging service rulebase action 68
active-charging service rulebase action priority 69
active-charging service rulebase action priority dynamic-only 69
active-charging service rulebase action priority dynamic-only adc group-of-ruledefs 69
active-charging service rulebase action priority dynamic-only adc ruledef 70
active-charging service rulebase action priority dynamic-only group-of-ruledefs 71
active-charging service rulebase action priority dynamic-only ruledef 72
active-charging service rulebase action priority group-of-ruledefs 73
active-charging service rulebase action priority ruledef 74
active-charging service rulebase action priority static-and-dynamic group-of-ruledefs 74
active-charging service rulebase action priority static-and-dynamic ruledef 75
active-charging service rulebase action priority timedef group-of-ruledefs 76

active-charging service rulebase action priority timedef ruledef 77
active-charging service rulebase bandwidth 78
active-charging service rulebase billing-records 78
active-charging service rulebase billing-records udr 79
active-charging service rulebase cca diameter requested-service-unit sub-avp time 79
active-charging service rulebase cca diameter requested-service-unit sub-avp units 80
active-charging service rulebase cca diameter requested-service-unit sub-avp volume 80
active-charging service rulebase cca quota holding-time 81
active-charging service rulebase cca quota retry-time 81
active-charging service rulebase cca quota time-duration 82
active-charging service rulebase content-filtering category 83
active-charging service rulebase content-filtering flow-any-error 83
active-charging service rulebase content-filtering mode 84
active-charging service rulebase credit-control-group 84
active-charging service rulebase dynamic-rule 85
active-charging service rulebase edr transaction-complete 86
active-charging service rulebase egcdr threshold 86
active-charging service rulebase egcdr threshold volume 87
active-charging service rulebase flow control-handshaking 88
active-charging service rulebase flow control-handshaking charge-to-application 88
active-charging service rulebase flow end-condition 89
active-charging service rulebase flow limit-across-applications 89
active-charging service rulebase ip 90
active-charging service rulebase p2p 90
active-charging service rulebase post-processing priority 91
active-charging service rulebase post-processing priority group-of-ruledefs 91
active-charging service rulebase post-processing priority ruledef 92
active-charging service rulebase route priority 92
active-charging service rulebase route priority ruledef 93
active-charging service rulebase rtp 94
active-charging service rulebase tcp 94
active-charging service rulebase tcp mss 95
active-charging service rulebase tcp packets-out-of-order 95
active-charging service rulebase tcp packets-out-of-order transmit 96

active-charging service rulebase tethering-detection 97
active-charging service rulebase url-blacklisting action 98
active-charging service rulebase url-blacklisting match-method 98
active-charging service ruledef 99
active-charging service ruledef bearer service-3gpp rat-type 100
active-charging service ruledef dns answer-name 100
active-charging service ruledef dns any-match 101
active-charging service ruledef dns previous-state 102
active-charging service ruledef dns query-name 103
active-charging service ruledef dns query-type 104
active-charging service ruledef dns return-code 105
active-charging service ruledef dns state 106
active-charging service ruledef dns tid 106
active-charging service ruledef http content type 107
active-charging service ruledef http host 108
active-charging service ruledef http referer 109
active-charging service ruledef http url 110
active-charging service ruledef http user-agent 111
active-charging service ruledef icmpv6 any-match 111
active-charging service ruledef ip any-match 112
active-charging service ruledef ip dst-address 113
active-charging service ruledef ip protocol 115
active-charging service ruledef ip server-ip-addr 115
active-charging service ruledef ip uplink 117
active-charging service ruledef ip version 117
active-charging service ruledef multi-line-or 118
active-charging service ruledef p2p 118
active-charging service ruledef p2p app-identifier 119
active-charging service ruledef p2p protocol 120
active-charging service ruledef p2p traffic-type 129
active-charging service ruledef rtp any-match 130
active-charging service ruledef rtsp any-match 131
active-charging service ruledef secure-http any-match 132
active-charging service ruledef secure-http uplink 133

active-charging service ruledef tcp any-match 134
active-charging service ruledef tcp either-port with-portMap-range 135
active-charging service ruledef tcp either-port with-range 135
active-charging service ruledef tcp either-port without-range 136
active-charging service ruledef tcp flag 137
active-charging service ruledef tcp state 138
active-charging service ruledef tethering-detection 139
active-charging service ruledef tethering-detection application 139
active-charging service ruledef tethering-detection dns-based 140
active-charging service ruledef tethering-detection ip-ttl 140
active-charging service ruledef tethering-detection os-ua 140
active-charging service ruledef udp any-match 141
active-charging service ruledef udp either-port with-portMap-range 142
active-charging service ruledef udp either-port with-range 142
active-charging service ruledef udp either-port without-range 143
active-charging service ruledef wsp any-match 144
active-charging service ruledef wtp any-match 145
active-charging service ruledef www any-match 146
active-charging service ruledef www host 147
active-charging service ruledef www url 148
active-charging service url-blacklisting 148
active-charging service urr-list 149
active-charging service urr-list urr-list-data 149
active-charging service urr-list urr-list-data service-identifier 150
apn 150
apn active-charging 151
apn authorize-with-hss 151
apn authorize-with-hss egtp 151
apn authorize-with-hss egtp gn-gp-enabled 152
apn authorize-with-hss egtp s2b 152
apn authorize-with-hss egtp s2b gn-gp-enabled 152
apn authorize-with-hss egtp s2b s5-s8 152
apn authorize-with-hss egtp s5-s8 153
apn authorize-with-hss egtp s5-s8 s2b 153

apn authorize-with-hss lma 154
apn cc-profile 154
apn content-filtering category 155
apn data-tunnel 155
apn gtpp group 155
apn ip access-group 156
apn ip source-violation 156
apn ppp 157
apn timeout 157
cd 157
cdl clear 158
cdl show sessions 158
cdl show status 159
clear diameter routes dynamic 160
clear ipam 160
clear ipam 160
clear lawful-intercept stats 161
clear subscriber 161
clear subscriber imsi-opt 163
clear subscriber supi-opt 164
client http header 165
client http ping 165
client inbound interface 166
client inbound interface limit overload 166
client inbound interface limit pending 166
client inbound limit overload 167
client inbound limit pending 167
client outbound host ping 167
client outbound interface 168
client outbound interface host ping 168
client outbound interface limit consecutive failure 169
client outbound interface limit pending 170
client outbound limit consecutive failure 170
client outbound limit pending 171

commit 171
compare 172
config 172
config-error info 173
datastore dbs 173
datastore dbs endpoints 173
datastore notification-ep 174
datastore session-db 174
datastore session-db endpoints 174
deployment 175
deployment resource 176
describe 176
diagnostics info 177
dump 178
dump core 178
dump transactionhistory 179
edr 179
edr file files 180
edr file files disable 181
edr file files flush 181
edr file files limit 181
edr file files procedure-id disable-event-id 182
edr file files procedure-id disable-event-id disable-inner disable 182
edr file files procedure-id disable-event-id disable-inner event-id disable-field-id 182
edr file files procedure-id disable-event-id disable-inner event-id disable-field-id disable 183
edr file transaction field priorityClass 183
endpoint all 184
endpoint info 184
exit 185
geo maintenance 185
geo replication-pull 186
geo reset-role 186
geo switch-role 186
geomonitor podmonitor pods 187

geomonitor remoteclustermonitor 188
geomonitor trafficMonitor 188
geomonitor vipmonitor instance 189
geomonitor vipmonitor instance vips 189
group nf-mgmt 190
group nf-mgmt heartbeat 191
group nrf discovery 191
group nrf discovery service type nrf 191
group nrf discovery service type nrf endpoint-profile 192
group nrf discovery service type nrf endpoint-profile endpoint-name 193
group nrf discovery service type nrf endpoint-profile endpoint-name primary ip-address 193
group nrf discovery service type nrf endpoint-profile endpoint-name secondary ip-address 194
group nrf discovery service type nrf endpoint-profile endpoint-name tertiary ip-address 195
group nrf discovery service type nrf endpoint-profile version uri-version 195
group nrf mgmt 196
group nrf mgmt service type nrf 196
group nrf mgmt service type nrf endpoint-profile 197
group nrf mgmt service type nrf endpoint-profile endpoint-name 197
group nrf mgmt service type nrf endpoint-profile endpoint-name primary ip-address 198
group nrf mgmt service type nrf endpoint-profile endpoint-name secondary ip-address 199
group nrf mgmt service type nrf endpoint-profile endpoint-name tertiary ip-address 199
group nrf mgmt service type nrf endpoint-profile version uri-version 200
gtpp group 200
gtpp group gtpp egcdr final-record closing-cause 201
gtpp group gtpp egcdr losdv-max-containers 201
gtpp group gtpp egcdr service-data-flow threshold 201
gtpp group gtpp egcdr service-data-flow threshold volume 202
gtpp group gtpp egcdr service-idle-timeout 202
gtpp group gtpp trigger 203
gtpp group gtpp trigger egcdr 203
help 203
history 205
id 205
idle-timeout 205

ignore-leading-space 206
infra metrics experimental 206
infra metrics verbose verboseLevels 206
infra metrics verbose verboseLevels metrics metricsList 207
infra transaction limit 208
infra transaction limit consecutive same 208
infra transaction loop 209
infra transaction loop category 209
infra transaction loop category threshold 209
infra transaction loop category threshold thresholds 210
instance instance-id 210
endpoint-gtpprime 211
instance instance-id endpoint ep 212
instance instance-id endpoint diameter 214
instance instance-id endpoint ep cpu 215
instance instance-id endpoint ep extended-service 215
instance instance-id endpoint ep heartbeat 216
instance instance-id endpoint gtpprime 216
instance instance-id endpoint ep interface 217
instance instance-id endpoint ep interface dispatcher 218
instance instance-id endpoint ep interface echo 220
instance instance-id endpoint ep interface heartbeat 220
instance instance-id endpoint ep interface internal base-port 221
instance instance-id endpoint ep interface overload-control client threshold critical 221
instance instance-id endpoint ep interface overload-control client threshold high 223
instance instance-id endpoint ep interface overload-control client threshold low 224
instance instance-id endpoint ep interface overload-control endpoint threshold critical 225
instance instance-id endpoint ep interface overload-control endpoint threshold high 226
instance instance-id endpoint ep interface overload-control endpoint threshold low 227
instance instance-id endpoint ep interface overload-control msg-type messageConfigs 228
instance instance-id endpoint ep interface path-failure 230
instance instance-id endpoint ep interface retransmission 230
instance instance-id endpoint ep interface secondary-ip 230
instance instance-id endpoint ep interface sla 231

instance instance-id endpoint ep interface supported-features 231
instance instance-id endpoint ep interface sx-path-failure 232
instance instance-id endpoint ep interface vip 232
instance instance-id endpoint ep interface vip6 233
instance instance-id endpoint ep internal base-port 233
instance instance-id endpoint ep labels pod-config 233
instance instance-id endpoint ep memory 234
instance instance-id endpoint ep path-failure 234
instance instance-id endpoint ep retransmission 235
instance instance-id endpoint ep secondary-ip 235
instance instance-id endpoint ep sla 236
instance instance-id endpoint ep sx-path-failure 236
instance instance-id endpoint ep system-health-level crash 236
instance instance-id endpoint ep system-health-level critical 237
instance instance-id endpoint ep system-health-level warn 238
instance instance-id endpoint ep vip 238
instance instance-id endpoint ep vip6 239
instance instance-id endpoint fqdn 239
instance instance-id endpoint gtp interface interface-name 240
instance instance-id endpoint pfcp interface n4 reactivate-peer condition 240
instance instance-id endpoint radius 241
instances instance 242
instance instance-id interface fqdn 242
instance instance-id smf-fqdn 243
instance instance-id interface fqdn 243
ipam 243
exec-ipam reclaim-chunk 243
ipam dp 244
ipam instance 244
ipam instance address-pool 245
ipam instance address-pool ipv4 246
ipam instance address-pool ipv4 address-range 246
ipam instance address-pool ipv4 chunk-group 247
ipam instance address-pool ipv4 prefix-range 247

ipam instance address-pool ipv4 split-size 248
ipam instance address-pool ipv4 threshold 248
ipam instance address-pool ipv4 vlan 249
ipam instance address-pool ipv6 249
ipam instance address-pool ipv6 address-ranges address-range 249
ipam instance address-pool ipv6 address-ranges prefix-range 250
ipam instance address-pool ipv6 prefix-ranges prefix-length 251
ipam instance address-pool ipv6 address-ranges chunk-group 251
ipam instance address-pool ipv6 address-ranges split-size 251
ipam instance address-pool ipv6 address-ranges threshold 252
ipam instance address-pool ipv6 vlan 253
ipam instance address-pool ipv6 prefix-ranges prefix-range 253
ipam instance address-pool ipv6 prefix-ranges chunk-group 253
ipam instance address-pool ipv6 prefix-ranges split-size 254
ipam instance address-pool ipv6 prefix-ranges threshold 255
ipam instance address-pool tags 255
ipam instance audit chunk 256
ipam instance chunk throttling 256
ipam instance chunk-reclamation 256
ipam instance data-sharding 257
ipam instance min-dp-addr-size 258
ipam instance source 258
ipam instance source external ipam 259
ipam instance threshold 259
ipam pool 260
ipam pool ipv4-addr 260
ipam pool ipv6-addr 260
job 261
k8 ccg 261
k8 ccg coverage 261
k8 label pod-group-config 262
leaf-prompting 262
license smart deregister 263
license smart register 263

license smart renew 264
local-instance 264
load factor 264
logging async application enable 265
logging async monitor-subscriber enable 265
logging async tracing enable 266
logging async transaction enable 266
logging error 266
logging json-logging 267
logging level 267
logging logger 269
logging logger level 269
logging transaction 271
logout 272
message type 272
mode debug exec action release-resource 273
monitor protocol 274
monitor active-instance-traffic 275
monitor-protocol cpu-limit 276
monitor subscriber 276
msid-opt 277
nf-tls ca-certificates 278
nf-tls certificate-status 278
nf-tls certificates 279
no 280
nodemonitor 280
nrf discovery-info discovery-filter 280
nrf discovery-info discovery-filter nf-discovery-profile 281
nrf discovery-info discovery-filter nf-discovery-profile nf-service 281
nrf registration-info 281
nrf subscription-info 281
nssai 282
paginate 282
pcscf mark-online 283

peers all 283
policy 283
policy actionmgmt 284
policy call-control-profile 285
policy call-control-profile cc 286
policy call-control-profile cc local-value 286
policy dnn 287
policy dnn dnn dnn 287
policy dnn dnn network-identifier 288
policy dnn dnn network-identifier operator-identifier 288
policy dnn dnn operator-identifier 288
policy eventmgmt 289
policy network-capability 290
policy operator 291
policy operator policy 291
policy path-failure-detection 292
policy path-failure-detection ignore 292
policy rulemgmt 293
policy subscriber 293
policy subscriber list-entry 294
policy subscriber list-entry imsi 295
policy subscriber list-entry imsi msin 296
policy subscriber list-entry serving-plmn 296
policy sx-path-failure-detection 297
policy sx-path-failure-detection ignore 297
policy upf-selection 298
policy upf-selection list-entry 298
policy upf-selection list-entry query-params 298
profile access 299
profile access eps-fallback cbr 299
profile access eps-fallback guard 300
profile access eps-fallback trigger-cause group 300
profile access erir 301
profile access gtpc 301

profile access gtpc message-handling create-session-request ho-ind 302
profile access gtpc message-handling create-session-response action 302
profile access gtpc message-handling create-session-response condition 303
profile access n1 message-handling pdu-establishment condition 303
profile access n1 message-handling pdu-release condition 304
profile access n1 t3591-pdu-mod-cmd 304
profile access n1 t3592-pdu-rel-cmd 305
profile access n1 305
profile access n2 306
profile access n11 306
profile access n2 idft 307
profile access n26 idft 307
profile charging 307
profile charging accounting limit 309
profile charging accounting limit volume 310
profile charging dynamic-rules request-quota 310
profile charging failure-handling error-type 311
profile charging limit 311
profile charging limit rating-group 312
profile charging mscc-final-unit-action terminate session 312
profile charging offline zero-usage 313
profile charging quota 313
profile charging quota suppress 314
profile charging quota validity-time 314
profile charging quota volume-threshold percent 315
profile charging reporting-level 315
profile charging requested-service-unit 316
profile charging requested-service-unit volume 316
profile charging send charging-initial 316
profile charging session-failover 317
profile charging tariff-time-change 317
profile charging triggers 318
profile charging-characteristics 318
profile charging-characteristics network-element-profile-list 319

profile charging-qbc 319
profile charging-qbc limit 321
profile charging usage-reporting quota-to-report based-on-grant 321
profile compliance 322
profile compliance service 322
profile compliance service n1 323
profile compliance service n2 324
profile compliance service namf-comm 325
profile compliance service nchf-convergedcharging 326
profile compliance service nnrf-disc 327
profile compliance service nnrf-nfm 328
profile compliance service npcf-smpolicycontrol 329
profile compliance service nsmf-pdusession 330
profile compliance service nudm-sdm 331
profile compliance service nudm-uecm 332
profile compliance service threegpp23502 333
profile content-filtering category database 334
profile content-filtering category database directory 334
profile converged-core activated-features 334
profile converged-core session-hold duration 335
profile converged-core supported-features 336
profile diameter-client 336
profile diameter-endpoint 337
profile diameter-host-selection 341
profile dnn 342
profile dnn ipam dhcp 346
profile dnn accounting 347
profile dnn authentication algorithm 347
profile dnn authentication secondary 348
profile dnn authorization 348
profile dnn dnn 349
profile dnn dnn nw-fu-conf 349
profile dnn dnn rmgr-conf 349
profile dnn dns primary 350

profile dnn dns secondary 350
profile dnn ims mark 351
profile dnn ipv6-prefix-delegation 351
profile dnn max-upf-sessions 351
profile dnn network-element-profiles 352
profile dnn nexthop-forwarding-address 353
profile dnn nssai 353
profile dnn outbound 354
profile dnn primary-plmn 354
profile dnn session-hold duration 354
profile dnn session type 355
profile dnn skip-n10-registration 356
profile dnn subscription 356
profile dnn ssc-mode 357
profile dnn timeout 357
profile dnn timeout bearer-inactivity 359
profile dnn timeout bearer-inactivity gbr 359
profile dnn timeout bearer-inactivity gbr volume 359
profile dnn timeout bearer-inactivity non-gbr 360
profile dnn timeout bearer-inactivity non-gbr volume 360
profile dnn upf 361
profile dnn upcp status 361
profile dns-proxy 362
profile dns-proxy servers 363
profile ecgi-group 364
profile ecgi-group ecgis 364
profile ecgi-group ecgis ecgi 364
profile ecgi-group ecgis ecgi range 365
profile emergency-profile 365
profile failure-handling 366
profile failure-handling interface diameter 366
profile failure-handling interface gtpc message 368
profile failure-handling interface gtpc message cause-code-type cause-code 368
profile failure-handling interface gtpc message cause-code-type cause-code action 368

profile failure-handling interface n11 369
profile failure-handling interface n11 message 369
profile failure-handling interface n11 message cause-code-value cause-code 370
profile failure-handling interface n11 message cause-code-value cause-code action 370
profile failure-handling interface pfcp 371
profile failure-handling interface pfcp message 371
profile failure-handling interface pfcp message cause-code-type-est cause-code 372
profile failure-handling interface pfcp message cause-code-type-est cause-code action 373
profile failure-handling interface pfcp message cause-code-type-mod cause-code 373
profile failure-handling interface pfcp message cause-code-type-mod cause-code action 374
profile failure-handling interface pfcp message cause-code-type-sessreport cause-code 375
profile failure-handling interface pfcp message cause-code-type-sessreport cause-code action 375
profile failure-handling interface sxa message 375
profile failure-handling interface sxa message cause-code-type-est cause-code 376
profile failure-handling interface sxa message cause-code-type-est cause-code action 376
profile gtpp-profile gtpp 377
profile icmpv6 379
profile icmpv6 options 379
profile icmpv6 ra trigger 380
profile interface-mapping default interface 381
profile load 381
profile load advertise 382
profile load interface 383
profile location-area-group 383
profile message-handling nf type udm mh-profile 384
profile n3-tunnel 384
profile n3-tunnel buffer 384
profile ncgi-group 385
profile ncgi-group ncgis 385
profile ncgi-group ncgis ncgi 386
profile ncgi-group ncgis ncgi range 386
profile network-element amf 386
profile network-element amf discovery 387
profile network-element amf query-params 388

profile network-element chf 388
profile network-element chf discovery 390
profile network-element chf query-params 390
profile network-element nrf 391
profile network-element pcf 392
profile network-element pcf bitrates 393
profile network-element pcf discovery 394
profile network-element pcf query-params 394
profile network-element scp 395
profile network-element sepp 396
profile network-element sepp discovery 396
profile network-element sepp query-params 397
profile network-element udm 397
profile network-element udm discovery 399
profile network-element udm failure-handling-profile-rat 399
profile network-element udm query-params 400
profile network-element upf 400
profile network-element upf n4-peer-address 402
profile nf-client nf-type amf amf-profile 403
profile nf-client nf-type amf amf-profile locality 403
profile nf-client nf-type amf amf-profile locality service name type 404
profile nf-client nf-type amf amf-profile locality service name type endpoint-profile 404
profile nf-client nf-type amf amf-profile locality service name type endpoint-profile endpoint-name 405
profile nf-client nf-type amf amf-profile locality service name type endpoint-profile endpoint-name primary ip-address 406
profile nf-client nf-type amf amf-profile locality service name type endpoint-profile endpoint-name secondary ip-address 407
profile nf-client nf-type amf amf-profile locality service name type endpoint-profile endpoint-name tertiary ip-address 407
profile nf-client nf-type amf amf-profile locality service name type endpoint-profile version uri-version 408
profile nf-client nf-type ausf ausf-profile 408
profile nf-client nf-type ausf ausf-profile locality 409
profile nf-client nf-type ausf ausf-profile locality service name type 409
profile nf-client nf-type ausf ausf-profile locality service name type endpoint-profile 410

profile nf-client nf-type ausf ausf-profile locality service name type endpoint-profile endpoint-name 411
profile nf-client nf-type ausf ausf-profile locality service name type endpoint-profile endpoint-name primary ip-address 411
profile nf-client nf-type ausf ausf-profile locality service name type endpoint-profile endpoint-name secondary ip-address 412
profile nf-client nf-type ausf ausf-profile locality service name type endpoint-profile endpoint-name tertiary ip-address 413
profile nf-client nf-type ausf ausf-profile locality service name type endpoint-profile version uri-version 413
profile nf-client nf-type chf chf-profile 414
profile nf-client nf-type chf chf-profile locality 414
profile nf-client nf-type chf chf-profile locality service name type 415
profile nf-client nf-type chf chf-profile locality service name type endpoint-profile 415
profile nf-client nf-type chf chf-profile locality service name type endpoint-profile endpoint-name 416
profile nf-client nf-type chf chf-profile locality service name type endpoint-profile endpoint-name primary ip-address 417
profile nf-client nf-type chf chf-profile locality service name type endpoint-profile endpoint-name secondary ip-address 418
profile nf-client nf-type chf chf-profile locality service name type endpoint-profile endpoint-name tertiary ip-address 418
profile nf-client nf-type chf chf-profile locality service name type endpoint-profile version uri-version 419
profile nf-client nf-type eir eir-profile 419
profile nf-client nf-type eir eir-profile locality 420
profile nf-client nf-type eir eir-profile locality service name type 420
profile nf-client nf-type eir eir-profile locality service name type endpoint-profile 421
profile nf-client nf-type eir eir-profile locality service name type endpoint-profile endpoint-name 422
profile nf-client nf-type eir eir-profile locality service name type endpoint-profile endpoint-name primary ip-address 422
profile nf-client nf-type eir eir-profile locality service name type endpoint-profile endpoint-name secondary ip-address 423
profile nf-client nf-type eir eir-profile locality service name type endpoint-profile endpoint-name tertiary ip-address 424
profile nf-client nf-type eir eir-profile locality service name type endpoint-profile version uri-version 424
profile nf-client nf-type endpoint-name fqdn name fqdn port 425
profile nf-client nf-type pcf pcf-profile 425

profile nf-client nf-type pcf pcf-profile locality 426
profile nf-client nf-type pcf pcf-profile locality service name type 426
profile nf-client nf-type pcf pcf-profile locality service name type endpoint-profile 427
profile nf-client nf-type pcf pcf-profile locality service name type endpoint-profile endpoint-name 428
profile nf-client nf-type pcf pcf-profile locality service name type endpoint-profile endpoint-name primary ip-address 428
profile nf-client nf-type pcf pcf-profile locality service name type endpoint-profile endpoint-name secondary ip-address 429
profile nf-client nf-type pcf pcf-profile locality service name type endpoint-profile endpoint-name tertiary ip-address 430
profile nf-client nf-type pcf pcf-profile locality service name type endpoint-profile version uri-version 430
profile nf-client nf-type scp scp-profile 431
profile nf-client nf-type sepp sepp-profile 432
profile nf-client nf-type sepp sepp-profile locality 432
profile nf-client nf-type sepp sepp-profile locality service name type 432
profile nf-client nf-type sepp sepp-profile locality service name type endpoint-profile 433
profile nf-client nf-type sepp sepp-profile locality service name type endpoint-profile endpoint-name 434
profile nf-client nf-type sepp sepp-profile locality service name type endpoint-profile endpoint-name primary ip-address 435
profile nf-client nf-type sepp sepp-profile locality service name type endpoint-profile endpoint-name secondary ip-address 435
profile nf-client nf-type sepp sepp-profile locality service name type endpoint-profile endpoint-name tertiary ip-address 436
profile nf-client nf-type sepp sepp-profile locality service name type endpoint-profile version uri-version 436
profile nf-client nf-type smf smf-profile 437
profile nf-client nf-type smf smf-profile locality 437
profile nf-client nf-type smf smf-profile locality service name type 438
profile nf-client nf-type smf smf-profile locality service name type endpoint-profile 438
profile nf-client nf-type smf smf-profile locality service name type endpoint-profile endpoint-name 439
profile nf-client nf-type smf smf-profile locality service name type endpoint-profile endpoint-name primary ip-address 440
profile nf-client nf-type smf smf-profile locality service name type endpoint-profile endpoint-name secondary ip-address 441

profile nf-client nf-type smf smf-profile locality service name type endpoint-profile endpoint-name tertiary ip-address 441

profile nf-client nf-type smf smf-profile locality service name type endpoint-profile version uri-version 442

profile nf-client nf-type udm udm-profile 442

profile nf-client nf-type udm udm-profile locality 443

profile nf-client nf-type udm udm-profile locality service name type 443

profile nf-client nf-type udm udm-profile locality service name type endpoint-profile 444

profile nf-client nf-type udm udm-profile locality service name type endpoint-profile endpoint-name 445

profile nf-client nf-type udm udm-profile locality service name type endpoint-profile endpoint-name primary ip-address 445

profile nf-client nf-type udm udm-profile locality service name type endpoint-profile endpoint-name secondary ip-address 446

profile nf-client nf-type udm udm-profile locality service name type endpoint-profile endpoint-name tertiary ip-address 447

profile nf-client nf-type udm udm-profile locality service name type endpoint-profile version uri-version 447

profile nf-client-failure nf-type amf 448

profile nf-client-failure nf-type amf profile failure-handling 448

profile nf-client-failure nf-type amf profile failure-handling service name type 448

profile nf-client-failure nf-type amf profile failure-handling service name type message type 449

profile nf-client-failure nf-type amf profile failure-handling service name type message type status-code httpv2 450

profile nf-client-failure nf-type ausf 451

profile nf-client-failure nf-type ausf profile failure-handling 451

profile nf-client-failure nf-type ausf profile failure-handling service name type 451

profile nf-client-failure nf-type ausf profile failure-handling service name type message type 452

profile nf-client-failure nf-type ausf profile failure-handling service name type message type status-code httpv2 452

profile nf-client-failure nf-type chf 453

profile nf-client-failure nf-type chf profile failure-handling 454

profile nf-client-failure nf-type chf profile failure-handling service name type 454

profile nf-client-failure nf-type chf profile failure-handling service name type message type 455

profile nf-client-failure nf-type chf profile failure-handling service name type message type status-code httpv2 455

profile nf-client-failure nf-type eir 456

profile nf-client-failure nf-type eir profile failure-handling 456
profile nf-client-failure nf-type eir profile failure-handling service name type 457
profile nf-client-failure nf-type eir profile failure-handling service name type message type 457
profile nf-client-failure nf-type eir profile failure-handling service name type message type status-code httpv2 458
profile nf-client-failure nf-type nrf 459
profile nf-client-failure nf-type nrf profile failure-handling 459
profile nf-client-failure nf-type nrf profile failure-handling service name type 459
profile nf-client-failure nf-type nrf profile failure-handling service name type message type 460
profile nf-client-failure nf-type nrf profile failure-handling service name type message type status-code httpv2 461
profile nf-client-failure nf-type pcf 461
profile nf-client-failure nf-type pcf profile failure-handling 462
profile nf-client-failure nf-type pcf profile failure-handling service name type 462
profile nf-client-failure nf-type pcf profile failure-handling service name type message type 463
profile nf-client-failure nf-type pcf profile failure-handling service name type message type status-code httpv2 463
profile nf-client-failure nf-type scp 464
profile nf-client-failure nf-type sepp 465
profile nf-client-failure nf-type sepp profile failure-handling 465
profile nf-client-failure nf-type sepp profile failure-handling service name type 466
profile nf-client-failure nf-type sepp profile failure-handling service name type message type 466
profile nf-client-failure nf-type sepp profile failure-handling service name type message type status-code httpv2 467
profile nf-client-failure nf-type smf 468
profile nf-client-failure nf-type smf profile failure-handling 468
profile nf-client-failure nf-type smf profile failure-handling service name type 468
profile nf-client-failure nf-type smf profile failure-handling service name type message type status-code httpv2 469
profile nf-client-failure nf-type udm 470
profile nf-client-failure nf-type udm profile failure-handling 470
profile nf-client-failure nf-type udm profile failure-handling service name type 471
profile nf-client-failure nf-type udm profile failure-handling service name type message type 471
profile nf-client-failure nf-type udm profile failure-handling service name type message type status-code httpv2 472

profile nf-pair nf-type 473
profile nf-pair nf-type cache invalidation true 474
profile nf-pair nf-type locality 475
profile overload 475
profile overload node-level 476
profile overload node-level advertise 476
profile overload node-level interface 477
profile overload node-level reduction-metric 477
profile overload node-level tolerance 478
profile overload overload-exclude-profile 478
profile overload peer-level interface 479
profile overload peer-level interface action throttle 479
profile overload peer-level message-prioritization 480
profile overload-exclude 480
profile overload-exclude message-priority 481
profile overload-exclude procedure-list 482
profile pcscf 482
profile pcscf fqdn 483
profile pcscf pcscf-selection 483
profile pcscf pcscf-restoration trigger 483
profile pcscf v4-list 484
profile pcscf v4-list list-entry 484
profile pcscf v4-list list-entry primary 484
profile pcscf v4-list list-entry secondary 485
profile pcscf v4-list list-entry tertiary 485
profile pcscf v4v6-list 486
profile pcscf v4v6-list list-entry 486
profile pcscf v4v6-list list-entry primary 486
profile pcscf v4v6-list list-entry secondary 487
profile pcscf v4v6-list list-entry tertiary 488
profile pcscf v6-list 488
profile pcscf v6-list list-entry 489
profile pcscf v6-list list-entry primary 489
profile pcscf v6-list list-entry secondary 489

profile pcscf v6-list list-entry tertiary 490
profile ppd 490
profile ppd dscp-list 491
profile qos 491
profile qos ambr 492
profile qos arp 493
profile qos dscp-map qi5 493
profile qos dscp-map qi5 arp-priority-level 494
profile qos dscp-map qi5 arp-priority-level dscp-info 494
profile qos dscp-map qi5 arp-priority-level dscp-info user-datagram 495
profile qos dscp-map qi5 dscp-info 496
profile qos dscp-map qi5 dscp-info user-datagram 497
profile qos max 497
profile qos qos-enforcement 498
profile qos qosflow qi5 498
profile qos qosflow qi5 arp-priority-level 498
profile qos qosflow qi5 arp-priority-level dscp-info downlink encaps-header 499
profile qos qosflow qi5 arp-priority-level dscp-info downlink user-datagram 499
profile qos qosflow qi5 arp-priority-level dscp-info uplink encaps-header 500
profile qos qosflow qi5 arp-priority-level dscp-info uplink user-datagram 501
profile qos qosflow qi5 arp-priority-level flow-parameter gfbr 501
profile qos qosflow qi5 arp-priority-level flow-parameter mfbr 502
profile qos qosflow qi5 dscp-info downlink encaps-header 502
profile qos qosflow qi5 dscp-info downlink user-datagram 503
profile qos qosflow qi5 dscp-info uplink encaps-header 504
profile qos qosflow qi5 dscp-info uplink user-datagram 504
profile qos qosflow qi5 flow-parameter gfbr 505
profile qos qosflow qi5 flow-parameter mfbr 505
profile radius 506
profile radius accounting 507
profile radius accounting attribute 507
profile radius accounting attribute instance 508
profile radius accounting detect-dead-server 509
profile radius allow auth 509

radius profile server group allow auth 510
profile radius attribute 510
profile radius attribute instance 511
profile radius consecutive failure dead server detection 511
profile radius detect-dead-server 512
profile radius dictionary 512
profile radius max transmissions 513
profile radius server 513
profile radius server-group 514
profile radius server-group accounting 515
profile radius server-group accounting attribute 515
profile radius server-group accounting attribute instance 516
profile radius server-group attribute 517
profile radius server-group attribute instance 517
profile radius server-group server 518
profile radius server group max transmissions 519
profile radius-dynamic-author 519
profile radius-dynamic-author client 520
profile sgw-qos-profile 520
profile sgw-qos-profile dscp-map operator-defined-qci 521
profile sgw-qos-profile dscp-map operator-defined-qci gbr arp-priority-level 521
profile sgw-qos-profile dscp-map operator-defined-qci gbr arp-priority-level dscp-info 521
profile sgw-qos-profile dscp-map operator-defined-qci gbr dscp-info 527
profile sgw-qos-profile dscp-map operator-defined-qci non-gbr 532
profile sgw-qos-profile dscp-map operator-defined-qci non-gbr arp-priority-level 533
profile sgw-qos-profile dscp-map operator-defined-qci non-gbr arp-priority-level dscp-info 533
profile sgw-qos-profile dscp-map operator-defined-qci non-gbr dscp-info 538
profile sgw-qos-profile dscp-map qci 544
profile sgw-qos-profile dscp-map qci arp-priority-level 544
profile sgw-qos-profile dscp-map qci arp-priority-level dscp-info 544
profile sgw-qos-profile dscp-map qci default 550
profile sgw-qos-profile dscp-map qci default dscp-info 550
profile sgw-qos-profile dscp-map qci gbr dscp-info 556
profile sgw-qos-profile dscp-map qci non-gbr dscp-info 561

profile smf 567
profile smf instances 568
profile smf instances deactivate-features 569
profile smf plmn-id 570
profile smf plmn-list 570
profile smf service 571
profile smf service http-endpoint 572
profile tai-group 573
profile tai-group tais 573
profile tai-group tais tac 574
profile tai-group tais tac range 574
profile upf-group 574
profile upf-group failure-profile 576
profile upf-group heartbeat 576
profile wps 576
profile wps dscp 577
service name type 579
radius 580
radius acct-server 580
radius auth-server 580
radius-dyn-auth 580
radius-dyn-auth clients 580
rcm switchover 581
reconcile ipam 581
resource pod 581
resource pod cpu 582
resource pod labels 582
resource pod memory 582
resources info 583
router bgplist 583
router bgplist bfd 584
router bgplist interfaceList 584
router bgplist interfaceList bondingInterfaces 585
router bgplist interfaceList neighbors 585

router bgplist policies 586
rpc all 587
running-status info 587
screen-length 588
screen-width 588
send 588
sessions affinity 589
sessions commit-pending 589
quit 589
show 590
show bfd-neighbor 590
show bgp-advertised-routes 590
show bgp-global 591
show bgp-kernel-route 591
show bgp-learned-routes 591
show bgp-neighbors 592
show bgp-route-summary 592
show bgp-routes 592
show diameter routes all 593
show edr 593
show geo-maintenance-mode 593
show georeplication-status 594
show georeplication 594
show idmgr-debug 594
show ipam dp 594
show ipam dp name 595
show ipam dp name ipv4-addr 595
show ipam dp name ipv6-addr 595
show ipam dp name ipv6-prefix 595
show ipam dp tag 596
show ipam dp tag tag-name 596
show ipam dp tag ipv4-addr 596
show ipam dp tag ipv6-addr 597
show ipam dp tag ipv6-prefix 597

show ipam pool 597
show ipam pool name 597
show ipam pool name ipv4-addr 598
show ipam pool name ipv6-addr 598
show ipam pool name ipv6-prefix 598
show ipam-staticdb 598
show peers 599
show role 599
show subscriber 599
show subscriber count-opt 604
show subscriber debug-opt 607
show subscriber gpsi-opt policy-opt 608
show subscriber imsi-opt 609
show subscriber msid-opt policy-opt 609
show subscriber msisdn-opt policy-opt 610
show subscriber pei-opt policy-opt 610
show subscriber supi-opt 610
show subscriber supi-opt policy-opt 611
show userplane userplane 611
show vrf-info 612
show vrf-route-info 612
show-defaults 613
show confd-state 613
show dns-cache 613
show dns-query 614
show gtpp-ep 614
show helm 614
show history 615
show jobs 615
show last-logins 615
show license 615
show local-interface-status 616
show mode 616
show nacm 616

show netconf-state 617
show nf-tls 617
show notification 617
show nrf 618
show ops 618
show overload-info 618
show parser 619
show pcscf 619
show resources 619
show restconf-state 620
show running-config 620
smiuser 620
system 622
system-diagnostics event-trace 622
system-diagnostics idmgr-secondary-recon 623
system-diagnostics ip-validation 623
system-diagnostics pod type 623
system-diagnostics pod type fault 624
system-diagnostics protocol supi 625
system-diagnostics protocol supi preferred-up 625
system-diagnostics session-consistency 625
terminal 626
test dns-query 626
test gtpc echo 627
test gtpp echo 627
test-radius accounting 628
test-radius authentication 629
timestamp 630
who 631

CHAPTER 2 **Input Pattern Types** 633

arg-type 633
crypt-hash 634
date-and-time 635

domain-name 635
dotted-quad 636
hex-list 636
hex-string 637
ipv4-address 637
ipv4-address-and-prefix-length 637
ipv4-address-no-zone 637
ipv4-prefix 637
ipv6-address 638
ipv6-address-and-prefix-length 638
ipv6-address-no-zone 639
ipv6-prefix 639
mac-address 640
object-identifier 640
object-identifier-128 640
octet-list 641
phys-address 641
sha-256-digest-string 641
sha-512-digest-string 642
size 642
uuid 643
yang-identifier 643



About this Guide

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

This preface describes the *5G Session Management Function Guide*, how it is organized and its document conventions.

This guide describes the Cisco Session Management Function (SMF) and includes infrastructure and interfaces, feature descriptions, specification compliance, session flows, configuration instructions, and CLI commands for monitoring and troubleshooting the system.

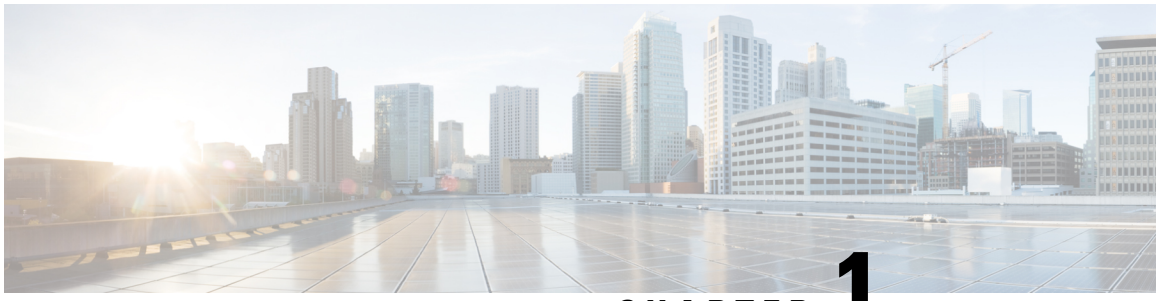
• Conventions Used, on page xxxv

Conventions Used

The following tables describe the conventions used throughout this documentation.

Notice Type	Description
Information Note	Provides information about important features or instructions.
Caution	Alerts you of potential damage to a program, device, or system.
Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.

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



CHAPTER 1

Configuration Command Reference

- aaa, on page 23
- active-charging service, on page 24
- active-charging service bandwidth-policy, on page 24
- active-charging service bandwidth-policy flow limit-for-bandwidth id, on page 25
- active-charging service bandwidth-policy group-id, on page 25
- active-charging service bandwidth-policy group-id direction downlink grpPeakBwp, on page 26
- active-charging service bandwidth-policy group-id direction uplink grpPeakBwp, on page 27
- active-charging service buffering-limit, on page 29
- active-charging service charging-action, on page 29
- active-charging service charging-action allocation-retention-priority, on page 30
- active-charging service charging-action billing-action, on page 31
- active-charging service charging-action cca charging credit, on page 32
- active-charging service charging-action flow action, on page 32
- active-charging service charging-action flow action discard, on page 33
- active-charging service charging-action flow action readdress, on page 33
- active-charging service charging-action flow limit-for-bandwidth, on page 34
- active-charging service charging-action flow limit-for-bandwidth direction downlink peak-data-rate, on page 34
- active-charging service charging-action flow limit-for-bandwidth direction uplink peak-data-rate, on page 35
- active-charging service charging-action tft packet-filter, on page 37
- active-charging service charging-action tos af11, on page 37
- active-charging service charging-action tos af12, on page 38
- active-charging service charging-action tos af13, on page 38
- active-charging service charging-action tos af21, on page 38
- active-charging service charging-action tos af22, on page 39
- active-charging service charging-action tos af23, on page 39
- active-charging service charging-action tos af31, on page 40
- active-charging service charging-action tos af32, on page 40
- active-charging service charging-action tos af33, on page 40
- active-charging service charging-action tos af41, on page 41
- active-charging service charging-action tos af42, on page 41
- active-charging service charging-action tos af43, on page 42
- active-charging service charging-action tos be, on page 42

- active-charging service charging-action tos ef, on page 42
- active-charging service charging-action tos lower-bits, on page 43
- active-charging service content-filtering category policy-id, on page 43
- active-charging service content-filtering category policy-id analyze priority, on page 44
- active-charging service content-filtering category policy-id analyze priority all, on page 44
- active-charging service content-filtering category policy-id analyze priority category, on page 45
- active-charging service content-filtering category policy-id analyze priority x-category, on page 47
- active-charging service credit-control group, on page 48
- active-charging service credit-control group associate, on page 48
- active-charging service credit-control group diameter, on page 49
- active-charging service credit-control group diameter origin, on page 49
- active-charging service credit-control group diameter service-context-id, on page 50
- active-charging service credit-control group diameter session, on page 50
- active-charging service credit-control group failure-handling initial-request continue, on page 50
- active-charging service credit-control group failure-handling initial-request retry-and-terminate, on page 51
- active-charging service credit-control group failure-handling initial-request terminate, on page 51
- active-charging service credit-control group failure-handling terminate-request continue, on page 52
- active-charging service credit-control group failure-handling terminate-request retry-and-terminate, on page 52
- active-charging service credit-control group failure-handling terminate-request terminate, on page 53
- active-charging service credit-control group failure-handling update-request continue, on page 53
- active-charging service credit-control group failure-handling update-request retry-and-terminate, on page 54
- active-charging service credit-control group failure-handling update-request terminate, on page 54
- active-charging service credit-control group pending-traffic-treatment forced-reauth, on page 55
- active-charging service credit-control group pending-traffic-treatment noquota, on page 55
- active-charging service credit-control group pending-traffic-treatment noquota limited-pass, on page 56
- active-charging service credit-control group pending-traffic-treatment quota-exhausted, on page 56
- active-charging service credit-control group pending-traffic-treatment trigger, on page 57
- active-charging service credit-control group pending-traffic-treatment validity-expired, on page 57
- active-charging service credit-control group quota holding-time, on page 58
- active-charging service credit-control group quota request-trigger, on page 58
- active-charging service credit-control group timestamp-rounding, on page 58
- active-charging service credit-control group usage-reporting quotas-to-report based-on-grant, on page 59
- active-charging service group-of-ruledefs, on page 59
- active-charging service group-of-ruledefs add-ruledef priority, on page 60
- active-charging service p2p-detection attribute ssl-renegotiation, on page 60
- active-charging service p2p-detection ecs-analysis, on page 61
- active-charging service p2p-detection protocol, on page 62
- active-charging service packet-filter, on page 62
- active-charging service packet-filter ip local-port operator, on page 63
- active-charging service packet-filter ip local-port range, on page 64
- active-charging service packet-filter ip protocol, on page 64
- active-charging service packet-filter ip remote-address, on page 65

- active-charging service packet-filter ip remote-port operator, on page 66
- active-charging service packet-filter ip remote-port range, on page 66
- active-charging service packet-filter ip tos-traffic-class, on page 67
- active-charging service rulebase, on page 67
- active-charging service rulebase action, on page 68
- active-charging service rulebase action priority, on page 69
- active-charging service rulebase action priority dynamic-only, on page 69
- active-charging service rulebase action priority dynamic-only adc group-of-ruledefs, on page 69
- active-charging service rulebase action priority dynamic-only adc ruledef, on page 70
- active-charging service rulebase action priority dynamic-only group-of-ruledefs, on page 71
- active-charging service rulebase action priority dynamic-only ruledef, on page 72
- active-charging service rulebase action priority group-of-ruledefs, on page 73
- active-charging service rulebase action priority ruledef, on page 74
- active-charging service rulebase action priority static-and-dynamic group-of-ruledefs, on page 74
- active-charging service rulebase action priority static-and-dynamic ruledef, on page 75
- active-charging service rulebase action priority timedef group-of-ruledefs, on page 76
- active-charging service rulebase action priority timedef ruledef, on page 77
- active-charging service rulebase bandwidth, on page 78
- active-charging service rulebase billing-records, on page 78
- active-charging service rulebase billing-records udr, on page 79
- active-charging service rulebase cca diameter requested-service-unit sub-avp time, on page 79
- active-charging service rulebase cca diameter requested-service-unit sub-avp units, on page 80
- active-charging service rulebase cca diameter requested-service-unit sub-avp volume, on page 80
- active-charging service rulebase cca quota holding-time, on page 81
- active-charging service rulebase cca quota retry-time, on page 81
- active-charging service rulebase cca quota time-duration, on page 82
- active-charging service rulebase content-filtering category, on page 83
- active-charging service rulebase content-filtering flow-any-error, on page 83
- active-charging service rulebase content-filtering mode, on page 84
- active-charging service rulebase credit-control-group, on page 84
- active-charging service rulebase dynamic-rule, on page 85
- active-charging service rulebase edr transaction-complete, on page 86
- active-charging service rulebase egcdr threshold, on page 86
- active-charging service rulebase egcdr threshold volume, on page 87
- active-charging service rulebase flow control-handshaking, on page 88
- active-charging service rulebase flow control-handshaking charge-to-application, on page 88
- active-charging service rulebase flow end-condition, on page 89
- active-charging service rulebase flow limit-across-applications, on page 89
- active-charging service rulebase ip, on page 90
- active-charging service rulebase p2p, on page 90
- active-charging service rulebase post-processing priority, on page 91
- active-charging service rulebase post-processing priority group-of-ruledefs, on page 91
- active-charging service rulebase post-processing priority ruledef, on page 92
- active-charging service rulebase route priority, on page 92
- active-charging service rulebase route priority ruledef, on page 93
- active-charging service rulebase rtp, on page 94

- active-charging service rulebase tcp, on page 94
- active-charging service rulebase tcp mss, on page 95
- active-charging service rulebase tcp packets-out-of-order, on page 95
- active-charging service rulebase tcp packets-out-of-order transmit, on page 96
- active-charging service rulebase tethering-detection, on page 97
- active-charging service rulebase url-blacklisting action, on page 98
- active-charging service rulebase url-blacklisting match-method, on page 98
- active-charging service ruledef, on page 99
- active-charging service ruledef bearer service-3gpp rat-type, on page 100
- active-charging service ruledef dns answer-name, on page 100
- active-charging service ruledef dns any-match, on page 101
- active-charging service ruledef dns previous-state, on page 102
- active-charging service ruledef dns query-name, on page 103
- active-charging service ruledef dns query-type, on page 104
- active-charging service ruledef dns return-code, on page 105
- active-charging service ruledef dns state, on page 106
- active-charging service ruledef dns tid, on page 106
- active-charging service ruledef http content type, on page 107
- active-charging service ruledef http host, on page 108
- active-charging service ruledef http referer, on page 109
- active-charging service ruledef http url, on page 110
- active-charging service ruledef http user-agent, on page 111
- active-charging service ruledef icmpv6 any-match, on page 111
- active-charging service ruledef ip any-match, on page 112
- active-charging service ruledef ip dst-address, on page 113
- active-charging service ruledef ip protocol, on page 115
- active-charging service ruledef ip server-ip-addr, on page 115
- active-charging service ruledef ip uplink, on page 117
- active-charging service ruledef ip version, on page 117
- active-charging service ruledef multi-line-or, on page 118
- active-charging service ruledef p2p, on page 118
- active-charging service ruledef p2p app-identifier, on page 119
- active-charging service ruledef p2p protocol, on page 120
- active-charging service ruledef p2p traffic-type, on page 129
- active-charging service ruledef rtp any-match, on page 130
- active-charging service ruledef rtsp any-match, on page 131
- active-charging service ruledef secure-http any-match, on page 132
- active-charging service ruledef secure-http uplink, on page 133
- active-charging service ruledef tcp any-match, on page 134
- active-charging service ruledef tcp either-port with-portMap-range, on page 135
- active-charging service ruledef tcp either-port with-range, on page 135
- active-charging service ruledef tcp either-port without-range, on page 136
- active-charging service ruledef tcp flag, on page 137
- active-charging service ruledef tcp state, on page 138
- active-charging service ruledef tethering-detection, on page 139
- active-charging service ruledef tethering-detection application, on page 139

- active-charging service ruledef tethering-detection dns-based, on page 140
- active-charging service ruledef tethering-detection ip-ttl, on page 140
- active-charging service ruledef tethering-detection os-ua, on page 140
- active-charging service ruledef udp any-match, on page 141
- active-charging service ruledef udp either-port with-portMap-range, on page 142
- active-charging service ruledef udp either-port with-range, on page 142
- active-charging service ruledef udp either-port without-range, on page 143
- active-charging service ruledef wsp any-match, on page 144
- active-charging service ruledef wtp any-match, on page 145
- active-charging service ruledef www any-match, on page 146
- active-charging service ruledef www host, on page 147
- active-charging service ruledef www url, on page 148
- active-charging service url-blacklisting, on page 148
- active-charging service urr-list, on page 149
- active-charging service urr-list urr-list-data, on page 149
- active-charging service urr-list urr-list-data service-identifier, on page 150
- apn, on page 150
- apn active-charging, on page 151
- apn authorize-with-hss, on page 151
- apn authorize-with-hss egtp, on page 151
- apn authorize-with-hss egtp gn-gp-enabled, on page 152
- apn authorize-with-hss egtp s2b, on page 152
- apn authorize-with-hss egtp s2b gn-gp-enabled, on page 152
- apn authorize-with-hss egtp s2b s5-s8, on page 152
- apn authorize-with-hss egtp s5-s8, on page 153
- apn authorize-with-hss egtp s5-s8 s2b, on page 153
- apn authorize-with-hss lma, on page 154
- apn cc-profile, on page 154
- apn content-filtering category, on page 155
- apn data-tunnel, on page 155
- apn gtpp group, on page 155
- apn ip access-group, on page 156
- apn ip source-violation, on page 156
- apn ppp, on page 157
- apn timeout, on page 157
- cd, on page 157
- cdl clear, on page 158
- cdl show sessions, on page 158
- cdl show status, on page 159
- clear diameter routes dynamic, on page 160
- clear ipam, on page 160
- clear ipam, on page 160
- clear lawful-intercept stats, on page 161
- clear subscriber, on page 161
- clear subscriber imsi-opt, on page 163
- clear subscriber supi-opt, on page 164

- client http header, on page 165
- client http ping, on page 165
- client inbound interface, on page 166
- client inbound interface limit overload, on page 166
- client inbound interface limit pending, on page 166
- client inbound limit overload, on page 167
- client inbound limit pending, on page 167
- client outbound host ping, on page 167
- client outbound interface, on page 168
- client outbound interface host ping, on page 168
- client outbound interface limit consecutive failure, on page 169
- client outbound interface limit pending, on page 170
- client outbound limit consecutive failure, on page 170
- client outbound limit pending, on page 171
- commit, on page 171
- compare, on page 172
- config, on page 172
- config-error info, on page 173
- datastore dbs, on page 173
- datastore dbs endpoints, on page 173
- datastore notification-ep, on page 174
- datastore session-db, on page 174
- datastore session-db endpoints, on page 174
- deployment, on page 175
- deployment resource, on page 176
- describe, on page 176
- diagnostics info, on page 177
- dump, on page 178
- dump core, on page 178
- dump transactionhistory, on page 179
- edr, on page 179
- edr file files, on page 180
- edr file files disable, on page 181
- edr file files flush, on page 181
- edr file files limit, on page 181
- edr file files procedure-id disable-event-id, on page 182
- edr file files procedure-id disable-event-id disable-inner disable, on page 182
- edr file files procedure-id disable-event-id disable-inner event-id disable-field-id, on page 182
- edr file files procedure-id disable-event-id disable-inner event-id disable-field-id disable, on page 183
- edr file transaction field priorityClass, on page 183
- endpoint all, on page 184
- endpoint info, on page 184
- exit, on page 185
- geo maintenance, on page 185
- geo replication-pull , on page 186
- geo reset-role, on page 186

- geo switch-role, on page 186
- geomonitor podmonitor pods, on page 187
- geomonitor remoteclustermonitor, on page 188
- geomonitor trafficMonitor, on page 188
- geomonitor vipmonitor instance, on page 189
- geomonitor vipmonitor instance vips, on page 189
- group nf-mgmt, on page 190
- group nf-mgmt heartbeat, on page 191
- group nrf discovery, on page 191
- group nrf discovery service type nrf, on page 191
- group nrf discovery service type nrf endpoint-profile, on page 192
- group nrf discovery service type nrf endpoint-profile endpoint-name, on page 193
- group nrf discovery service type nrf endpoint-profile endpoint-name primary ip-address, on page 193
- group nrf discovery service type nrf endpoint-profile endpoint-name secondary ip-address, on page 194
- group nrf discovery service type nrf endpoint-profile endpoint-name tertiary ip-address, on page 195
- group nrf discovery service type nrf endpoint-profile version uri-version, on page 195
- group nrf mgmt, on page 196
- group nrf mgmt service type nrf, on page 196
- group nrf mgmt service type nrf endpoint-profile, on page 197
- group nrf mgmt service type nrf endpoint-profile endpoint-name, on page 197
- group nrf mgmt service type nrf endpoint-profile endpoint-name primary ip-address, on page 198
- group nrf mgmt service type nrf endpoint-profile endpoint-name secondary ip-address, on page 199
- group nrf mgmt service type nrf endpoint-profile endpoint-name tertiary ip-address, on page 199
- group nrf mgmt service type nrf endpoint-profile version uri-version, on page 200
- gtpp group, on page 200
- gtpp group gtpp egcdr final-record closing-cause, on page 201
- gtpp group gtpp egcdr losdv-max-containers, on page 201
- gtpp group gtpp egcdr service-data-flow threshold, on page 201
- gtpp group gtpp egcdr service-data-flow threshold volume, on page 202
- gtpp group gtpp egcdr service-idle-timeout, on page 202
- gtpp group gtpp trigger, on page 203
- gtpp group gtpp trigger egcdr, on page 203
- help, on page 203
- history, on page 205
- id, on page 205
- idle-timeout, on page 205
- ignore-leading-space, on page 206
- infra metrics experimental, on page 206
- infra metrics verbose verboseLevels, on page 206
- infra metrics verbose verboseLevels metrics metricsList, on page 207
- infra transaction limit, on page 208
- infra transaction limit consecutive same, on page 208
- infra transaction loop, on page 209
- infra transaction loop category, on page 209
- infra transaction loop category threshold, on page 209
- infra transaction loop category threshold thresholds, on page 210

- instance instance-id, on page 210
- instance instance-id endpoint ep, on page 212
- instance instance-id endpoint diameter, on page 214
- instance instance-id endpoint ep cpu, on page 215
- instance instance-id endpoint ep extended-service, on page 215
- instance instance-id endpoint ep heartbeat, on page 216
- instance instance-id endpoint gtpprime, on page 216
- instance instance-id endpoint ep interface, on page 217
- instance instance-id endpoint ep interface dispatcher, on page 218
- instance instance-id endpoint ep interface echo, on page 220
- instance instance-id endpoint ep interface heartbeat, on page 220
- instance instance-id endpoint ep interface internal base-port, on page 221
- instance instance-id endpoint ep interface overload-control client threshold critical, on page 221
- instance instance-id endpoint ep interface overload-control client threshold high, on page 223
- instance instance-id endpoint ep interface overload-control client threshold low, on page 224
- instance instance-id endpoint ep interface overload-control endpoint threshold critical, on page 225
- instance instance-id endpoint ep interface overload-control endpoint threshold high, on page 226
- instance instance-id endpoint ep interface overload-control endpoint threshold low, on page 227
- instance instance-id endpoint ep interface overload-control msg-type messageConfigs, on page 228
- instance instance-id endpoint ep interface path-failure, on page 230
- instance instance-id endpoint ep interface retransmission, on page 230
- instance instance-id endpoint ep interface secondary-ip, on page 230
- instance instance-id endpoint ep interface sla, on page 231
- instance instance-id endpoint ep interface supported-features, on page 231
- instance instance-id endpoint ep interface sx-path-failure, on page 232
- instance instance-id endpoint ep interface vip, on page 232
- instance instance-id endpoint ep interface vip6, on page 233
- instance instance-id endpoint ep internal base-port, on page 233
- instance instance-id endpoint ep labels pod-config, on page 233
- instance instance-id endpoint ep memory, on page 234
- instance instance-id endpoint ep path-failure, on page 234
- instance instance-id endpoint ep retransmission, on page 235
- instance instance-id endpoint ep secondary-ip, on page 235
- instance instance-id endpoint ep sla, on page 236
- instance instance-id endpoint ep sx-path-failure, on page 236
- instance instance-id endpoint ep system-health-level crash, on page 236
- instance instance-id endpoint ep system-health-level critical, on page 237
- instance instance-id endpoint ep system-health-level warn, on page 238
- instance instance-id endpoint ep vip, on page 238
- instance instance-id endpoint ep vip6, on page 239
- instance instance-id endpoint fqdn, on page 239
- instance instance-id endpoint gtp interface interface-name, on page 240
- instance instance-id endpoint pfcp interface n4 reactivate-peer condition, on page 240
- instance instance-id endpoint radius, on page 241
- instances instance, on page 242
- instance instance-id interface fqdn, on page 242

- instance instance-id smf-fqdn, on page 243
- ipam, on page 243
- exec-ipam reclaim-chunk, on page 243
- ipam dp, on page 244
- ipam instance, on page 244
- ipam instance address-pool, on page 245
- ipam instance address-pool ipv4, on page 246
- ipam instance address-pool ipv4 address-range, on page 246
- ipam instance address-pool ipv4 chunk-group, on page 247
- ipam instance address-pool ipv4 prefix-range, on page 247
- ipam instance address-pool ipv4 split-size, on page 248
- ipam instance address-pool ipv4 threshold, on page 248
- ipam instance address-pool ipv4 vlan, on page 249
- ipam instance address-pool ipv6, on page 249
- ipam instance address-pool ipv6 address-ranges address-range, on page 249
- ipam instance address-pool ipv6 address-ranges prefix-range, on page 250
- ipam instance address-pool ipv6 prefix-ranges prefix-length, on page 251
- ipam instance address-pool ipv6 address-ranges chunk-group, on page 251
- ipam instance address-pool ipv6 address-ranges split-size, on page 251
- ipam instance address-pool ipv6 address-ranges threshold, on page 252
- ipam instance address-pool ipv6 vlan, on page 253
- ipam instance address-pool ipv6 prefix-ranges prefix-range, on page 253
- ipam instance address-pool ipv6 prefix-ranges chunk-group, on page 253
- ipam instance address-pool ipv6 prefix-ranges split-size, on page 254
- ipam instance address-pool ipv6 prefix-ranges threshold, on page 255
- ipam instance address-pool tags, on page 255
- ipam instance audit chunk, on page 256
- ipam instance chunk throttling, on page 256
- ipam instance chunk-reclamation, on page 256
- ipam instance data-sharding, on page 257
- ipam instance min-dp-addr-size, on page 258
- ipam instance source, on page 258
- ipam instance source external ipam, on page 259
- ipam instance threshold, on page 259
- ipam pool, on page 260
- ipam pool ipv4-addr, on page 260
- ipam pool ipv6-addr, on page 260
- job, on page 261
- k8 ccg, on page 261
- k8 ccg coverage, on page 261
- k8 label pod-group-config, on page 262
- leaf-prompting, on page 262
- license smart deregister, on page 263
- license smart register, on page 263
- license smart renew, on page 264
- local-instance, on page 264

- load factor, on page 264
- logging async application enable, on page 265
- logging async monitor-subscriber enable, on page 265
- logging async tracing enable, on page 266
- logging async transaction enable, on page 266
- logging error, on page 266
- logging json-logging, on page 267
- logging level, on page 267
- logging logger, on page 269
- logging logger level, on page 269
- logging transaction, on page 271
- logout, on page 272
- message type, on page 272
- mode debug exec action release-resource, on page 273
- monitor protocol, on page 274
- monitor active-instance-traffic, on page 275
- monitor-protocol cpu-limit, on page 276
- monitor subscriber, on page 276
- msid-opt, on page 277
- nf-tls ca-certificates, on page 278
- nf-tls certificate-status, on page 278
- nf-tls certificates, on page 279
- no, on page 280
- nodemonitor, on page 280
- nrf discovery-info discovery-filter, on page 280
- nrf discovery-info discovery-filter nf-discovery-profile, on page 281
- nrf discovery-info discovery-filter nf-discovery-profile nf-service, on page 281
- nrf registration-info, on page 281
- nrf subscription-info, on page 281
- nssai, on page 282
- paginate, on page 282
- pcscf mark-online, on page 283
- peers all, on page 283
- policy, on page 283
- policy actionmgmt, on page 284
- policy call-control-profile, on page 285
- policy call-control-profile cc, on page 286
- policy call-control-profile cc local-value, on page 286
- policy dnn, on page 287
- policy dnn dnn dnn, on page 287
- policy dnn dnn network-identifier, on page 288
- policy dnn dnn network-identifier operator-identifier, on page 288
- policy dnn dnn operator-identifier, on page 288
- policy eventmgmt, on page 289
- policy network-capability, on page 290
- policy operator, on page 291

- policy operator policy, on page 291
- policy path-failure-detection, on page 292
- policy path-failure-detection ignore, on page 292
- policy rulemgmt, on page 293
- policy subscriber, on page 293
- policy subscriber list-entry, on page 294
- policy subscriber list-entry imsi, on page 295
- policy subscriber list-entry imsi msin, on page 296
- policy subscriber list-entry serving-plmn, on page 296
- policy sx-path-failure-detection, on page 297
- policy sx-path-failure-detection ignore, on page 297
- policy upf-selection, on page 298
- policy upf-selection list-entry, on page 298
- policy upf-selection list-entry query-params, on page 298
- profile access, on page 299
- profile access eps-fallback cbr, on page 299
- profile access eps-fallback guard, on page 300
- profile access eps-fallback trigger-cause group, on page 300
- profile access erir, on page 301
- profile access gtpc, on page 301
- profile access gtpc message-handling create-session-request ho-ind, on page 302
- profile access gtpc message-handling create-session-response action, on page 302
- profile access gtpc message-handling create-session-response condition, on page 303
- profile access n1 message-handling pdu-establishment condition, on page 303
- profile access n1 message-handling pdu-release condition, on page 304
- profile access n1 t3591-pdu-mod-cmd, on page 304
- profile access n1 t3592-pdu-rel-cmd, on page 305
- profile access n1, on page 305
- profile access n2, on page 306
- profile access n11, on page 306
- profile access n2 idft, on page 307
- profile access n26 idft, on page 307
- profile charging, on page 307
- profile charging accounting limit, on page 309
- profile charging accounting limit volume, on page 310
- profile charging dynamic-rules request-quota, on page 310
- profile charging failure-handling error-type, on page 311
- profile charging limit, on page 311
- profile charging limit rating-group, on page 312
- profile charging mscc-final-unit-action terminate session, on page 312
- profile charging offline zero-usage, on page 313
- profile charging quota, on page 313
- profile charging quota suppress, on page 314
- profile charging quota validity-time, on page 314
- profile charging quota volume-threshold percent, on page 315
- profile charging reporting-level, on page 315

- profile charging requested-service-unit, on page 316
- profile charging requested-service-unit volume, on page 316
- profile charging send charging-initial, on page 316
- profile charging session-failover, on page 317
- profile charging tariff-time-change, on page 317
- profile charging triggers, on page 318
- profile charging-characteristics, on page 318
- profile charging-characteristics network-element-profile-list, on page 319
- profile charging-qbc, on page 319
- profile charging-qbc limit, on page 321
- profile charging usage-reporting quota-to-report based-on-grant, on page 321
- profile compliance, on page 322
- profile compliance service, on page 322
- profile compliance service n1, on page 323
- profile compliance service n2, on page 324
- profile compliance service namf-comm, on page 325
- profile compliance service nchf-convergedcharging, on page 326
- profile compliance service nnrf-disc, on page 327
- profile compliance service nnrf-nfm, on page 328
- profile compliance service npcf-smpolicycontrol, on page 329
- profile compliance service nsmf-pdusession, on page 330
- profile compliance service nudm-sdm, on page 331
- profile compliance service nudm-uecm, on page 332
- profile compliance service threegpp23502, on page 333
- profile content-filtering category database, on page 334
- profile content-filtering category database directory, on page 334
- profile converged-core activated-features, on page 334
- profile converged-core session-hold duration, on page 335
- profile converged-core supported-features, on page 336
- profile diameter-client, on page 336
- profile diameter-endpoint, on page 337
- profile diameter-host-selection, on page 341
- profile dnn, on page 342
- profile dnn ipam dhcp, on page 346
- profile dnn accounting, on page 347
- profile dnn authentication algorithm, on page 347
- profile dnn authentication secondary, on page 348
- profile dnn authorization, on page 348
- profile dnn dnn, on page 349
- profile dnn dnn nw-fu-conf, on page 349
- profile dnn dnn rmgr-conf, on page 349
- profile dnn dns primary, on page 350
- profile dnn dns secondary, on page 350
- profile dnn ims mark, on page 351
- profile dnn ipv6-prefix-delegation, on page 351
- profile dnn max-upf-sessions, on page 351

- profile dnn network-element-profiles, on page 352
- profile dnn nexthop-forwarding-address, on page 353
- profile dnn nssai, on page 353
- profile dnn outbound, on page 354
- profile dnn primary-plmn, on page 354
- profile dnn session-hold duration, on page 354
- profile dnn session type, on page 355
- profile dnn skip-n10-registration, on page 356
- profile dnn subscription, on page 356
- profile dnn ssc-mode, on page 357
- profile dnn timeout, on page 357
- profile dnn timeout bearer-inactivity, on page 359
- profile dnn timeout bearer-inactivity gbr, on page 359
- profile dnn timeout bearer-inactivity gbr volume, on page 359
- profile dnn timeout bearer-inactivity non-gbr, on page 360
- profile dnn timeout bearer-inactivity non-gbr volume, on page 360
- profile dnn upf, on page 361
- profile dnn upcp status, on page 361
- profile dns-proxy, on page 362
- profile dns-proxy servers, on page 363
- profile ecgi-group, on page 364
- profile ecgi-group ecgis, on page 364
- profile ecgi-group ecgis ecgi, on page 364
- profile ecgi-group ecgis ecgi range, on page 365
- profile emergency-profile, on page 365
- profile failure-handling, on page 366
- profile failure-handling interface diameter, on page 366
- profile failure-handling interface gtpc message, on page 368
- profile failure-handling interface gtpc message cause-code-type cause-code, on page 368
- profile failure-handling interface gtpc message cause-code-type cause-code action, on page 368
- profile failure-handling interface n11, on page 369
- profile failure-handling interface n11 message, on page 369
- profile failure-handling interface n11 message cause-code-value cause-code, on page 370
- profile failure-handling interface n11 message cause-code-value cause-code action, on page 370
- profile failure-handling interface pfcp, on page 371
- profile failure-handling interface pfcp message, on page 371
- profile failure-handling interface pfcp message cause-code-type-est cause-code, on page 372
- profile failure-handling interface pfcp message cause-code-type-est cause-code action, on page 373
- profile failure-handling interface pfcp message cause-code-type-mod cause-code, on page 373
- profile failure-handling interface pfcp message cause-code-type-mod cause-code action, on page 374
- profile failure-handling interface pfcp message cause-code-type-sessreport cause-code, on page 375
- profile failure-handling interface pfcp message cause-code-type-sessreport cause-code action, on page 375
- profile failure-handling interface sxa message, on page 375
- profile failure-handling interface sxa message cause-code-type-est cause-code, on page 376
- profile failure-handling interface sxa message cause-code-type-est cause-code action, on page 376

- profile gtpp-profile gtpp, on page 377
- profile icmpv6, on page 379
- profile icmpv6 options, on page 379
- profile icmpv6 ra trigger, on page 380
- profile interface-mapping default interface, on page 381
- profile load, on page 381
- profile load advertise, on page 382
- profile load interface, on page 383
- profile location-area-group, on page 383
- profile message-handling nf type udm mh-profile, on page 384
- profile n3-tunnel, on page 384
- profile n3-tunnel buffer, on page 384
- profile ncgi-group, on page 385
- profile ncgi-group ncgis, on page 385
- profile ncgi-group ncgis ncgi, on page 386
- profile ncgi-group ncgis ncgi range, on page 386
- profile network-element amf, on page 386
- profile network-element amf discovery, on page 387
- profile network-element amf query-params, on page 388
- profile network-element chf, on page 388
- profile network-element chf discovery, on page 390
- profile network-element chf query-params, on page 390
- profile network-element nrf, on page 391
- profile network-element pcf, on page 392
- profile network-element pcf bitrates, on page 393
- profile network-element pcf discovery, on page 394
- profile network-element pcf query-params, on page 394
- profile network-element scp, on page 395
- profile network-element sepp, on page 396
- profile network-element sepp discovery, on page 396
- profile network-element sepp query-params, on page 397
- profile network-element udm, on page 397
- profile network-element udm discovery, on page 399
- profile network-element udm failure-handling-profile-rat, on page 399
- profile network-element udm query-params, on page 400
- profile network-element upf, on page 400
- profile network-element upf n4-peer-address, on page 402
- profile nf-client nf-type amf amf-profile, on page 403
- profile nf-client nf-type amf amf-profile locality, on page 403
- profile nf-client nf-type amf amf-profile locality service name type, on page 404
- profile nf-client nf-type amf amf-profile locality service name type endpoint-profile, on page 404
- profile nf-client nf-type amf amf-profile locality service name type endpoint-profile endpoint-name, on page 405
- profile nf-client nf-type amf amf-profile locality service name type endpoint-profile endpoint-name primary ip-address, on page 406

- profile nf-client nf-type amf amf-profile locality service name type endpoint-profile endpoint-name secondary ip-address, on page 407
- profile nf-client nf-type amf amf-profile locality service name type endpoint-profile endpoint-name tertiary ip-address, on page 407
- profile nf-client nf-type amf amf-profile locality service name type endpoint-profile version uri-version, on page 408
- profile nf-client nf-type ausf ausf-profile, on page 408
- profile nf-client nf-type ausf ausf-profile locality, on page 409
- profile nf-client nf-type ausf ausf-profile locality service name type, on page 409
- profile nf-client nf-type ausf ausf-profile locality service name type endpoint-profile, on page 410
- profile nf-client nf-type ausf ausf-profile locality service name type endpoint-profile endpoint-name, on page 411
- profile nf-client nf-type ausf ausf-profile locality service name type endpoint-profile endpoint-name primary ip-address, on page 411
- profile nf-client nf-type ausf ausf-profile locality service name type endpoint-profile endpoint-name secondary ip-address, on page 412
- profile nf-client nf-type ausf ausf-profile locality service name type endpoint-profile endpoint-name tertiary ip-address, on page 413
- profile nf-client nf-type ausf ausf-profile locality service name type endpoint-profile version uri-version, on page 413
- profile nf-client nf-type chf chf-profile, on page 414
- profile nf-client nf-type chf chf-profile locality, on page 414
- profile nf-client nf-type chf chf-profile locality service name type, on page 415
- profile nf-client nf-type chf chf-profile locality service name type endpoint-profile, on page 415
- profile nf-client nf-type chf chf-profile locality service name type endpoint-profile endpoint-name, on page 416
- profile nf-client nf-type chf chf-profile locality service name type endpoint-profile endpoint-name primary ip-address, on page 417
- profile nf-client nf-type chf chf-profile locality service name type endpoint-profile endpoint-name secondary ip-address, on page 418
- profile nf-client nf-type chf chf-profile locality service name type endpoint-profile endpoint-name tertiary ip-address, on page 418
- profile nf-client nf-type chf chf-profile locality service name type endpoint-profile version uri-version, on page 419
- profile nf-client nf-type eir eir-profile, on page 419
- profile nf-client nf-type eir eir-profile locality, on page 420
- profile nf-client nf-type eir eir-profile locality service name type, on page 420
- profile nf-client nf-type eir eir-profile locality service name type endpoint-profile, on page 421
- profile nf-client nf-type eir eir-profile locality service name type endpoint-profile endpoint-name, on page 422
- profile nf-client nf-type eir eir-profile locality service name type endpoint-profile endpoint-name primary ip-address, on page 422
- profile nf-client nf-type eir eir-profile locality service name type endpoint-profile endpoint-name secondary ip-address, on page 423
- profile nf-client nf-type eir eir-profile locality service name type endpoint-profile endpoint-name tertiary ip-address, on page 424
- profile nf-client nf-type eir eir-profile locality service name type endpoint-profile version uri-version, on page 424

- profile nf-client nf-type endpoint-name fqdn name fqdn port, on page 425
- profile nf-client nf-type pcf pcf-profile, on page 425
- profile nf-client nf-type pcf pcf-profile locality, on page 426
- profile nf-client nf-type pcf pcf-profile locality service name type, on page 426
- profile nf-client nf-type pcf pcf-profile locality service name type endpoint-profile, on page 427
- profile nf-client nf-type pcf pcf-profile locality service name type endpoint-profile endpoint-name, on page 428
- profile nf-client nf-type pcf pcf-profile locality service name type endpoint-profile endpoint-name primary ip-address, on page 428
- profile nf-client nf-type pcf pcf-profile locality service name type endpoint-profile endpoint-name secondary ip-address, on page 429
- profile nf-client nf-type pcf pcf-profile locality service name type endpoint-profile endpoint-name tertiary ip-address, on page 430
- profile nf-client nf-type pcf pcf-profile locality service name type endpoint-profile version uri-version, on page 430
- profile nf-client nf-type scp scp-profile, on page 431
- profile nf-client nf-type sepp sepp-profile, on page 432
- profile nf-client nf-type sepp sepp-profile locality, on page 432
- profile nf-client nf-type sepp sepp-profile locality service name type, on page 432
- profile nf-client nf-type sepp sepp-profile locality service name type endpoint-profile, on page 433
- profile nf-client nf-type sepp sepp-profile locality service name type endpoint-profile endpoint-name, on page 434
- profile nf-client nf-type sepp sepp-profile locality service name type endpoint-profile endpoint-name primary ip-address, on page 435
- profile nf-client nf-type sepp sepp-profile locality service name type endpoint-profile endpoint-name secondary ip-address, on page 435
- profile nf-client nf-type sepp sepp-profile locality service name type endpoint-profile endpoint-name tertiary ip-address, on page 436
- profile nf-client nf-type sepp sepp-profile locality service name type endpoint-profile version uri-version, on page 436
- profile nf-client nf-type smf smf-profile, on page 437
- profile nf-client nf-type smf smf-profile locality, on page 437
- profile nf-client nf-type smf smf-profile locality service name type, on page 438
- profile nf-client nf-type smf smf-profile locality service name type endpoint-profile, on page 438
- profile nf-client nf-type smf smf-profile locality service name type endpoint-profile endpoint-name, on page 439
- profile nf-client nf-type smf smf-profile locality service name type endpoint-profile endpoint-name primary ip-address, on page 440
- profile nf-client nf-type smf smf-profile locality service name type endpoint-profile endpoint-name secondary ip-address, on page 441
- profile nf-client nf-type smf smf-profile locality service name type endpoint-profile endpoint-name tertiary ip-address, on page 441
- profile nf-client nf-type smf smf-profile locality service name type endpoint-profile version uri-version, on page 442
- profile nf-client nf-type udm udm-profile, on page 442
- profile nf-client nf-type udm udm-profile locality, on page 443
- profile nf-client nf-type udm udm-profile locality service name type, on page 443

- profile nf-client nf-type udm udm-profile locality service name type endpoint-profile, on page 444
- profile nf-client nf-type udm udm-profile locality service name type endpoint-profile endpoint-name, on page 445
- profile nf-client nf-type udm udm-profile locality service name type endpoint-profile endpoint-name primary ip-address, on page 445
- profile nf-client nf-type udm udm-profile locality service name type endpoint-profile endpoint-name secondary ip-address, on page 446
- profile nf-client nf-type udm udm-profile locality service name type endpoint-profile endpoint-name tertiary ip-address, on page 447
- profile nf-client nf-type udm udm-profile locality service name type endpoint-profile version uri-version, on page 447
- profile nf-client-failure nf-type amf, on page 448
- profile nf-client-failure nf-type amf profile failure-handling, on page 448
- profile nf-client-failure nf-type amf profile failure-handling service name type, on page 448
- profile nf-client-failure nf-type amf profile failure-handling service name type message type, on page 449
- profile nf-client-failure nf-type amf profile failure-handling service name type message type status-code httpv2, on page 450
- profile nf-client-failure nf-type ausf, on page 451
- profile nf-client-failure nf-type ausf profile failure-handling, on page 451
- profile nf-client-failure nf-type ausf profile failure-handling service name type, on page 451
- profile nf-client-failure nf-type ausf profile failure-handling service name type message type, on page 452
- profile nf-client-failure nf-type ausf profile failure-handling service name type message type status-code httpv2, on page 452
- profile nf-client-failure nf-type chf, on page 453
- profile nf-client-failure nf-type chf profile failure-handling, on page 454
- profile nf-client-failure nf-type chf profile failure-handling service name type, on page 454
- profile nf-client-failure nf-type chf profile failure-handling service name type message type, on page 455
- profile nf-client-failure nf-type chf profile failure-handling service name type message type status-code httpv2, on page 455
- profile nf-client-failure nf-type eir, on page 456
- profile nf-client-failure nf-type eir profile failure-handling, on page 456
- profile nf-client-failure nf-type eir profile failure-handling service name type, on page 457
- profile nf-client-failure nf-type eir profile failure-handling service name type message type, on page 457
- profile nf-client-failure nf-type eir profile failure-handling service name type message type status-code httpv2, on page 458
- profile nf-client-failure nf-type nrf, on page 459
- profile nf-client-failure nf-type nrf profile failure-handling, on page 459
- profile nf-client-failure nf-type nrf profile failure-handling service name type, on page 459
- profile nf-client-failure nf-type nrf profile failure-handling service name type message type, on page 460
- profile nf-client-failure nf-type nrf profile failure-handling service name type message type status-code httpv2, on page 461
- profile nf-client-failure nf-type pcf, on page 461
- profile nf-client-failure nf-type pcf profile failure-handling, on page 462
- profile nf-client-failure nf-type pcf profile failure-handling service name type, on page 462
- profile nf-client-failure nf-type pcf profile failure-handling service name type message type, on page 463

- profile nf-client-failure nf-type pcf profile failure-handling service name type message type status-code httpv2, on page 463
- profile nf-client-failure nf-type scp, on page 464
- profile nf-client-failure nf-type sepp, on page 465
- profile nf-client-failure nf-type sepp profile failure-handling, on page 465
- profile nf-client-failure nf-type sepp profile failure-handling service name type, on page 466
- profile nf-client-failure nf-type sepp profile failure-handling service name type message type, on page 466
- profile nf-client-failure nf-type sepp profile failure-handling service name type message type status-code httpv2, on page 467
- profile nf-client-failure nf-type smf, on page 468
- profile nf-client-failure nf-type smf profile failure-handling, on page 468
- profile nf-client-failure nf-type smf profile failure-handling service name type, on page 468
- profile nf-client-failure nf-type smf profile failure-handling service name type message type status-code httpv2, on page 469
- profile nf-client-failure nf-type udm, on page 470
- profile nf-client-failure nf-type udm profile failure-handling, on page 470
- profile nf-client-failure nf-type udm profile failure-handling service name type, on page 471
- profile nf-client-failure nf-type udm profile failure-handling service name type message type, on page 471
- profile nf-client-failure nf-type udm profile failure-handling service name type message type status-code httpv2, on page 472
- profile nf-pair nf-type, on page 473
- profile nf-pair nf-type cache invalidation true, on page 474
- profile nf-pair nf-type locality, on page 475
- profile overload, on page 475
- profile overload node-level, on page 476
- profile overload node-level advertise, on page 476
- profile overload node-level interface, on page 477
- profile overload node-level reduction-metric, on page 477
- profile overload node-level tolerance, on page 478
- profile overload overload-exclude-profile, on page 478
- profile overload peer-level interface, on page 479
- profile overload peer-level interface action throttle, on page 479
- profile overload peer-level message-prioritization, on page 480
- profile overload-exclude, on page 480
- profile overload-exclude message-priority, on page 481
- profile overload-exclude procedure-list, on page 482
- profile pcscf, on page 482
- profile pcscf fqdn, on page 483
- profile pcscf pcscf-selection, on page 483
- profile pcscf pcscf-restoration trigger, on page 483
- profile pcscf v4-list, on page 484
- profile pcscf v4-list list-entry, on page 484
- profile pcscf v4-list list-entry primary, on page 484
- profile pcscf v4-list list-entry secondary, on page 485

- profile pcscf v4-list list-entry tertiary, on page 485
- profile pcscf v4v6-list, on page 486
- profile pcscf v4v6-list list-entry, on page 486
- profile pcscf v4v6-list list-entry primary, on page 486
- profile pcscf v4v6-list list-entry secondary, on page 487
- profile pcscf v4v6-list list-entry tertiary, on page 488
- profile pcscf v6-list, on page 488
- profile pcscf v6-list list-entry, on page 489
- profile pcscf v6-list list-entry primary, on page 489
- profile pcscf v6-list list-entry secondary, on page 489
- profile pcscf v6-list list-entry tertiary, on page 490
- profile ppd, on page 490
- profile ppd dscp-list, on page 491
- profile qos, on page 491
- profile qos ambr, on page 492
- profile qos arp, on page 493
- profile qos dscp-map qi5, on page 493
- profile qos dscp-map qi5 arp-priority-level, on page 494
- profile qos dscp-map qi5 arp-priority-level dscp-info, on page 494
- profile qos dscp-map qi5 arp-priority-level dscp-info user-datagram, on page 495
- profile qos dscp-map qi5 dscp-info, on page 496
- profile qos dscp-map qi5 dscp-info user-datagram, on page 497
- profile qos max, on page 497
- profile qos qos-enforcement, on page 498
- profile qos qosflow qi5, on page 498
- profile qos qosflow qi5 arp-priority-level, on page 498
- profile qos qosflow qi5 arp-priority-level dscp-info downlink encaps-header, on page 499
- profile qos qosflow qi5 arp-priority-level dscp-info downlink user-datagram, on page 499
- profile qos qosflow qi5 arp-priority-level dscp-info uplink encaps-header, on page 500
- profile qos qosflow qi5 arp-priority-level dscp-info uplink user-datagram, on page 501
- profile qos qosflow qi5 arp-priority-level flow-parameter gfbr, on page 501
- profile qos qosflow qi5 arp-priority-level flow-parameter mfbr, on page 502
- profile qos qosflow qi5 dscp-info downlink encaps-header, on page 502
- profile qos qosflow qi5 dscp-info downlink user-datagram, on page 503
- profile qos qosflow qi5 dscp-info uplink encaps-header, on page 504
- profile qos qosflow qi5 dscp-info uplink user-datagram, on page 504
- profile qos qosflow qi5 flow-parameter gfbr, on page 505
- profile qos qosflow qi5 flow-parameter mfbr, on page 505
- profile radius, on page 506
- profile radius accounting, on page 507
- profile radius accounting attribute, on page 507
- profile radius accounting attribute instance, on page 508
- profile radius accounting detect-dead-server, on page 509
- profile radius allow auth, on page 509
- radius profile server group allow auth, on page 510
- profile radius attribute, on page 510

- profile radius attribute instance, on page 511
- profile radius consecutive failure dead server detection, on page 511
- profile radius detect-dead-server, on page 512
- profile radius dictionary, on page 512
- profile radius max transmissions, on page 513
- profile radius server, on page 513
- profile radius server-group, on page 514
- profile radius server-group accounting, on page 515
- profile radius server-group accounting attribute, on page 515
- profile radius server-group accounting attribute instance, on page 516
- profile radius server-group attribute, on page 517
- profile radius server-group attribute instance, on page 517
- profile radius server-group server, on page 518
- profile radius server group max transmissions, on page 519
- profile radius-dynamic-author, on page 519
- profile radius-dynamic-author client, on page 520
- profile sgw-qos-profile, on page 520
- profile sgw-qos-profile dscp-map operator-defined-qci, on page 521
- profile sgw-qos-profile dscp-map operator-defined-qci gbr arp-priority-level, on page 521
- profile sgw-qos-profile dscp-map operator-defined-qci gbr arp-priority-level dscp-info, on page 521
- profile sgw-qos-profile dscp-map operator-defined-qci gbr dscp-info, on page 527
- profile sgw-qos-profile dscp-map operator-defined-qci non-gbr, on page 532
- profile sgw-qos-profile dscp-map operator-defined-qci non-gbr arp-priority-level, on page 533
- profile sgw-qos-profile dscp-map operator-defined-qci non-gbr arp-priority-level dscp-info, on page 533
- profile sgw-qos-profile dscp-map operator-defined-qci non-gbr dscp-info, on page 538
- profile sgw-qos-profile dscp-map qci, on page 544
- profile sgw-qos-profile dscp-map qci arp-priority-level, on page 544
- profile sgw-qos-profile dscp-map qci arp-priority-level dscp-info, on page 544
- profile sgw-qos-profile dscp-map qci default, on page 550
- profile sgw-qos-profile dscp-map qci default dscp-info, on page 550
- profile sgw-qos-profile dscp-map qci gbr dscp-info, on page 556
- profile sgw-qos-profile dscp-map qci non-gbr dscp-info, on page 561
- profile smf, on page 567
- profile smf instances, on page 568
- profile smf instances deactivate-features, on page 569
- profile smf plmn-id, on page 570
- profile smf plmn-list, on page 570
- profile smf service, on page 571
- profile smf service http-endpoint, on page 572
- profile tai-group, on page 573
- profile tai-group tais, on page 573
- profile tai-group tais tac, on page 574
- profile tai-group tais tac range, on page 574
- profile upf-group, on page 574
- profile upf-group failure-profile, on page 576
- profile upf-group heartbeat, on page 576

- profile wps, on page 576
- profile wps dscp, on page 577
- service name type, on page 579
- radius, on page 580
- radius acct-server, on page 580
- radius auth-server, on page 580
- radius-dyn-auth, on page 580
- radius-dyn-auth clients, on page 580
- rcm switchover, on page 581
- reconcile ipam, on page 581
- resource pod, on page 581
- resource pod cpu, on page 582
- resource pod labels, on page 582
- resource pod memory, on page 582
- resources info, on page 583
- router bgplist, on page 583
- router bgplist bfd, on page 584
- router bgplist interfaceList, on page 584
- router bgplist interfaceList bondingInterfaces, on page 585
- router bgplist interfaceList neighbors, on page 585
- router bgplist policies, on page 586
- rpc all, on page 587
- running-status info, on page 587
- screen-length, on page 588
- screen-width, on page 588
- send, on page 588
- sessions affinity, on page 589
- sessions commit-pending, on page 589
- quit, on page 589
- show, on page 590
- show bfd-neighbor, on page 590
- show bgp-advertised-routes, on page 590
- show bgp-global, on page 591
- show bgp-kernel-route, on page 591
- show bgp-learned-routes, on page 591
- show bgp-neighbors, on page 592
- show bgp-route-summary, on page 592
- show bgp-routes, on page 592
- show diameter routes all, on page 593
- show edr, on page 593
- show geo-maintenance-mode, on page 593
- show georeplication-status, on page 594
- show georeplication, on page 594
- show idmgr-debug, on page 594
- show ipam dp, on page 594
- show ipam dp name, on page 595

- show ipam dp name ipv4-addr, on page 595
- show ipam dp name ipv6-addr, on page 595
- show ipam dp name ipv6-prefix, on page 595
- show ipam dp tag, on page 596
- show ipam dp tag tag-name, on page 596
- show ipam dp tag ipv4-addr, on page 596
- show ipam dp tag ipv6-addr, on page 597
- show ipam dp tag ipv6-prefix, on page 597
- show ipam pool, on page 597
- show ipam pool name, on page 597
- show ipam pool name ipv4-addr, on page 598
- show ipam pool name ipv6-addr, on page 598
- show ipam pool name ipv6-prefix, on page 598
- show ipam-staticdb, on page 598
- show peers, on page 599
- show role, on page 599
- show subscriber, on page 599
- show subscriber count-opt, on page 604
- show subscriber debug-opt, on page 607
- show subscriber gpsi-opt policy-opt, on page 608
- show subscriber imsi-opt, on page 609
- show subscriber msid-opt policy-opt, on page 609
- show subscriber msisdn-opt policy-opt, on page 610
- show subscriber pei-opt policy-opt, on page 610
- show subscriber supi-opt, on page 610
- show subscriber supi-opt policy-opt, on page 611
- show userplane userplane, on page 611
- show vrf-info, on page 612
- show vrf-route-info, on page 612
- show-defaults, on page 613
- show confd-state, on page 613
- show dns-cache, on page 613
- show dns-query, on page 614
- show gtpp-ep, on page 614
- show helm, on page 614
- show history, on page 615
- show jobs, on page 615
- show last-logins, on page 615
- show license, on page 615
- show local-interface-status, on page 616
- show mode, on page 616
- show nacm, on page 616
- show netconf-state, on page 617
- show nf-tls, on page 617
- show notification, on page 617
- show nrf, on page 618

- show ops, on page 618
- show overload-info, on page 618
- show parser, on page 619
- show pcscf, on page 619
- show resources, on page 619
- show restconf-state, on page 620
- show running-config, on page 620
- smiuser, on page 620
- system, on page 622
- system-diagnostics event-trace, on page 622
- system-diagnostics idmgr-secondary-recon, on page 623
- system-diagnostics ip-validation, on page 623
- system-diagnostics pod type, on page 623
- system-diagnostics pod type fault, on page 624
- system-diagnostics protocol supi, on page 625
- system-diagnostics protocol supi preferred-up, on page 625
- system-diagnostics session-consistency, on page 625
- terminal, on page 626
- test dns-query, on page 626
- test gtpc echo , on page 627
- test gtpp echo, on page 627
- test-radius accounting, on page 628
- test-radius authentication, on page 629
- timestamp, on page 630
- who, on page 631

aaa

Configures AAA based user management parameters.

Privilege

Security Administrator, Administrator

Command Modes

Exec

Syntax Description

aaa { authentication { users *list_of_local_users* **admin change-password old-password** *user_password* **new-password** *user_password* **confirm-password** *user_password* **} }**

users *list_of_local_users*

Specify the user name.

Must be a string.

old-password *user_password*

Specifies the current password of the user.

Must be a string.

new-password *user_password*

Specifies a new password of the user.

Must be a string.

confirm-password *user_password*

Enter the new password once again to change the password.

Must be a string.

Usage Guidelines Use this command to configure the AAA based user management parameters.

active-charging service

Configures Active Charging Service (ACS) parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **`active-charging service`** *`service_name`*

service *service_name*

Specify name of the Active Charging Service.

Must be a string of 1-15 characters.

Usage Guidelines Use this command to configure the ACS parameters.

You can configure a maximum of one element with this command.

active-charging service bandwidth-policy

Configures ACS bandwidth policy parameters.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*)

Syntax Description **`bandwidth-policy`** *`bandwidth_policy_name`*

bandwidth-policy *bandwidth_policy_name*

Specify name of the ACS Bandwidth Policy.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to configure ACS bandwidth policy parameters. The CLI prompt changes to the Bandwidth Policy Configuration mode (config-bandwidth-policy-<policy_name>).

You can configure a maximum of 64 elements with this command.

active-charging service bandwidth-policy flow limit-for-bandwidth id

Configures bandwidth ID and bandwidth policy group parameters.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Bandwidth Policy Configuration (config-bandwidth-policy-*policy_name*)

Syntax Description

flow limit-for-bandwidth id *id* **group-id** *group_id*

group-id *group_id*

Specify the bandwidth policy group ID.

Must be an integer in the range of 1-65535.

id *id*

Specify the bandwidth ID.

Must be an integer in the range of 1-65535.

Usage Guidelines

Use this command to configure the bandwidth ID and bandwidth policy group parameters.

You can configure a maximum of 1000 elements with this command.

active-charging service bandwidth-policy group-id

Configures bandwidth policy group ID.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Bandwidth Policy Configuration (config-bandwidth-policy-*policy_name*)

Syntax Description

group-id *group_id*

group-id *group_id*

Specify the bandwidth policy group ID.

Must be an integer in the range of 1-65535.

Usage Guidelines

Use this command to configure the bandwidth policy group ID.

You can configure a maximum of 1000 elements with this command.

active-charging service bandwidth-policy group-id direction downlink grpPeakBwp

Configures peak bandwidth parameters.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Bandwidth Policy Configuration (config-bandwidth-policy-*policy_name*)

Syntax Description

group-id *group_id* **direction downlink peak-data-rate-kbps** *peak_data_rate* **peak-burst-size** *peak_burst_size* **violate-action lower-ip-precedence committed-data-rate-kbps**

Syntax Description

group-id *group_id* **direction uplink peak-data-rate-kbps** *peak_data_rate* **peak-burst-size** *peak_burst_size* **violate-action lower-ip-precedence committed-data-rate-kbps**

committed-burst-size *committed_burst_size*

Specify the committed burst size in bytes.

Must be an integer in the range of 1-4294967295.

committed-options *committed_option*

Specify the committed option.

Must be one of the following:

- **committed-data-rate-kbps**: Specify Committed Data Rate in kilo bits per second. This can also be used to specify GBR for Bearer Binding (without the exceed-action).
- **committed-data-rate**: Specify Committed Data Rate in bits per second. This can also be used to specify GBR for flow Binding (without the exceed-action).

committed-value *committed_value*

Specify the bandwidth in bits per second.

Must be an integer in the range of 1-4294967295.

exceed-action *exceed_action*

Specify the action to be taken if committed data rate is surpassed.

Must be one of the following:

- **discard**: Specify to discard the packet.
- **lower-ip-precedence**: Specify to lower the IP precedence of the packet.

peak-burst-size *peak_burst_size*

Specify the burst size in bytes.

Must be an integer in the range of 1-4294967295.

peak-options *peak_options*

Specify the peak data rate option.

Must be one of the following:

- **peak-data-rate-kbps**: Specify Peak Data Rate in kilo bits per second.
- **peak-data-rate**: Specify Peak Data Rate in bits per second.

peak-value *peak_value*

Specify the bandwidth in bits per second.

Must be an integer in the range of 1-4294967295.

violate-action *violate_action*

Specify the action to be taken if Peak Data Rate is surpassed.

Must be one of the following:

- **discard**: Specify to discard the packet.
- **lower-ip-precedence**: Specify to lower the IP precedence of the packet.

Usage Guidelines Configures bandwidth control in downlink or uplink directions. Use this command to configure the peak bandwidth parameters.

active-charging service bandwidth-policy group-id direction uplink grpPeakBwp

Configures peak bandwidth parameters.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Bandwidth Policy Configuration (config-bandwidth-policy-*policy_name*)

Syntax Description **group-id** *group_id* **direction downlink peak-data-rate-kbps** *peak_data_rate* **peak-burst-size** *peak_burst_size* **violate-action lower-ip-precedence committed-data-rate-kbps**

Syntax Description **group-id** *group_id* **direction uplink peak-data-rate-kbps** *peak_data_rate* **peak-burst-size** *peak_burst_size* **violate-action lower-ip-precedence committed-data-rate-kbps**

committed-burst-size *committed_burst_size*

Specify the committed burst size in bytes.

Must be an integer in the range of 1-4294967295.

committed-options *committed_option*

Specify the committed option.

Must be one of the following:

- **committed-data-rate-kbps**: Specify Committed Data Rate in kilo bits per second. This can also be used to specify GBR for Bearer Binding (without the exceed-action).
- **committed-data-rate**: Specify Committed Data Rate in bits per second. This can also be used to specify GBR for flow Binding (without the exceed-action).

committed-value *committed_value*

Specify the bandwidth in bits per second.

Must be an integer in the range of 1-4294967295.

exceed-action *exceed_action*

Specify the action to be taken if committed data rate is surpassed.

Must be one of the following:

- **discard**: Specify to discard the packet.
- **lower-ip-precedence**: Specify to lower the IP precedence of the packet.

peak-burst-size *peak_burst_size*

Specify the burst size in bytes.

Must be an integer in the range of 1-4294967295.

peak-options *peak_options*

Specify the peak data rate option.

Must be one of the following:

- **peak-data-rate-kbps**: Specify Peak Data Rate in kilo bits per second.
- **peak-data-rate**: Specify Peak Data Rate in bits per second.

peak-value *peak_value*

Specify the bandwidth in bits per second.

Must be an integer in the range of 1-4294967295.

violate-action *violate_action*

Specify the action to be taken if Peak Data Rate is surpassed.

Must be one of the following:

- **discard**: Specify to discard the packet.
- **lower-ip-precedence**: Specify to lower the IP precedence of the packet.

Usage Guidelines Configures bandwidth control in downlink or uplink directions. Use this command to configure the peak bandwidth parameters.

active-charging service buffering-limit

Configures flow/session-based packet buffering.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*)

Syntax Description **buffering-limit { [flow-max-packets** *flow_max_packets* **] [subscriber-max-packets** *subscriber_max_packets* **] }**

flow-max-packets *flow_max_packets*

Specify the maximum number of packets to be buffered per flow.

Must be an integer in the range of 1-255.

subscriber-max-packets *subscriber_max_packets*

Specify the maximum number of packets to be buffered per subscriber.

Must be an integer in the range of 1-255.

Usage Guidelines Use this command to configure flow/session-based packet buffering configuration.

active-charging service charging-action

Configures ACS charging actions.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*)

Syntax Description **charging-action** *charging_action_name* **[[content-id** *content_id* **] [nexthop-forwarding-address {** *ipv4_address* **|** *ipv6_address* **} [qos-class-identifier** *qos_class_id* **] [service-identifier** *service_id* **] [ft-notify-ue]]**

charging-action *charging_action_name*

Specify name of the charging action.

Must be a string of 1-63 characters.

content-id *content_id*

Specify the content ID to use in the generated billing records, as well as the AVP used by the Credit Control Application, such as the "Rating-Group" AVP for use by the Diameter Credit Control Application (DCCA). This identifier assists the carrier's billing post processing and is also used by the credit-control system to use independent quotas for different value of content-id.

Must be an integer in the range of 1-2147483647.

nexthop-forwarding-address { *ipv4_address* | *ipv6_address* }

Specify the nexthop forwarding address for this charging action. When an uplink packet matches a rule and a charging action is applied to it this nexthop forwarding address is used.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

qos-class-identifier *qos_class_id*

Specify the QoS Class Identifier (QCI).

Must be an integer in the range of 1-9.

service-identifier *service_id*

Specify the service identifier to use in the generated billing records, as well as the AVP used by the Credit Control Application, such as the "Service-Identifier" AVP for use by DCCA. This is a more general classifier than content-id.

Must be an integer in the range of 1-2147483647.

tft-notify-ue

Specify whether or not TFT updates are sent to UE. Use this command to suppress the selected TFT updates from being sent to the UE. This helps to identify if the appropriate TFT defined in the charging action needs to be sent to the UE or not.

Usage Guidelines

Use this command to create and configure an ACS charging action. A charging action represents actions to be taken when a configured rule is matched. Actions could range from generating an accounting record (for example, an EDR) to dropping the IP packet, etc. The charging action will also determine the metering principle whether to count retransmitted packets and which protocol field to use for billing (L3/L4/L7 etc).

Example

The following command creates a charging action named action123 and changes to the ACS Charging Action Configuration Mode:

```
charging-action action123
```

active-charging service charging-action allocation-retention-priority

Configures the Allocation Retention Priority (ARP).

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description **allocation-retention-priority** *priority_level* **{ pci** *preemption_capability_indicator* **| pvi** *preemption_vulnerability_indicator* **}**

allocation-retention-priority *priority_level*

Specify the priority.

Must be an integer in the range of 1-15.

pci *preemption_capability_indicator*

Specify the Pre-emption Capability Indicator (PCI).

Must be one of the following:

- **MAY_PREEMPT**
- **NOT_PREEMPT**

pvi *preemption_vulnerability_indicator*

Specify the Pre-emption Vulnerability Indicator (PVI).

Must be one of the following:

- **NOT_PREEMPTABLE**
- **PREEMPTABLE**

Usage Guidelines This command configures the ARP, which indicates the priority of allocation and retention of the service data flow. The ARP resolves conflicts in demand for network resources. At the time of resource crunch, this parameter prioritizes allocation of resources during bearer establishment and modification. In a congestion situation, a lower ARP flow may be dropped to free up capacity. Once a service flow is successfully established, this parameter plays no role in quality of service (QoS) experienced by the flow.

Example

The following command sets the ARP to 10:

```
allocation-retention-priority 10
```

active-charging service charging-action billing-action

Configures the billing action for packets that match specific ruledefs.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description **billing-action egcdr**

egcdr

Specify to enable eG-CDR billing.

Usage Guidelines Use this command to enable eG-CDR type of billing for content matching this charging action.

active-charging service charging-action cca charging credit

Configures the Credit Control Charging Credit behavior.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description **`cca charging credit [ rating-group`** *`coupon_id`* **`] [ preemptively-request ]`**

preemptively-request

Specify preemptively requested charging credit behavior.

rating-group *coupon_id*

Specify the coupon ID used in prepaid charging as rating-group which maps to the coupon ID for prepaid customer. This option also assigns different content-types for the same charging action depending upon whether or not prepaid is enabled. This rating-group overrides the content ID, if present in the same charging-action for the prepaid customer in Diameter Credit Control Application (DCCA). But, only the content IDs will be used in eG-CDRs irrespective of the presence of rating-group in that charging action.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure RADIUS/Diameter Prepaid Credit Control Charging Credit behavior.

active-charging service charging-action flow action

Configures to take the redirect-url or terminate-flow action on packets that match ruledefs.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description **`flow action { redirect-url`** *`redirect_url`* **`| terminate-flow }`**

redirect-url *redirect_url*

Specify to redirect URL.

Must be a string.

terminate-flow

Specify to terminate flow.

Usage Guidelines Use this command to specify the action to take on packets, for example to terminate.

Example

The following command sets the flow action to terminate:

```
flow action terminate-flow
```

active-charging service charging-action flow action discard

Configures discard action on packets that match ruledefs.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description **`flow action discard [ downlink | uplink ]`**

downlink

Specify only downlink packets.

uplink

Specify only uplink packets.

Usage Guidelines Use this command to configure discard action on packets that match ruledefs.

active-charging service charging-action flow action readdress

Configures the readdress server for this charging action.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description **`flow action readdress server {`** *`ipv4_address`* **`|`** *`ipv6_address`* **`}`**

server { *ipv4_address* | *ipv6_address* }

Specify IP address of the readdress server.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure the readdress server for this charging action.

active-charging service charging-action flow limit-for-bandwidth

For Session Control functionality, this command allows you to enable or disable bandwidth limiting.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description

flow limit-for-bandwidth { direction | id *bw_limit_id* **}**

id *bw_limit_id*

Specify the bandwidth limiting ID.

Must be an integer in the range of 1-65535.

Usage Guidelines

Use this command to limit the bandwidth a subscriber uses in the uplink and downlink directions under Session Control.

active-charging service charging-action flow limit-for-bandwidth direction downlink peak-data-rate

Configures the peak data rate in bits per second.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description

flow limit-for-bandwidth direction downlink peak-data-rate *peak_data_rate* **peak-burst-size** *peak_burst_size* **violate-action** *violate_action* **[committed-data-rate** *committed_data_rate* **committed-burst-size** *committed_burst_size* **exceed-action** *exceed_action* **]**

Syntax Description

flow limit-for-bandwidth direction uplink peak-data-rate *peak_data_rate* **peak-burst-size** *peak_burst_size* **violate-action** *violate_action* **[committed-data-rate** *committed_data_rate* **committed-burst-size** *committed_burst_size* **exceed-action** *exceed_action* **]**

committed-burst-size *committed_burst_size*

Specify the committed burst size in bytes.

Must be an integer in the range of 1-4294967295.

Default Value: 3000.

committed-data-rate *committed_data_rate*

Specify the Committed Data Rate in bits per second. This can also be used to specify GBR for Bearer Binding (without the exceed-action).

Must be an integer in the range of 1-4294967295.

Default Value: 144000.

exceed-action *exceed_action*

Specify the action to be taken if the Committed Data Rate is surpassed.

Must be one of the following:

- **discard**: Specify to discard the packet.
- **lower-ip-precedence**: Specify to lower the IP precedence of the packet.

peak-burst-size *peak_burst_size*

Specify the peak burst size in bytes.

Must be an integer in the range of 1-4294967295.

violate-action *violate_action*

Specify the action to be taken if the Peak Data Rate is surpassed.

Must be one of the following:

- **discard**: Specify to discard the packet.
- **lower-ip-precedence**: Specify to lower the IP precedence of the packet.

peak_data_rate

Specify the peak data rate in bits per second.

Must be an integer in the range of 1-4294967295.

Usage Guidelines Configures bandwidth control in downlink or uplink directions. Use this command to configure the peak data rate in bits per second.

active-charging service charging-action flow limit-for-bandwidth direction uplink peak-data-rate

Configures the peak data rate in bits per second.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description **`flow limit-for-bandwidth direction downlink peak-data-rate`** *`peak_data_rate`* **`peak-burst-size`** *`peak_burst_size`* **`violate-action`** *`violate_action`* **`[`**

committed-data-rate *committed_data_rate* **committed-burst-size** *committed_burst_size* **exceed-action** *exceed_action* **]**

Syntax Description

flow limit-for-bandwidth direction uplink peak-data-rate *peak_data_rate* **peak-burst-size** *peak_burst_size* **violate-action** *violate_action* **[committed-data-rate** *committed_data_rate* **committed-burst-size** *committed_burst_size* **exceed-action** *exceed_action* **]**

committed-burst-size *committed_burst_size*

Specify the committed burst size in bytes.

Must be an integer in the range of 1-4294967295.

Default Value: 3000.

committed-data-rate *committed_data_rate*

Specify the Committed Data Rate in bits per second. This can also be used to specify GBR for Bearer Binding (without the exceed-action).

Must be an integer in the range of 1-4294967295.

Default Value: 144000.

exceed-action *exceed_action*

Specify the action to be taken if the Committed Data Rate is surpassed.

Must be one of the following:

- **discard**: Specify to discard the packet.
- **lower-ip-precedence**: Specify to lower the IP precedence of the packet.

peak-burst-size *peak_burst_size*

Specify the peak burst size in bytes.

Must be an integer in the range of 1-4294967295.

violate-action *violate_action*

Specify the action to be taken if the Peak Data Rate is surpassed.

Must be one of the following:

- **discard**: Specify to discard the packet.
- **lower-ip-precedence**: Specify to lower the IP precedence of the packet.

peak_data_rate

Specify the peak data rate in bits per second.

Must be an integer in the range of 1-4294967295.

Usage Guidelines Configures bandwidth control in downlink or uplink directions. Use this command to configure the peak data rate in bits per second.

active-charging service charging-action tft packet-filter

Configures the packet filter to use in Traffic Flow Template (TFT) sent to the MS.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description **`tft packet-filter`** *`packet_filter_name`*

packet-filter *packet_filter_name*

Specify name of the packet filter.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to configure the packet filter to be sent to the MS. Up to eight packet filters can be specified in a charging action.

You can configure a maximum of eight elements with this command.

Example

The following command configures the packet filter filter23 to be sent to the MS:

```
tft packet-filter filter23
```

active-charging service charging-action tos af11

Configures using Assured Forwarding 11 Per Hop Behavior (PHB).

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description **`tos af11 [ downlink | uplink ]`**

downlink

Specify only downlink packets.

uplink

Specify only uplink packets.

Usage Guidelines Use this command to configure using Assured Forwarding 11 Per Hop Behavior (PHB).

active-charging service charging-action tos af12

Configures using Assured Forwarding 12 Per Hop Behavior (PHB).

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description `tos af12 [ downlink | uplink ]`

downlink

Specify only downlink packets.

uplink

Specify only uplink packets.

Usage Guidelines Use this command to configure using Assured Forwarding 12 Per Hop Behavior (PHB).

active-charging service charging-action tos af13

Configures using Assured Forwarding 13 Per Hop Behavior (PHB).

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description `tos af13 [ downlink | uplink ]`

downlink

Specify only downlink packets.

uplink

Specify only uplink packets.

Usage Guidelines Use this command to configure using Assured Forwarding 13 Per Hop Behavior (PHB).

active-charging service charging-action tos af21

Configures using Assured Forwarding 21 Per Hop Behavior (PHB).

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description `tos af21 [ downlink | uplink ]`

downlink

Specify only downlink packets.

uplink

Specify only uplink packets.

Usage Guidelines Use this command to configure using Assured Forwarding 21 Per Hop Behavior (PHB).

active-charging service charging-action tos af22

Configures using Assured Forwarding 22 Per Hop Behavior (PHB).

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description `tos af22 [ downlink | uplink ]`

downlink

Specify only downlink packets.

uplink

Specify only uplink packets.

Usage Guidelines Use this command to configure using Assured Forwarding 22 Per Hop Behavior (PHB).

active-charging service charging-action tos af23

Configures using Assured Forwarding 23 Per Hop Behavior (PHB).

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description `tos af23 [ downlink | uplink ]`

downlink

Specify only downlink packets.

uplink

Specify only uplink packets.

Usage Guidelines Use this command to configure using Assured Forwarding 23 Per Hop Behavior (PHB).

active-charging service charging-action tos af31

Configures using Assured Forwarding 31 Per Hop Behavior (PHB).

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description `tos af31 [ downlink | uplink ]`

downlink

Specify only downlink packets.

uplink

Specify only uplink packets.

Usage Guidelines Use this command to configure using Assured Forwarding 31 Per Hop Behavior (PHB).

active-charging service charging-action tos af32

Configures using Assured Forwarding 32 Per Hop Behavior (PHB).

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description `tos af32 [ downlink | uplink ]`

downlink

Specify only downlink packets.

uplink

Specify only uplink packets.

Usage Guidelines Use this command to configure using Assured Forwarding 32 Per Hop Behavior (PHB).

active-charging service charging-action tos af33

Configures using Assured Forwarding 33 Per Hop Behavior (PHB).

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description `tos af33 [ downlink | uplink ]`

downlink

Specify only downlink packets.

uplink

Specify only uplink packets.

Usage Guidelines Use this command to configure using Assured Forwarding 33 Per Hop Behavior (PHB).

active-charging service charging-action tos af41

Configures using Assured Forwarding 41 Per Hop Behavior (PHB).

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description `tos af41 [ downlink | uplink ]`

downlink

Specify only downlink packets.

uplink

Specify only uplink packets.

Usage Guidelines Use this command to configure using Assured Forwarding 41 Per Hop Behavior (PHB).

active-charging service charging-action tos af42

Configures using Assured Forwarding 42 Per Hop Behavior (PHB).

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description `tos af42 [ downlink | uplink ]`

downlink

Specify only downlink packets.

uplink

Specify only uplink packets.

Usage Guidelines Use this command to configure using Assured Forwarding 42 Per Hop Behavior (PHB).

active-charging service charging-action tos af43

Configures using Assured Forwarding 43 Per Hop Behavior (PHB).

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description `tos af43 [ downlink | uplink ]`

downlink

Specify only downlink packets.

uplink

Specify only uplink packets.

Usage Guidelines Use this command to configure using Assured Forwarding 43 Per Hop Behavior (PHB).

active-charging service charging-action tos be

Configures using Best Effort Forwarding PHB.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description `tos be [ downlink | uplink ]`

downlink

Specify only downlink packets.

uplink

Specify only uplink packets.

Usage Guidelines Use this command to configure using Best Effort Forwarding Per Hop Behavior (PHB).

active-charging service charging-action tos ef

Configures using Expedited Forwarding PHB.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description `tos ef [ downlink | uplink ]`

downlink

Specify only downlink packets.

uplink

Specify only uplink packets.

Usage Guidelines Use this command to configure using Expedited Forwarding Per Hop Behavior (PHB).

active-charging service charging-action tos lower-bits

Configures the least-significant six bits in the ToS byte with the specified numeric value.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Charging Action Configuration (config-charging-action-*charging_action_name*)

Syntax Description **`tos lower-bits`** *`value`* **`[ downlink | uplink ]`**

downlink

Specify the ToS only for downlink packets.

lower-bits *value*

Specify the value.

Must be an integer in the range of 0-63.

uplink

Specify the ToS only for uplink packets.

Usage Guidelines Use this command to configure the least-significant six bits in the ToS byte with the specified numeric value.

active-charging service content-filtering category policy-id

Configures Content Filtering Category Policy ID.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*)

Syntax Description **`content-filtering category policy-id`** *`cf_category_policy_id`*

policy-id *cf_category_policy_id*

Specify the Content Filtering Category Policy ID.

Must be an integer in the range of 1-4294967295.

Usage Guidelines Use this command to configure the Content Filtering Category Policy ID. The CLI prompt changes to the Content Filtering Category Policy Configuration mode (config-policy-id-<content_filtering_policy_id>).

active-charging service content-filtering category policy-id analyze priority

Assigns priority to a Content Filtering Category in the Content Filtering Policy.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Content Filtering Category Policy Configuration (config-policy-id-*content_filtering_policy_id*)

Syntax Description

analyze priority *cf_category_priority*

priority *cf_category_priority*

Specify priority of the Content Filtering Category in the Content Filtering Policy.

Must be an integer in the range of 1-65535.

Usage Guidelines

Use this command to assign priority to a Content Filtering Category in a Content Filtering Policy.

active-charging service content-filtering category policy-id analyze priority all

Configures all content to be rated.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Content Filtering Category Policy Configuration (config-policy-id-*content_filtering_policy_id*)

Syntax Description

analyze priority *cf_category_priority* **all action { allow | content-insert** *content_to_insert* **}**

action

Specify an action.

allow

Specify the allow action.

content-insert *content_to_insert*

Specify the content insert action, and the content string to insert.

Must be a string.

Usage Guidelines

Use this command to configure the all content to be rated.

active-charging service content-filtering category policy-id analyze priority category

Configures category of the content to be rated.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Content Filtering Category Policy Configuration (config-policy-id-*content_filtering_policy_id*)

Syntax Description

`analyze priority` *`cf_category_priority`* **`category`** *`category_name`* **`action { allow | content-insert`** *`content_to_insert`* **`}`**

action

Specify an action.

allow

Specify the allow action.

category *category_name*

Specify name of the category.

Must be one of the following:

- **ABOR**
- **ADULT**
- **ADVERT**
- **ANON**
- **ART**
- **AUTO**
- **BACKUP**
- **BLACK**
- **BLOG**
- **BUSI**
- **CAR**
- **CDN**
- **CHAT**
- **CMC**
- **CRIME**
- **CULT**

- **DRUG**
- **DYNAM**
- **EDU**
- **ENERGY**
- **ENT**
- **FIN**
- **FORUM**
- **GAMB**
- **GAME**
- **GLAM**
- **GOVERN**
- **HACK**
- **HATE**
- **HEALTH**
- **HOBBY**
- **HOSTS**
- **KIDS**
- **LEGAL**
- **LIFES**
- **MAIL**
- **MIL**
- **NEWS**
- **OCCULT**
- **PEER**
- **PERS**
- **PHOTO**
- **PLAG**
- **POLTIC**
- **PORN**
- **PORTAL**
- **PROXY**
- **REF**

- **REL**
- **SCI**
- **SEARCH**
- **SHOP**
- **SPORT**
- **STREAM**
- **SUIC**
- **SXED**
- **TECH**
- **TRAVE**
- **UNKNOW**
- **VIOL**
- **VOIP**
- **WEAP**
- **WHITE**

content-insert *content_to_insert*

Specify the content insert action, and the content string to insert.

Must be a string.

Usage Guidelines Use this command to configure the category of the content to be rated.

active-charging service content-filtering category policy-id analyze priority x-category

Configures unclassified categories to be rated.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Content Filtering Category Policy Configuration (config-policy-id-*content_filtering_policy_id*)

Syntax Description **`analyze priority`** *`cf_category_priority`* **`x-category`** *`xcategory_name`* **`action { allow | content-insert`** *`content_to_insert`* **`}`**

action

Specify an action.

allow

Specify the allow action.

content-insert *content_to_insert*

Specify the content insert action, and the content string to insert.

Must be a string.

x-category *xcategory_name*

Specify name of the x-category.

Must be a string of 1-6 characters.

Usage Guidelines Use this command to configure unclassified categories to be rated.

active-charging service credit-control group

Configures prepaid services for Diameter/RADIUS applications.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*)

Syntax Description **credit-control group** *cc_group_name*

group *cc_group_name*

Specify name of the credit control group.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to enable/disable Prepaid Credit Control Configuration for RADIUS/Diameter charging mode, and specify the credit control group.

active-charging service credit-control group associate

Associates the failure handling template.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Group Configuration (config-group-*credit_control_group_name*)

Syntax Description **associate failure-handling-template** *template_name*

failure-handling-template *template_name*

Specify name of the failure handling template.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to associate the failure handling template.

active-charging service credit-control group diameter

Configures accepting/ignoring service ID in the Service-Identifier AVP defined in the Diameter dictionaries.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Group Configuration (config-group-*credit_control_group_name*)

Syntax Description

`diameter ignore-service-id { false | true }`

ignore-service-id { false | true }

Specify to enable or disable usage of service ID. To disable, set to true.

Must be one of the following:

- **false**
- **true**

Default Value: false.

Usage Guidelines

Use this command to ignore/accept service ID value in the Service-Identifier AVP in the Diameter dictionaries.

Example

The following command specifies to ignore service ID in the Diameter dictionaries:

```
diameter ignore-service-id
```

active-charging service credit-control group diameter origin

Configures the Diameter Credit Control Origin Endpoint parameter.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Group Configuration (config-group-*credit_control_group_name*)

Syntax Description

`diameter origin endpoint` *`origin_endpoint_name`*

origin endpoint *origin_endpoint_name*

Specify name of the Diameter Credit Control Origin Endpoint.

Must be a string of 1-63 characters.

Usage Guidelines

Use this command to configure the Diameter Credit Control Origin Endpoint parameter.

active-charging service credit-control group diameter service-context-id

Configures the value to be sent in the Service-Context-Id AVP, which defines the context in which DCCA is used.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Group Configuration (config-group-*credit_control_group_name*)

Syntax Description

diameter service-context-id *service_context_id*

service-context-id *service_context_id*

Specify the value to be sent in the Service-Context-Id AVP.

Must be a string of 1-63 characters.

Usage Guidelines

Use this command to specify the value to be sent in the Service-Context-Id AVP, which defines the context in which DCCA is used.

active-charging service credit-control group diameter session

Configures Diameter Credit Control Session Failover configuration.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Group Configuration (config-group-*credit_control_group_name*)

Syntax Description

diameter session failover

failover

Specify Diameter Credit Control Session Failover.

Usage Guidelines

Use this command to configure Diameter Credit Control Session Failover.

active-charging service credit-control group failure-handling initial-request continue

Configures Diameter Credit Control Failure Handling action to continue.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Group Configuration (config-group-*credit_control_group_name*)

Syntax Description

failure-handling initial-request continue *continue_action*

Syntax Description **failure-handling terminate-request continue** *continue_action*

Syntax Description **failure-handling update-request continue** *continue_action*

continue *continue_action*

Specify the continue action.

Must be one of the following:

- **go-offline-after-tx-expiry**: After Tx expiry, start offline charging.
- **retry-after-tx-expiry**: After Tx expiry, retry.

Usage Guidelines Use this command to configure Diameter Credit Control Failure Handling action for CCR-Initial/CCR-Terminate/CR-Update to continue.

active-charging service credit-control group failure-handling initial-request retry-and-terminate

Configures Diameter Credit Control Failure Handling action to retry, and in case of failure, to terminate.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Group Configuration (config-group-*credit_control_group_name*)

Syntax Description **failure-handling initial-request retry-and-terminate** *retry_and_terminate_action*

Syntax Description **failure-handling terminate-request retry-and-terminate** *retry_and_terminate_action*

Syntax Description **failure-handling update-request retry-and-terminate** *retry_and_terminate_action*

retry-and-terminate *retry_and_terminate_action*

Specify the retry-and-terminate action.

Must be one of the following:

- **retry-after-tx-expiry**: After Tx expiry, retry.

Usage Guidelines Configures Diameter Credit Control Failure Handling action for CCR-Initial/CCR-Terminate/CR-Update to retry, and in case of failure, to terminate.

active-charging service credit-control group failure-handling initial-request terminate

Configures Diameter Credit Control Failure Handling action as terminate.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Group Configuration (config-group-*credit_control_group_name*)

Syntax Description **`failure-handling initial-request terminate`**

Syntax Description **`failure-handling terminate-request terminate`**

Syntax Description **`failure-handling update-request terminate`**

Usage Guidelines Configures Diameter Credit Control Failure Handling action for CCR-Initial/CCR-Terminate/CR-Update to terminate.

active-charging service credit-control group failure-handling terminate-request continue

Configures Diameter Credit Control Failure Handling action to continue.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Group Configuration (config-group-*credit_control_group_name*)

Syntax Description **`failure-handling initial-request continue`** *`continue_action`*

Syntax Description **`failure-handling terminate-request continue`** *`continue_action`*

Syntax Description **`failure-handling update-request continue`** *`continue_action`*

continue *continue_action*

Specify the continue action.

Must be one of the following:

- **go-offline-after-tx-expiry**: After Tx expiry, start offline charging.
- **retry-after-tx-expiry**: After Tx expiry, retry.

Usage Guidelines Use this command to configure Diameter Credit Control Failure Handling action for CCR-Initial/CCR-Terminate/CR-Update to continue.

active-charging service credit-control group failure-handling terminate-request retry-and-terminate

Configures Diameter Credit Control Failure Handling action to retry, and in case of failure, to terminate.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Group Configuration (config-group-*credit_control_group_name*)

Syntax Description **failure-handling initial-request retry-and-terminate** *retry_and_terminate_action*

Syntax Description **failure-handling terminate-request retry-and-terminate** *retry_and_terminate_action*

Syntax Description **failure-handling update-request retry-and-terminate** *retry_and_terminate_action*

retry-and-terminate *retry_and_terminate_action*

Specify the retry-and-terminate action.

Must be one of the following:

- **retry-after-tx-expiry**: After Tx expiry, retry.

Usage Guidelines Configures Diameter Credit Control Failure Handling action for CCR-Initial/CCR-Terminate/CR-Update to retry, and in case of failure, to terminate.

active-charging service credit-control group failure-handling terminate-request terminate

Configures Diameter Credit Control Failure Handling action as terminate.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Group Configuration (config-group-*credit_control_group_name*)

Syntax Description **failure-handling initial-request terminate**

Syntax Description **failure-handling terminate-request terminate**

Syntax Description **failure-handling update-request terminate**

Usage Guidelines Configures Diameter Credit Control Failure Handling action for CCR-Initial/CCR-Terminate/CR-Update to terminate.

active-charging service credit-control group failure-handling update-request continue

Configures Diameter Credit Control Failure Handling action to continue.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Group Configuration (config-group-*credit_control_group_name*)

Syntax Description **failure-handling initial-request continue** *continue_action*

Syntax Description **failure-handling terminate-request continue** *continue_action*

Syntax Description **failure-handling update-request continue** *continue_action*

continue *continue_action*

Specify the continue action.

Must be one of the following:

- **go-offline-after-tx-expiry**: After Tx expiry, start offline charging.
- **retry-after-tx-expiry**: After Tx expiry, retry.

Usage Guidelines Use this command to configure Diameter Credit Control Failure Handling action for CCR-Initial/CCR-Terminate/CR-Update to continue.

active-charging service credit-control group failure-handling update-request retry-and-terminate

Configures Diameter Credit Control Failure Handling action to retry, and in case of failure, to terminate.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Group Configuration (config-group-*credit_control_group_name*)

Syntax Description **failure-handling initial-request retry-and-terminate** *retry_and_terminate_action*

Syntax Description **failure-handling terminate-request retry-and-terminate** *retry_and_terminate_action*

Syntax Description **failure-handling update-request retry-and-terminate** *retry_and_terminate_action*

retry-and-terminate *retry_and_terminate_action*

Specify the retry-and-terminate action.

Must be one of the following:

- **retry-after-tx-expiry**: After Tx expiry, retry.

Usage Guidelines Configures Diameter Credit Control Failure Handling action for CCR-Initial/CCR-Terminate/CR-Update to retry, and in case of failure, to terminate.

active-charging service credit-control group failure-handling update-request terminate

Configures Diameter Credit Control Failure Handling action as terminate.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Group Configuration (config-group-*credit_control_group_name*)

Syntax Description `failure-handling initial-request terminate`

Syntax Description `failure-handling terminate-request terminate`

Syntax Description `failure-handling update-request terminate`

Usage Guidelines Configures Diameter Credit Control Failure Handling action for CCR-Initial/CCR-Terminate/CR-Update to terminate.

active-charging service credit-control group pending-traffic-treatment forced-reauth

Configures the Diameter Credit Control pending traffic treatment to forced reauthorization.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Group Configuration (config-group-*credit_control_group_name*)

Syntax Description `pending-traffic-treatment forced-reauth { drop | pass }`

drop

Specify to drop.

pass

Specify to pass.

Usage Guidelines Use this command to configure the Diameter Credit Control pending traffic treatment to forced reauthorization.

active-charging service credit-control group pending-traffic-treatment noquota

Configures the Diameter Credit Control Pending Traffic Treatment.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Group Configuration (config-group-*credit_control_group_name*)

Syntax Description `pending-traffic-treatment noquota { buffer | drop | pass }`

buffer

Specify to tentatively count/time traffic, and then buffer traffic pending arrival of quota. Buffered traffic will be forwarded and fully charged against the quota when the quota is eventually obtained and the traffic is passed.

drop

Specify to drop any traffic when there is no quota present.

pass

Specify to pass all traffic more or less regardless of quota state.

Usage Guidelines Controls the pass/drop treatment of traffic while waiting for definitive credit information from the server. Use this command to configure the Credit Control pending traffic treatment.

active-charging service credit-control group pending-traffic-treatment noquota limited-pass

Enables limited access for subscribers when the OCS is unreachable.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Group Configuration (config-group-*credit_control_group_name*)

Syntax Description **`pending-traffic-treatment noquota limited-pass volume`** *`volume`*

volume *volume*

Specify limited volume access to subscriber in case OCS is unreachable.

Must be an integer in the range of 1-4294967295.

Usage Guidelines Use this command to enable limited access for subscribers when the OCS is unreachable.

active-charging service credit-control group pending-traffic-treatment quota-exhausted

Configures the Diameter Credit Control Pending Traffic Treatment parameter for quota exhaustion.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Group Configuration (config-group-*credit_control_group_name*)

Syntax Description **`pending-traffic-treatment quota-exhausted { buffer | drop | pass }`**

buffer

Specify to tentatively count/time traffic, and then buffer traffic pending arrival of quota. Buffered traffic will be forwarded and fully charged against the quota when the quota is eventually obtained and the traffic is passed.

drop

Specify to drops any traffic when there is no quota present.

pass

Specify to pass all traffic more or less regardless of quota state.

Usage Guidelines Use this command to configure the Diameter Credit Control Pending Traffic Treatment for quota exhaustion.

active-charging service credit-control group pending-traffic-treatment trigger

Configures the Diameter Credit Control pending traffic treatment to trigger.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Group Configuration (config-group-*credit_control_group_name*)

Syntax Description `pending-traffic-treatment trigger { drop | pass }`

drop

Specify to drop.

pass

Specify to pass.

Usage Guidelines Use this command to configure the Diameter Credit Control pending traffic treatment to trigger.

active-charging service credit-control group pending-traffic-treatment validity-expired

Configures the Diameter Credit Control pending traffic treatment to validity-expired.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Group Configuration (config-group-*credit_control_group_name*)

Syntax Description `pending-traffic-treatment validity-expired { drop | pass }`

drop

Specify to drop.

pass

Specify to pass.

Usage Guidelines Use this command to configure the Diameter Credit Control pending traffic treatment to validity-expired.

active-charging service credit-control group quota holding-time

Configures the Credit Control Quota Holding Time (QHT).

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Configuration (config-group-*credit_control_group_name*)

Syntax Description **`quota holding-time`** *`holding_time`*

holding-time *holding_time*

Specify the quota holding time in seconds.

Must be an integer in the range of 1-4000000000.

Usage Guidelines This command configures the time-based quotas in the prepaid credit control service. Use this command to configure the Credit Control Quota Holding Time.

active-charging service credit-control group quota request-trigger

Configures Credit Control include/exclude packet causing threshold.

Syntax Description **`quota request-trigger { exclude-packet-causing-trigger | include-packet-causing-trigger }`**

exclude-packet-causing-trigger

Specify to exclude packet causing trigger.

include-packet-causing-trigger

Specify to include packet causing trigger.

Usage Guidelines This command sets the time-based quotas in the prepaid credit control service. Use this command to configure the Credit Control include/exclude packet causing threshold.

active-charging service credit-control group timestamp-rounding

Configures the timestamp rounding mechanism for quota consumption.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Group Configuration (config-group-*credit_control_group_name*)

Syntax Description **`timestamp-rounding`** *`timestamp_rounding_mechanism`*

timestamp-rounding *timestamp_rounding_mechanism*

Specify the timestamp rounding mechanism for quota consumption.

Must be one of the following:

- **ceiling**: Specify to round off to the smallest integer greater than the fraction.
- **floor**: Specify to always discard the fraction.
- **roundoff**: If the fractional part is greater than or equal to 0.5, specify to round off to the smallest integer greater than the fraction.

Usage Guidelines Use this command to configure the timestamp rounding mechanism for quota consumption.

active-charging service credit-control group usage-reporting quotas-to-report based-on-grant

Configures the ACS Credit Control usage reporting type.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Credit Control Group Configuration (config-group-*credit_control_group_name*)

Syntax Description

```
usage-reporting quotas-to-report based-on-grant [
report-only-granted-volume ]
```

report-only-granted-volume

Suppresses the input and output octets. If the Granted-Service-Unit (GSU) AVP comes with CC-Total-Octets, then the device will send total, input and output octets in Used-Service-Unit (USU) AVP. If it comes with Total-Octets, the device will send only Total-Octets in USU.

Usage Guidelines Use this command to configure reporting usage only for granted quota. On issuing this command, the Used-Service-Unit AVP will report quotas based on grant i.e, only the quotas present in the Granted-Service-Unit AVP. With this command only the units for which the quota was granted by the DCCA server will be reported irrespective of the reporting reason.

active-charging service group-of-ruledefs

Configures ACS group-of-ruledefs parameters.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Group of Ruledefs Configuration (config-group-of-ruledefs-*group_name*)

Syntax Description

```
group-of-ruledefs group_of_ruledefs_name
```

group-of-ruledefs *group_of_ruledefs_name*

Specify name of the group-of-ruledefs.

Must be a string.

Usage Guidelines Use this command to create/configure a group-of-ruledefs. A group-of-ruledefs is a collection of ruledefs to use in access policy creation. Maximum of 384 group-of-ruledefs can be created.

You can configure a maximum of 384 elements with this command.

Example

The following command creates a group-of-ruledefs named group1:

```
group-of-ruledefs group1
```

active-charging service group-of-ruledefs add-ruledef priority

Configures the priority of the ruledef in the current group-of-ruledefs.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Group of Ruledefs Configuration (config-group-of-ruledefs-*group_name*)

Syntax Description **add-ruledef priority** *ruledef_priority* **ruledef** *ruledef_name*

priority *ruledef_priority*

Specify the priority of the ruledef. The priority must be unique within the group-of-ruledefs.

Must be an integer in the range of 1-10000.

ruledef *ruledef_name*

Specify name of the ruledef to add to the current group-of-ruledefs.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to add ruledefs to a group-of-ruledefs, and configure the priority of the ruledef in the current group-of-ruledefs. A maximum of 512 ruledefs can be added to a group of ruledefs.

You can configure a maximum of 512 elements with this command.

active-charging service p2p-detection attribute ssl-renegotiation

Specify the supported attribute of configurable P2P detection attributes populated from the currently loaded P2P plugin.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*)

Syntax Description **p2p-detection attribute ssl-renegotiation { [id-reduce-factor** *id_reduce_factor* **] [max-entry-per-sessmgr** *max_entry_per_sessmgr* **] }**

id-reduce-factor *id_reduce_factor*

Specify by what factor the SSL ID is stored in the SSL Session ID Tracker table.

Must be an integer in the range of 0-65535.

max-entry-per-sessmgr *max_entry_per_sessmgr*

Specify maximum SSL Session IDs tracked per session manager.

Must be an integer in the range of 0-65535.

Usage Guidelines

Configures the detection of SSL renegotiation flows. Use this command to specify the supported attribute of configurable P2P detection attributes populated from the currently loaded P2P plugin.

Example

The following command enables SSL renegotiation with SSL session IDs as 40000 and factor as 4:

```
p2p-detection attribute ssl-renegotiation max-entry-per-sessmgr 40000 id-reduce-factor 4
```

active-charging service p2p-detection ecs-analysis

Enables or disables ACS analysis for all or specified analyzer.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*)

Syntax Description

`p2p-detection ecs-analysis` *`analyzer`*

ecs-analysis *analyzer*

Specify the ACS analyzers.

Must be one of the following:

- **all**: ACS analysis for all analyzers.
- **ftp**: ACS analysis for FTP analyzer.
- **http**: ACS analysis for HTTP analyzer.
- **https**: ACS analysis for HTTPS analyzer.
- **rtsp**: ACS analysis for RTSP analyzer.
- **sip**: ACS analysis for SIP analyzer.

Usage Guidelines

Use this command to enable or disable ACS analysis for analyzers. This feature is enabled by default if P2P protocols are enabled.

Example

The following command enables ACS analysis for the FTP analyzer:

```
p2p-detection ecs-analysis ftp
```

active-charging service p2p-detection protocol

Enables or disables the detection of all or specified peer-to-peer (P2P) protocols.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*)

Syntax Description **p2p-detection protocol** *p2p_protocol*

protocol *p2p_protocol*

Specify the P2P protocol.

Must be one of the following:

- **all**
- **cisco-jabber**
- **eros**
- **fasttrack**
- **googlemaps**
- **skype**
- **teamspeak**
- **uber**
- **ufc**
- **yahoo**

Usage Guidelines Use this command to configure detection of all or specified P2P protocol.

Example

The following command enables detection of all P2P protocols:

```
p2p-detection protocol all
```

active-charging service packet-filter

Configures ACS Packet Filter parameters.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*)

Syntax Description **packet-filter** *packet_filter_name*

direction *direction*

Specify the direction in which the current packet filter will be applied.

Must be one of the following:

- **bi-directional**: Specify to apply the filter both in the uplink and downlink directions. This is the default value.
- **downlink**: Specify to apply the filter only in the downlink direction.
- **uplink**: Specify to apply the filter only in the uplink direction.

Default Value: bi-directional.

packet-filter *packet_filter_name*

Specify name of the packet filter.

Must be a string of 1-63 characters.

priority *priority*

Specify the priority of the packet filter.

Must be an integer in the range of 0-255.

Usage Guidelines Use this command to configure ACS Packet Filter parameters.

active-charging service packet-filter ip local-port operator

Configures the port number of the local or remote transport protocol.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Packet Filter Configuration (config-service-packet-filter-*packet_filter_name*)

Syntax Description **`ip local-port`** *`operator port_number`*

Syntax Description **`ip remote-port`** *`operator port_number`*

operator

Specify how to match.

Must be one of the following:

- **=**: Equals.

port_number

Specify the port number of the transport protocol.

Must be an integer in the range of 0-65535.

Usage Guidelines Configures the IP 5-tuple port(s) for the current packet filter. Use this command to configure the port number of the local or remote transport protocol.

active-charging service packet-filter ip local-port range

Configures a range of port numbers of the local or remote transport protocol.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Packet Filter Configuration (config-service-packet-filter-*packet_filter_name*)

Syntax Description **ip local-port range** *start_port_number* **to** *end_port_number*

Syntax Description **ip remote-port range** *start_port_number* **to** *end_port_number*

to *end_port_number*

Specify the ending port number for the port number range. The ending port number must be greater than the starting port number.

Must be an integer in the range of 0-65535.

start_port_number

Specify the starting port number for the port number range. The starting port number must be lesser than the ending port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure a range of port number of the local or remote transport protocol.

active-charging service packet-filter ip protocol

Configures the IP protocol(s) for the current packet filter.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Packet Filter Configuration (config-service-packet-filter-*packet_filter_name*)

Syntax Description **ip protocol** *operator protocol_number*

operator

Specify how to match.

Must be one of the following:

- =: Equals.

protocol_number

Specify the protocol number.

Must be an integer in the range of 0-255.

Usage Guidelines

Configures the IP 5-tuple local port(s) for the current packet filter. Use this command to configure the protocol(s) for a packet filter.

Example

The following command configures the protocol assignment number 300:

```
ip protocol = 300
```

active-charging service packet-filter ip remote-address

Configures the IP remote address(es) for the current packet filter.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Packet Filter Configuration (config-service-packet-filter-*packet_filter_name*)

Syntax Description

ip remote-address *operator ip_address/mask*

ip_address_mask

Specify the IP address and mask.

Must be a string in the ipv4-prefix pattern. For information on the ipv4-prefix pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-prefix pattern. For information on the ipv6-prefix pattern, see the *Input Pattern Types* chapter.

operator

Specify how to match.

Must be one of the following:

- **=**: Equals.

Usage Guidelines

Configures the IP 5-tuple local port(s) for the current packet filter. Use this command to configure the remote address(es) for a packet filter.

Example

The following command configures the IP remote address as 10.2.3.4/24:

```
ip remote-address = 10.2.3.4/24
```

active-charging service packet-filter ip remote-port operator

Configures the port number of the local or remote transport protocol.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Packet Filter Configuration (config-service-packet-filter-*packet_filter_name*)

Syntax Description **ip local-port** *operator port_number*

Syntax Description **ip remote-port** *operator port_number*

operator

Specify how to match.

Must be one of the following:

- =: Equals.

port_number

Specify the port number of the transport protocol.

Must be an integer in the range of 0-65535.

Usage Guidelines Configures the IP 5-tuple port(s) for the current packet filter. Use this command to configure the port number of the local or remote transport protocol.

active-charging service packet-filter ip remote-port range

Configures a range of port numbers of the local or remote transport protocol.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Packet Filter Configuration (config-service-packet-filter-*packet_filter_name*)

Syntax Description **ip local-port range** *start_port_number* **to** *end_port_number*

Syntax Description **ip remote-port range** *start_port_number* **to** *end_port_number*

to *end_port_number*

Specify the ending port number for the port number range. The ending port number must be greater than the starting port number.

Must be an integer in the range of 0-65535.

start_port_number

Specify the starting port number for the port number range. The starting port number must be lesser than the ending port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure a range of port number of the local or remote transport protocol.

active-charging service packet-filter ip tos-traffic-class

Configures the type of service (TOS) traffic class under charging action in the Packet filter mode.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Packet Filter Configuration (config-service-packet-filter-*packet_filter_name*)

Syntax Description **ip tos-traffic-class** *tos_traffic_class_operator traffic_class* **mask** *mask_operator mask_field_value*

mask *mask_operator*

Specify how to match the specified mask.

Must be one of the following:

- =: Equals.

mask_field_value

Specify the traffic-class mask field.

Must be an integer in the range of 0-255.

tos_traffic_class_operator

Specify how to match the specified TOS Traffic Class.

Must be one of the following:

- =: Equals.

traffic_class

Specify the traffic class value to filter the traffic.

Must be an integer in the range of 0-255.

Usage Guidelines Use this command to configure the TOS traffic class under charging action in the Packet filter mode.

active-charging service rulebase

Configures ACS rulebases.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*)

Syntax Description **rulebase** *rulebase_name* **[retransmissions-counted | transactional-rule-matching]**

retransmissions-counted { false | true }

Specify whether to count retransmissions in all charging modules.

Must be one of the following:

- **false**
- **true**

Default Value: true.

rulebase *rulebase_name*

Specify name of the rulebase. If the named rulebase does not exist, it is created, and the CLI mode changes to the ACS Rulebase Configuration Mode wherein the rulebase can be configured. If the named rulebase already exists, the CLI mode changes to the ACS Rulebase Configuration Mode for that rulebase.

Must be a string.

transactional-rule-matching

Specify to enable or disable transactional rule matching (TRM), which allows the ACS to bypass per-packet rule matching on a transaction once the transaction is fully classified.

Usage Guidelines

Use this command to create/configure an ACS rulebase. A rulebase is a collection of protocol rules to match a flow and associated actions to be taken for matching flow. The default rulebase is used when a subscriber/APN is not configured with a specific rulebase to use.

Example

The following command creates a rulebase named test1:

```
rulebase test1
```

active-charging service rulebase action

Configures the action priority for a ruledef or group-of-ruledefs in the current rulebase.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description

`action priority` *`action_priority`* **`{ dynamic-only | static-and-dynamic | timedef`** *`timedef_name`* **`}`**

Usage Guidelines

Use this command to configure action priorities for ruledefs / group-of-ruledefs in a rulebase. This CLI command can be entered multiple times to specify multiple ruledefs and charging actions. The ruledefs are examined in priority order, until a match is found and the corresponding charging action is applied.

Example

The following command assigns a rule and action with the action priority of 23, a ruledef named test, and a charging action named test1 to the current rulebase:

```
action priority 23 ruledef test charging-action test1
```

active-charging service rulebase action priority

Configures priority for the specified ruledef or group-of-ruledefs in the current rulebase.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **priority** *action_priority*

priority *action_priority*

Specify the action priority.

Must be an integer in the range of 1-65535.

Usage Guidelines Use this command to assign priority to a rule in a rulebase.

active-charging service rulebase action priority dynamic-only

Enables matching of dynamic rules with static rules for this action priority on a flow.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **dynamic-only**

Usage Guidelines Use this command to enable matching of dynamic rules with static rules for this action priority on a flow.

active-charging service rulebase action priority dynamic-only adc group-of-ruledefs

Assigns a group-of-ruledefs to the rulebase.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **adc ruledef** *ruledef_name* **{ [charging-action** *charging_action_name* **] [description** *description* **] [monitoring-key** *monitoring_key* **] [umid** *instance_id* **] }**

Syntax Description **ruledef** *ruledef_name* **{ [charging-action** *charging_action_name* **] [description** *description* **] [monitoring-key** *monitoring_key* **] [umid** *instance_id* **] }**

charging-action *charging_action_name*

Assigns the specified charging action to the rulebase.

Must be a string of 1-63 characters.

description *description*

Adds specified text to the rule and action.

Must be a string of 1-63 characters.

group-of-ruledefs *group_of_ruledefs_name*

Specify name of the group-of-ruledefs.

Must be a string of 1-63 characters.

monitoring-key *monitoring_key*

Associates the specified monitoring-key with ruledefs for usage monitoring.

Must be an integer in the range of 1-134217727.

umid *um_id*

Specify the Usage Monitoring Control Instance Identifier as required for usage reporting over N7.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to assign a group-of-ruledefs to the rulebase.

active-charging service rulebase action priority dynamic-only adc ruledef

Assigns ruledefs to the rulebase.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **ruledef** *ruledef_name* **{ [charging-action** *charging_action_name* **] [description** *description* **] [monitoring-key** *monitoring_key* **] [umid** *instance_id* **] }**

charging-action *charging_action_name*

Assigns the specified charging action to the rulebase.

Must be a string of 1-63 characters.

description *description*

Adds specified text to the rule and action.

Must be a string of 1-63 characters.

monitoring-key *monitoring_key*

Associates the specified monitoring-key with ruledefs for usage monitoring.

Must be an integer in the range of 1-134217727.

ruledef *ruledef_name*

Specify name of the ruledef.

Must be a string of 1-63 characters.

umid *um_id*

Specify the Usage Monitoring Control Instance Identifier as required for usage reporting over N7.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to assign ruledefs to the rulebase.

active-charging service rulebase action priority dynamic-only group-of-ruledefs

Assigns a group-of-ruledefs to the rulebase.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **adc ruledef** *ruledef_name* **{ [charging-action** *charging_action_name* **] [description** *description* **] [monitoring-key** *monitoring_key* **] [umid** *instance_id* **] }**

Syntax Description **ruledef** *ruledef_name* **{ [charging-action** *charging_action_name* **] [description** *description* **] [monitoring-key** *monitoring_key* **] [umid** *instance_id* **] }**

charging-action *charging_action_name*

Assigns the specified charging action to the rulebase.

Must be a string of 1-63 characters.

description *description*

Adds specified text to the rule and action.

Must be a string of 1-63 characters.

group-of-ruledefs *group_of_ruledefs_name*

Specify name of the group-of-ruledefs.

Must be a string of 1-63 characters.

monitoring-key *monitoring_key*

Associates the specified monitoring-key with ruledefs for usage monitoring.

Must be an integer in the range of 1-134217727.

umid *um_id*

Specify the Usage Monitoring Control Instance Identifier as required for usage reporting over N7.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to assign a group-of-ruledefs to the rulebase.

active-charging service rulebase action priority dynamic-only ruledef

Assigns ruledefs to the rulebase.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **ruledef** *ruledef_name* **{ [charging-action** *charging_action_name* **] [description** *description* **] [monitoring-key** *monitoring_key* **] [umid** *instance_id* **] }**

charging-action *charging_action_name*

Assigns the specified charging action to the rulebase.

Must be a string of 1-63 characters.

description *description*

Adds specified text to the rule and action.

Must be a string of 1-63 characters.

monitoring-key *monitoring_key*

Associates the specified monitoring-key with ruledefs for usage monitoring.

Must be an integer in the range of 1-134217727.

ruledef *ruledef_name*

Specify name of the ruledef.

Must be a string of 1-63 characters.

umid *um_id*

Specify the Usage Monitoring Control Instance Identifier as required for usage reporting over N7.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to assign ruledefs to the rulebase.

active-charging service rulebase action priority group-of-ruledefs

Assigns a group-of-ruledefs to the rulebase. Or, associates a time definition with a group-of-ruledefs.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **action priority** *action_priority* **static-and-dynamic group-of-ruledefs** *group_of_ruledefs_name*

Syntax Description **action priority** *action_priority* **timedef group-of-ruledefs** *group_of_ruledefs_name* **charging-action** *charging_action_name* **[description** *description* **] [monitoring-key** *monitoring_key* **]**

charging-action *charging_action_name*

Assigns the specified charging action to the rulebase.

Must be a string of 1-63 characters.

description *description*

Adds specified text to the rule and action.

Must be a string of 1-63 characters.

group-of-ruledefs *group_of_ruledefs_name*

Specify name of the group-of-ruledefs.

Must be a string of 1-63 characters.

monitoring-key *monitoring_key*

Associates the specified monitoring-key with ruledefs for usage monitoring.

Must be an integer in the range of 1-134217727.

Usage Guidelines Use this command to assign a group-of-ruledefs to the rulebase. Or, associate a time definition with a group-of-ruledefs. Timedefs activate or deactivate groups-of-ruledefs, making them available for rule matching only when they are active.

active-charging service rulebase action priority ruledef

Assigns ruledefs to the rulebase. Or, associates a time definition with a ruledef.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description

action priority *action_priority* **static-and-dynamic ruledef** *ruledef_name* **charging-action** *charging_action_name* **ruledef** *ruledef_name* **[description** *description* **] [monitoring-key** *monitoring_key* **]**

Syntax Description

action priority *action_priority* **timedef ruledef** *ruledef_name* **charging-action** *charging_action_name* **[description** *description* **] [monitoring-key** *monitoring_key* **]**

charging-action *charging_action_name*

Assigns the specified charging action to the rulebase.

Must be a string of 1-63 characters.

description *description*

Adds specified text to the rule and action.

Must be a string of 1-63 characters.

monitoring-key *monitoring_key*

Associates the specified monitoring-key with ruledefs for usage monitoring.

Must be an integer in the range of 1-134217727.

ruledef *ruledef_name*

Specify name of the ruledef.

Must be a string of 1-63 characters.

Usage Guidelines

Use this command to assign ruledefs to the rulebase. Or, associate a time definition with a ruledef. Timedefs activate or deactivate ruledefs, making them available for rule matching only when they are active.

active-charging service rulebase action priority static-and-dynamic group-of-ruledefs

Assigns a group-of-ruledefs to the rulebase. Or, associates a time definition with a group-of-ruledefs.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **action priority** *action_priority* **static-and-dynamic group-of-ruledefs** *group_of_ruledefs_name*

Syntax Description **action priority** *action_priority* **timedef group-of-ruledefs** *group_of_ruledefs_name* **charging-action** *charging_action_name* **[description** *description* **] [monitoring-key** *monitoring_key* **]**

charging-action *charging_action_name*

Assigns the specified charging action to the rulebase.

Must be a string of 1-63 characters.

description *description*

Adds specified text to the rule and action.

Must be a string of 1-63 characters.

group-of-ruledefs *group_of_ruledefs_name*

Specify name of the group-of-ruledefs.

Must be a string of 1-63 characters.

monitoring-key *monitoring_key*

Associates the specified monitoring-key with ruledefs for usage monitoring.

Must be an integer in the range of 1-134217727.

Usage Guidelines Use this command to assign a group-of-ruledefs to the rulebase. Or, associate a time definition with a group-of-ruledefs. Timedefs activate or deactivate groups-of-ruledefs, making them available for rule matching only when they are active.

active-charging service rulebase action priority static-and-dynamic ruledef

Assigns ruledefs to the rulebase. Or, associates a time definition with a ruledef.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **action priority** *action_priority* **static-and-dynamic ruledef** *ruledef_name* **charging-action** *charging_action_name* **ruledef** *ruledef_name* **[description** *description* **] [monitoring-key** *monitoring_key* **]**

Syntax Description **action priority** *action_priority* **timedef ruledef** *ruledef_name* **charging-action** *charging_action_name* **[description** *description* **] [monitoring-key** *monitoring_key* **]**

charging-action *charging_action_name*

Assigns the specified charging action to the rulebase.

Must be a string of 1-63 characters.

description *description*

Adds specified text to the rule and action.

Must be a string of 1-63 characters.

monitoring-key *monitoring_key*

Associates the specified monitoring-key with ruledefs for usage monitoring.

Must be an integer in the range of 1-134217727.

ruledef *ruledef_name*

Specify name of the ruledef.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to assign ruledefs to the rulebase. Or, associate a time definition with a ruledef. Timedefs activate or deactivate ruledefs, making them available for rule matching only when they are active.

active-charging service rulebase action priority timedef group-of-ruledefs

Assigns a group-of-ruledefs to the rulebase. Or, associates a time definition with a group-of-ruledefs.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **action priority** *action_priority* **static-and-dynamic group-of-ruledefs** *group_of_ruledefs_name*

Syntax Description **action priority** *action_priority* **timedef group-of-ruledefs** *group_of_ruledefs_name* **charging-action** *charging_action_name* **[description** *description* **] [monitoring-key** *monitoring_key* **]**

charging-action *charging_action_name*

Assigns the specified charging action to the rulebase.

Must be a string of 1-63 characters.

description *description*

Adds specified text to the rule and action.

Must be a string of 1-63 characters.

group-of-ruledefs *group_of_ruledefs_name*

Specify name of the group-of-ruledefs.

Must be a string of 1-63 characters.

monitoring-key *monitoring_key*

Associates the specified monitoring-key with ruledefs for usage monitoring.

Must be an integer in the range of 1-134217727.

Usage Guidelines

Use this command to assign a group-of-ruledefs to the rulebase. Or, associate a time definition with a group-of-ruledefs. Timedefs activate or deactivate groups-of-ruledefs, making them available for rule matching only when they are active.

active-charging service rulebase action priority timedef ruledef

Assigns ruledefs to the rulebase. Or, associates a time definition with a ruledef.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description

action priority *action_priority* **static-and-dynamic ruledef** *ruledef_name* **charging-action** *charging_action_name* **ruledef** *ruledef_name* **[description** *description* **] [monitoring-key** *monitoring_key* **]**

Syntax Description

action priority *action_priority* **timedef ruledef** *ruledef_name* **charging-action** *charging_action_name* **[description** *description* **] [monitoring-key** *monitoring_key* **]**

charging-action *charging_action_name*

Assigns the specified charging action to the rulebase.

Must be a string of 1-63 characters.

description *description*

Adds specified text to the rule and action.

Must be a string of 1-63 characters.

monitoring-key *monitoring_key*

Associates the specified monitoring-key with ruledefs for usage monitoring.

Must be an integer in the range of 1-134217727.

ruledef *ruledef_name*

Specify name of the ruledef.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to assign ruledefs to the rulebase. Or, associate a time definition with a ruledef. Timedefs activate or deactivate ruledefs, making them available for rule matching only when they are active.

active-charging service rulebase bandwidth

Configures rulebase bandwidth policy parameters.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **`bandwidth default-policy`** *`default_firewall_policy_name`*

default-policy *default_firewall_policy_name*

Specify the default firewall policy.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to configure the rulebase bandwidth policy parameter for default firewall policy.

active-charging service rulebase billing-records

Configures the type of billing to be performed for subscriber sessions.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **`billing-records { [ egcdr ] [ radius ] [ rf ] }`**

egcdr

Generates an enhanced G-CDR (eG-CDR) for GGSN / P-GW-CDR for P-GW, and/or UDR with specified format on the occurrence of an interim trigger condition at the end of a subscriber session, or an SGSN-to-SGSN handoff

radius

Generates postpaid RADIUS accounting records at the start and end of a subscriber session, and on the occurrence of an interim trigger condition. RADIUS accounting records are generated for each content ID.

rf

Specify to enable Rf accounting.

Usage Guidelines Use this command to generate enhanced G-CDRs (eG-CDRs), P-GW-CDR for P-GW, RADIUS CDRs and/or UDRs for billing records. The format of eG-CDRs for the default GTPP group is controlled by the inspector command in the Context Configuration Mode.

active-charging service rulebase billing-records udr

Generates Usage Data Record (UDR) with specified the format on the occurrence of an interim trigger condition, at the end of a subscriber session, or a handoff.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description

billing-records udr udr-format *udr_format_name*

udr-format *udr_format_name*

Specify name of the UDR format.

Must be a string of 1-63 characters.

Usage Guidelines

Use this command to enable Usage Data Record.

Example

The following command sets the billing record to UDR with UDR format named udr_format1:

```
billing-records udr udr-format udr_format1
```

active-charging service rulebase cca diameter requested-service-unit sub-avp time

Configures the ACS Diameter Credit Control Requesting Service Unit - time values.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description

cca diameter requested-service-unit sub-avp time cc-time *cc_time*

cc-time *cc_time*

Specify requested service unit for charging time duration in seconds in included sub-AVP.

Must be an integer in the range of 1-4000000000.

Usage Guidelines

Configures the Diameter sub-AVPs to be included in "Requested-Service-Unit", the Diameter group AVP sent with DCCA Credit Control Requests (CCRs). Use this command to configure the ACS Diameter Credit Control requesting service unit - time values.

active-charging service rulebase cca diameter requested-service-unit sub-avp units

Configures ACS Diameter Credit Control Requesting Service Unit - Service-specific values.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description

cca diameter requested-service-unit sub-avp units cc-service-specific-units *charging_unit*

cc-service-specific-units *charging_unit*

Specify the service-specific charging units.

Must be an integer in the range of 1-4000000000.

Usage Guidelines

Configures sub-AVP of the Requested-Service-Unit AVP. Use this command to configure the ACS Diameter Credit Control Requesting Service Unit - Service-specific values.

active-charging service rulebase cca diameter requested-service-unit sub-avp volume

Configures the ACS Diameter Credit Control Requesting Service Unit - Time values.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description

cca diameter requested-service-unit sub-avp volume { [cc-input-octets *cc_input_octets* **] [cc-output-octets** *cc_output_octets* **[cc-total-octets** *cc_total_octets* **] }**

cc-input-octets *cc_input_octets*

Specify the volume in bytes.

Must be an integer in the range of 1-4000000000.

cc-output-octets *cc_output_octets*

Specify the output charging octets in bytes.

Must be an integer in the range of 1-4000000000.

cc-total-octets *cc_total_octets*

Specify the total charging octets in bytes.

Must be an integer in the range of 1-4000000000.

Usage Guidelines Configures sub-AVP of the Requested-Service-Unit AVP. Use this command to configure the ACS Diameter Credit Control Requesting Service Unit - Time values.

active-charging service rulebase cca quota holding-time

Configures the Quota Holding Time (QHT). QHT is used with both time- and volume-based quotas.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **cca quota holding-time** *holding_time* **content-id** *content_id*

content-id *content_id*

Specify the content ID (Rating group AVP) to use for the Quota holding time for the current rulebase. Must be the content ID specified for Credit Control Service in the ACS.

Must be an integer in the range of 1-2147483647.

holding-time *holding_time*

Specify the holding time.

Must be an integer in the range of 1-4000000000.

Usage Guidelines Configures various time and threshold-based quotas in the Prepaid Credit Control Service (Credit Control Application). Use this command to configure the value for the Quota Holding Time (QHT). QHT is used with both time- and volume-based quotas. After the configured number of seconds has passed without user traffic, the quota is reported back and the charging stops until new traffic starts.

active-charging service rulebase cca quota retry-time

Configures the retry time for the quota request.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **cca quota retry-time** *retry_time* **[max-retries** *max_retries* **]**

max-retries *max_retries*

Specify the maximum number of retries allowed for blacklisted categories.

Must be an integer in the range of 1-65535.

retry-time *retry_time*

Specify the retry interval in seconds.

Must be an integer in the range of 0-86400.

Usage Guidelines Use this command to configure credit control quota retry time.

active-charging service rulebase cca quota time-duration

Configures the algorithm to compute time duration for Prepaid Credit Control Application quotas in the current rulebase.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **`cca quota time-duration algorithm { consumed-time`** *`consumed_time`* **`[ plus-idle ] | continuous-time-periods`** *`continuous_time_periods`* **`| parking-meter`** *`parking_meter`* **`} [ content-id`** *`content_id`* **`]`**

algorithm

Specify the Credit Control Quota Time Duration algorithm.

consumed-time *consumed_time*

Specify the Credit Control consumed time.

Must be an integer in the range of 1-4294967295.

content-id *content_id*

Specify the Content ID.

Must be an integer in the range of 1-2147483647.

continuous-time-periods *continuous_time_periods*

Specify the continuous time periods.

Must be an integer in the range of 1-4294967295.

parking-meter *parking_meter*

Specify the Credit Control Parking Meter.

Must be an integer in the range of 1-4294967295.

plus-idle

Specify the Credit Control idle time.

Usage Guidelines Use this command to configure the various time charging algorithms/schemes for prepaid credit control charging. If operator chooses parking-meter style charging, then time is billed in seconds chunks.

Example

The following command configures the QCT to consumed-time duration of 400 seconds:

```
cca quota time-duration algorithm consumed-time 400
```

active-charging service rulebase content-filtering category

Configures the Content Filtering Category Policy Identifier for Policy-based Content Filtering support in the current rulebase.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description

content-filtering category policy-id *cf_policy_id*

policy-id *cf_policy_id*

Specify the Content Filtering Policy ID.

Must be an integer in the range of 1-4294967295.

Usage Guidelines

Use this command to configure the Content Filtering Category Policy ID for Policy-based Content Filtering support in the rulebase.

Example

The following command configures the Content Filtering Category Policy ID 101 in the rulebase:

```
content-filtering category policy-id 101
```

active-charging service rulebase content-filtering flow-any-error

Configures the action to take on Content Filtering packets in the case of ACS error scenarios.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description

content-filtering flow-any-error { deny | permit }

deny

Specify the flow-any-error configuration as deny. All the denied packets will be accounted for by the discarded-flow-content-id configuration in the Content Filtering Policy Configuration Mode. This content ID will be used to generate UDRs for packets denied via content filtering.

permit

Specify the flow-any-error configuration as permit.

Usage Guidelines

Use this command to allow/discard content filtering packets in case of ACS error scenarios.

Example

The following command allows content filtering packets in case of an ACS error:

```
content-filtering flow-any-error permit
```

active-charging service rulebase content-filtering mode

Enables or disables the specified Category-based Content Filtering mode in the current rulebase.

Syntax Description

content-filtering mode { category { static-and-dynamic | static-only } | server-group *cf_server_group_name* **}**

category { static-and-dynamic | static-only }

Using Category-based Content Filtering support requires Content Filtering Category configuration in the Global Configuration Mode.

Must be one of the following:

- **static-and-dynamic**: Configures Category-based Content Filtering in Static-and-Dynamic mode, wherein a static rating of the URL is first performed, and only if the static rating fails to find a match, dynamic rating of the content that the server returns is then performed.
- **static-only**: Configures Category-based Content Filtering in static only mode, wherein all URLs are compared against an internal database to categorize the requested content.

server-group *server_group_name*

Specify name of the Content Filtering Server Group.

Must be a string of 1-63 characters.

Usage Guidelines

Use this command to enable and apply the content filtering mode in the rulebase to manage a content filtering server with an ICAP client system.

Example

The following command enables the content filtering mode for external content filtering server group cf_server1 in the rulebase:

```
content-filtering mode server-group cf_server1
```

active-charging service rulebase credit-control-group

Configures the credit control group to be used for subscribers who use this rulebase.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **credit-control-group** *cc_group_name*

credit-control-group *cc_group_name*

Specify name of the credit control group.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to specify the desired CC group whenever the rulebase is selected during the subscriber session setup. This is an optional CLI configuration, and used only when customized Assume Positive behavior is required for subscribers. This CLI configuration is applicable only during the session setup. Mid-session change in the CC group is not allowed.

Example

The following command configures the association of a credit-control group named test for the current rulebase:

```
credit-control-group test
```

active-charging service rulebase dynamic-rule

Configfures whether dynamic rules are matched before statically configured rules.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **dynamic-rule order** *dynamic_rule_order*

order *dynamic_rule_order*

Specify dynamic rule order.

Must be one of the following:

- **always-first**: Specify to match all the dynamic rules against the flow prior to any static rule. This is the default value.
- **first-if-tied**: Specify to match rules against the flow based on their priority with the condition that dynamic rules match before a static rule of the same priority. A rule is a combination of a ruledef, charging action, and precedence. Static rules are defined by the "action" CLI command in the ACS Rulebase Configuration Mode, and are applicable to all subscribers that are associated with the rulebase. Dynamic rules are obtained via a dynamic protocol, such as, the Gx-interface for a particular subscriber session.

Usage Guidelines Use this command to configure the order in which rules are selected for matching in between dynamic rules (per subscriber) and static rules (from rulebase).

Example

The following command matches all dynamic rules against the flow prior to any static rule:

```
dynamic-rule order always-first
```

active-charging service rulebase edr transaction-complete

Configures EDR-related parameters.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description

edr transaction-complete { dns | http } [charging-edr *charging_edr_format_name* **| edr-format** *edr_format_name* **| reporting-edr** *reporting_edr_format_name* **]**

charging-edr *charging_edr_format_name*

Specify to generate charging EDR on transaction completion.

Must be a string of 1-63 characters.

dns

DNS protocol-related configuration.

edr-format *edr_format_name*

Specify to generate EDR on transaction completion for DNS or HTTP protocol.

Must be a string of 1-63 characters.

http

HTTP protocol-related configuration.

reporting-edr *reporting_edr_format_name*

Specify the reporting EDR format name to generate reporting EDR on transaction completion.

Must be a string of 1-63 characters.

Usage Guidelines

Configures the generation of an EDR on the completion of a transaction. Use this command to configure the generation of an EDR when certain application transactions (for example, request/response pairs) complete. EDR generation is supported for DNS or HTTP protocol. Note that these EDRs are in addition to those that might be generated due to other conditions, for example, EDR configurations in a charging action.

Example

The following command configures the generation of charging EDRs on the completion of transactions for HTTP protocol specifying the EDR format as test123:

```
edr transaction-complete http charging-edr test123
```

active-charging service rulebase egcdr threshold

Assigns volume or interval values to the interim G-CDRs.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **egcdr threshold interval** *duration*

interval *duration*

Specify the time interval, in seconds, for closing the G-CDR/PGW-CDR if the minimum time duration thresholds are satisfied.

Must be an integer in the range of 60-40000000.

Usage Guidelines Configures the thresholds for generating eG-CDRs for GGSN and PGW-CDRs for P-GW. Use this command to assign the interval values to the interim G-CDRs.

Example

The following command defines an eG-CDR threshold interval of 600 seconds:

```
egcdr threshold interval 600
```

active-charging service rulebase egcdr threshold volume

Configures the uplink/downlink volume octet counts for the generation of the interim G-CDRs/PGW-CDRs.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **egcdr threshold volume { downlink | total | uplink }** *bytes*

downlink *bytes*

Specify the limit for the number of downlink (from network to subscriber) octets after which the G-CDR/PGW-CDR is closed.

Must be an integer in the range of 100000-4000000000.

total *bytes*

Specify the limit for the total number of octets (uplink+downlink) after which the G-CDR/PGW-CDR is closed.

Must be an integer in the range of 100000-4000000000.

uplink *bytes*

Specify the limit for the number of uplink (from subscriber to network) octets after which the G-CDR/PGW-CDR is closed.

Must be an integer in the range of 100000-4000000000.

Usage Guidelines Configures the thresholds for generating G-CDRs and PGW-CDRs. Use this command to configure the uplink/downlink volume octet counts for the generation of the interim G-CDRs.

active-charging service rulebase flow control-handshaking

Specify control protocol handshake packets.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description

```
flow control-handshaking charge-separate-from-application
```

charge-separate-from-application

Specify the charging action to separate the charging of the initial control packets or all subsequent control packets from regular charging.

Usage Guidelines

Configures the charge for the control traffic associated with an application. Use this command to specify control protocol handshake packets.

active-charging service rulebase flow control-handshaking charge-to-application

Configures the charging action to include the flow control packets either during initial handshaking only or specified control packets during session for charging.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description

```
flow control-handshaking charge-to-application { [ all-packets ] [
initial-packets ] [ mid-session-packets ] [ tear-down-packets ] }
```

all-packets

Specify that the initial setup packets will wait until the application has been determined before assigning the content-id, and all mid-session ACK packets as well as the final tear-down packets will use that content-id.

initial-packets

Specify that only the initial setup packets will wait for content-id assignment.

mid-session-packets

Specify that the ACK packets after the initial setup will use the application's or content-id assignment.

tear-down-packets

Specify that the final tear-down packets (TCP or WAP) will use the application's or content-id assignment.

Usage Guidelines

Use this command to charge control packets to application ruledefs.

active-charging service rulebase flow end-condition

Configures the end condition of the session flows related to a user session and triggers EDR generation.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description

flow end-condition { normal-end-signaling | session-end | timeout } [charging-edr *charging_edr_format_name* **]**

charging-edr *charging_edr_format_name*

Specify name of the charging EDR format.

Must be a string of 1-63 characters.

normal-end-signaling

Creates an EDR with the specified EDR format whenever flow end is signaled normally, for example like detecting FIN and ACK for a TCP flow, or a WSP-DISCONNECT terminating a connection-oriented WSP flow over UDP) and create an EDR for the flow using the specified EDR format.

session-end

Creates an EDR with the specified EDR format whenever a subscriber session ends. By this option ACS creates an EDR with the specified format name for every flow that has had any activity since last EDR was created for the flow on session end.

timeout

Creates an EDR with the specified EDR format whenever a flow ends due to a timeout condition.

Usage Guidelines

Use this command to enable or disable the capturing of EDRs based on flow end condition.

active-charging service rulebase flow limit-across-applications

This command allows you to limit the total number of simultaneous flows per Subscriber/APN sent to a rulebase regardless of the flow type, or limit flows based on the protocol type under the Session Control feature.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description

flow limit-across-applications { *limit* **| non-tcp** *non_tcp_limit* **| tcp** *tcp_limit* **}**

non-tcp *non_tcp_limit*

Specify the maximum limit of non-TCP type flows.

Must be an integer in the range of 1-4000000000.

tcp *tcp_limit*

Specify the maximum limit of TCP flows.

Must be an integer in the range of 1-4000000000.

limit

Specify the maximum limit.

Must be an integer in the range of 1-4000000000.

Usage Guidelines Use this command to limit the total number of flows allowed per subscriber for a rulebase regardless of flow type, or limit flows based on the protocol non-TCP (connection-less) or TCP (connection-oriented).

Example

The following command configures the maximum number of 200000 flows for the rulebase:

```
flow limit-across-applications 200000
```

active-charging service rulebase ip

Configures IP parameters related to user session.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **ip reassembly-timeout** *reassembly_timeout*

reassembly-timeout *reassembly_timeout*

Specify the maximum duration for which ip packet fragments are retained, in milliseconds.

Must be an integer in the range of 100-30000.

Default Value: 5000.

Usage Guidelines Use this command to configure IP parameters related to user session.

active-charging service rulebase p2p

Enables or disables the P2P analyzer to detect peer-to-peer (P2P) applications.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **p2p dynamic-flow-detection**

dynamic-flow-detection

Enables dynamic-flow detection, allowing the P2P analyzer to detect the P2P applications configured for the ACS.

Usage Guidelines Use this command to enable/disable the P2P analyzer to detect peer-to-peer (P2P) applications.

active-charging service rulebase post-processing priority

Configures the post-processing priority of a specific ruledef in the current rulebase.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **post-processing priority** *post_processing_priority*

priority *post_processing_priority*

Specify the post-processing priority.

Must be an integer in the range of 1-65535.

Usage Guidelines Use this command to configure the post-processing priority of a specific ruledef in the current rulebase.

Example

The following command configures the ruledef named test_ruledef with a priority of 10:

```
post-processing priority 10
```

active-charging service rulebase post-processing priority group-of-ruledefs

Configures group-of-ruledefs parameters.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **post-processing priority** *post_processing_priority* **group-of-ruledefs** *group_of_ruledefs_name* **charging-action** *charging_action* **[description** *description* **]**

charging-action *charging_action_name*

Specify name of the charging action.

Must be a string of 1-63 characters.

description *description*

Specify an optional description for this configuration.

Must be a string of 1-63 characters.

group-of-ruledefs *group_of_ruledefs_name*

Specify name of the group-of-ruledefs.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to configure group-of-ruledefs parameters.

active-charging service rulebase post-processing priority ruledef

Assigns ruledefs to the current rulebase.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **post-processing priority** *post_processing_priority* **ruledef** *ruledef_name* **charging-action** *charging_action_name* **[description** *description* **]**

charging-action *charging_action_name*

Specify name of the charging action.

Must be a string of 1-63 characters.

description *description*

Specify an optional description for this configuration.

Must be a string of 1-63 characters.

ruledef *ruledef_name*

Specify name of the ruledef.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to assign ruledefs to the current rulebase.

active-charging service rulebase route priority

Configures the priority of the route in the rulebase.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **priority** *route_priority*

priority *route_priority*

Specify the route priority.

Must be an integer in the range of 0-65535.

Usage Guidelines Configures the routing of packets to protocol analyzers. Use this command to configure the priority of the route in the rulebase.

active-charging service rulebase route priority ruledef

Configures the ruledef to evaluate packets to determine analyzer.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **route priority** *route_priority* **ruledef** *ruledef_name* **analyzer** *analyzer*

analyzer *analyzer*

Specify the analyzer for the ruledef.

Must be one of the following:

- **dns**: Route to DNS protocol.
- **file-transfer**: Route to file analyzer.
- **ftp-control**: Route to FTP Control protocol.
- **ftp-data**: Route to FTP Data protocol.
- **h323**: Route to H323 protocol.
- **http**: Route to HTTP protocol.
- **imap**: Route to IMAP protocol analyzer.
- **mipv6**: Route to MIPv6 protocol analyzer.
- **mms**: Route to MMS protocol analyzer.
- **pop3**: Route to POP3 protocol analyzer.
- **pptp**: Route to PPTP protocol analyzer.
- **radius**: Route to light-weight RADIUS protocol analyzer.
- **rtcp**: Route to RTCP protocol analyzer.
- **rtp**: Route to RTP protocol analyzer.
- **rtsp**: Route to RTSP protocol analyzer.
- **sdp**: Route to SDP protocol analyzer.

- **secure-http**: Route to secure HTTP protocol analyzer.
- **sip**: Route to SIP protocol analyzer.
- **smtp**: Route to SMTP protocol analyzer.
- **tftp**: Route to TFTP protocol analyzer.
- **wsp-connection-less**: Route to WSP connection-less protocol analyzer.
- **wsp-connection-oriented**: Route to WSP connection-oriented protocol analyzer.

description *description*

Specify to add a description to the rule and action in the saved configuration file for later reference.

Must be a string of 1-31 characters.

ruledef *ruledef_name*

Specify name of the ruledef.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to assign a ruledef to a rulebase,

active-charging service rulebase rtp

Configures the Real Time Streaming Protocol (RTSP) and Session Description Protocol (SDP) analyzers to detect the start/stop of RTP and RTCP flows.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description `rtp dynamic-flow-detection`

dynamic-flow-detection

Specify to enable dynamic RTP/RTCP flow detection.

Usage Guidelines Use this command to enable the RTSP and SDP analyzers to detect the start/stop of RTP and RTCP flows. This command is used in conjunction with the route priority command.

active-charging service rulebase tcp

Configures TCP window size checking.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description `tcp check-window-size`

check-window-size

Specify to enable TCP window-size checking.

Usage Guidelines

Use this command to enable/disable TCP window-size check for packets out of TCP window.

Example

The following command enables TCP window-size check:

```
tcp check-window-size
```

active-charging service rulebase tcp mss

Configures the TCP Maximum Segment Size (MSS) in TCP SYN packets.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description

`tcp mss` *`tcp_mss`* **`{ [ add-if-not-present ] [ limit-if-present ] }`**

add-if-not-present

Specify to add the TCP MSS if not present in the packet.

limit-if-present

Specify to limit the TCP MSS if present in the packet.

mss *tcp_mss*

Specify the TCP MSS.

Must be an integer in the range of 496-65535.

Usage Guidelines

Using this command, TCP MSS can be limited if already present in the TCP SYN packets. If there are no errors detected in IP header/TCP mandatory header and there are no memory allocation failures, TCP optional header is parsed. If TCP MSS is present in the optional header and its value is greater than the configured MSS value, the value present in the TCP packet is replaced with the configured one.

Example

The following command limits the TCP maximum segment size to 3000, and if not present adds it to the packets:

```
tcp mss 3000 limit-if-present add-if-not-present
```

active-charging service rulebase tcp packets-out-of-order

Configures processing of TCP packets that are out of order, while waiting for the earlier packet(s) to arrive.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **`tcp packets-out-of-order timeout`** *`timeout_duration`*

timeout *timeout_duration*

Specify the timeout duration for re-assembly of TCP out-of-order packets in milliseconds.

Must be an integer in the range of 100-30000.

Default Value: 5000.

Usage Guidelines Use this command to configure how to process TCP packets that are out of order, while waiting for the earlier packet(s) to arrive.

Example

The following command sets the timeout timer to 10000 milliseconds:

```
tcp packets-out-of-order timeout 10000
```

active-charging service rulebase tcp packets-out-of-order transmit

Configures the TCP out-of-order segment behavior after buffering a copy.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **`tcp packets-out-of-order transmit`** *`transmit_behavior`*

transmit *transmit_behavior*

Specify the TCP out-of-order segment behavior after buffering a copy.

Must be one of the following:

- **after-reordering**: Specify to deliver the TCP out-of-order segments in-sequence to the ACS analyzer after all packets are received and successfully reordered. The "after-reordering" option is doing this by buffering out-of-order packets, and only releasing them after the missing out-of-order packets are received (or after OOO timeout). When the missing packet is received, complete deep packet inspection of all the packets and all relevant in-line services is done, and then the last packet is forwarded (as the latest). If reordering is not successful within the specified OOO timeout, all the subsequent received packets in that TCP flow are forwarded without being passed through the analysers (except the L3/L4 analyzer). As a consequence, only L3/L4 rule matching will take place. If memory allocation fails or the received packet is partial retransmitted data, the packet will also be forwarded immediately without being passed through the protocol analyzers, except for the L3/L4 analyzers.
- **immediately**: Specify to deliver the TCP out-of-order segments in-sequence to the ACS analyzer after all packets are received and successfully reordered. The "immediately" option is accomplishing this by

making a copy of out-of-order packets, and buffering those, while transmitting the original data packets through the outgoing interface immediately. When the missing packet is received, complete deep packet inspection of all the packets and all relevant in-line services is done, and then the last packet is forwarded. If reordering of the buffered packets is not successful within the specified OOO timeout, all the subsequent received packets in that TCP flow are forwarded without being passed through the analysers (except the L3/L4 analyzer). As a consequence only L3/L4 rule matching will take place. If memory allocation fails or the received packet is partial retransmitted data, the packet will also be forwarded immediately without being passed through the protocol analyzers, except for the L3/L4 analysers.

Usage Guidelines Use this command to configure the TCP out-of-order segment behavior after buffering a copy.

active-charging service rulebase tethering-detection

Enables or disables the Tethering Detection feature for the current rulebase, and specifies the database to use.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **`tethering-detection { application | dns-based | ip-ttl-value`** *`ttl_value`* **`| max-syn-packet-in-flow`** *`max_syn_packets`* **`|`** *`tethering_database`* **`}`**

application

Specify to perform tethering detection based on App-based method.

dns-based

Specify to perform tethering detection based on DNS-based method.

max-syn-packet-in-flow *max_syn_packets*

Specify the number of SYN packets applicable for tethering detection in a flow.

Must be an integer in the range of 1-3.

tethering_database

Specify to perform tethering detection using the specified database.

Must be one of the following:

- **os-db-only**: Specify to perform tethering detection using IPv4 and IPv6 OS signature databases.
- **os-ua-db**: Specify to perform tethering detection using IPv4 OS, IPv6 OS, and UA signature databases.
- **ua-db-only**: Specify to perform tethering detection using only the UA signature database.

Usage Guidelines Use this command to enable/disable the Tethering Detection feature for a rulebase, and configures the database to use. Tethering Detection can be done for IPv4, IPv6, TCP and UDP flows.

Example

The following command enables the Tethering Detection feature in the rulebase, and specifies to use only the OS database:

```
tethering-detection os-db-only
```

active-charging service rulebase url-blacklisting action

Configures URL Blacklisting action.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description

`url-blacklisting action { discard | redirect-url` *`redirect_url`* **`| terminate-flow | www-reply-code-and-terminate-flow`** *`reply_code`* **`} [ content-id`** *`content_id`* **`]`**

content-id *content_id*

Specify the content ID, a number assigned to URL Blacklisting.

Must be an integer in the range of 1-65535.

discard

Specify the URL Blacklisting action as "discard".

redirect-url *redirect_url*

Specify the redirect URL/URI, which must be a fully qualified URL/URI.

Must be a string.

terminate-flow

Specify the URL Blacklisting action as "terminate-flow".

www-reply-code-and-terminate-flow *reply_code*

Specify the URL Blacklisting action as "terminate-flow action with reply code".

Must be an integer in the range of 400-599.

Usage Guidelines

Enables or disables URL Blacklisting functionality for the current rulebase, and configures the action to be taken when there is a URL match. Use this command to configure the URL Blacklisting action.

active-charging service rulebase url-blacklisting match-method

Configures URL Blacklisting match-method.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Rulebase Configuration (config-rulebase-*rulebase_name*)

Syntax Description **`url-blacklisting match-method`** *`match_method`*

match-method *match_method*

Specify the match method.

Must be one of the following:

- **exact**: URL Blacklisting performs an exact match of URL.
- **generic**: URL Blacklisting performs generic match of URL.

Usage Guidelines Use this command to configure the URL Blacklisting match method.

active-charging service ruledef

Configures ACS rule definitions (ruledef).

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*)

Syntax Description **`ruledef`** *`ruledef_name`* **`[ rule-application`** *`ruledef_purpose`* **`]`**

rule-application *ruledef_purpose*

Specify the purpose of the ruledef. When a ruledef is evaluated, if the multi-line-or all-lines command is configured, the logical OR.

Must be one of the following:

- **charging**: Specify that the current ruledef is for charging purposes.
- **post-processing**: Specify that the current ruledef is for post-processing purposes. This enables processing of packets even if the rule matching for them has been disabled.
- **routing**: Specify that the current ruledef is for routing purposes. Up to 256 ruledefs can be defined for routing in an ACS.

ruledef *ruledef_name*

Specify name of the ruledef. If the named ruledef does not exist, it is created, and the CLI mode changes to the ACS Ruledef Configuration Mode wherein the ruledef can be configured. If the named ruledef already exists, the CLI mode changes to the ACS Ruledef Configuration Mode for that ruledef.

Must be a string.

Usage Guidelines Use this command to create/configure an ACS ruledef. A ruledef represents a set of matching conditions across multiple L3 L7 protocol based on protocol fields and state information. Each ruledef can be used across multiple rulebases within the ACS.

Example

The following command creates/configures an ACS ruledef named test1:

```
ruledef test1
```

active-charging service ruledef bearer service-3gpp rat-type

Specify RAT type associated with the bearer flow.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **bearer service-3gpp rat-type** *operator rat_type*

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **=**: Equals.

rat_type

Specify the RAT type.

Must be one of the following:

- **geran**: GSM EDGE Radio Access Network type.
- **utran**: UMTS Terrestrial Radio Access Network type.
- **wlan**: Wireless LAN type.

Usage Guidelines Configures rule expression to match Radio Access Technology (RAT) in the bearer flow. Use this command to configure the RAT type associated with the bearer flow.

active-charging service ruledef dns answer-name

Configures ruledef to match DNS answer name.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **dns answer-name** *operator value*

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **!contains**: Does not contains.
- **!ends-with**: Does not end with.
- **!starts-with**: Does not start with.
- **=**: Equals.
- **case-sensitive**: Strings will be matched in case-sensitive manner.
- **contains**: Contains.
- **ends-with**: Ends with.
- **starts-with**: Starts with.

value

Specify the value.

Must be a string of 1-127 characters.

Usage Guidelines Configures ruledef to match answer name in the answer section of DNS response messages.

active-charging service ruledef dns any-match

Configures rule expression to match all packets of the specified protocol.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **dns any-match** *operator condition*

Syntax Description **icmpv6 any-match** *operator condition*

Syntax Description **rtp any-match** *operator condition*

Syntax Description **rtsp any-match** *operator condition*

Syntax Description **secure-http any-match** *operator condition*

Syntax Description **tcp any-match** *operator condition*

Syntax Description **udp any-match** *operator condition*

Syntax Description **wsp any-match** *operator condition*

Syntax Description **wtp any-match** *operator condition*

condition

Specify the condition.

Must be one of the following:

- **FALSE**
- **TRUE**

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **=**: Equals.

Usage Guidelines Use this command to configure rule expression to match all packets of a specified protocol.

Example

The following command defines a rule expression to match all RTP packets:

```
rtp any-match = TRUE
```

active-charging service ruledef dns previous-state

Configures rule expression to match previous state of the DNS FSM.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **dns previous-state** *operator previous_state*

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **=**: Equals.

previous_state

Specify the previous state to match.

Must be one of the following:

- **dns-timeout**: DNS timeout.
- **init**: Init.
- **req-sent**: Request sent.
- **resp-error**: Response error.
- **resp-success**: Response success.

Usage Guidelines Use this command to define rule expressions to match previous state of DNS FSM.

Example

The following command defines a rule expression to match the DNS FSM previous state "req-sent":

```
dns previous-state = req-sent
```

active-charging service ruledef dns query-name

Configures rule expression to match query name in DNS request messages.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **dns query-name [case-sensitive]** *operator query_name*

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **!contains**: Does not contain.
- **!ends-with**: Does not end with.
- **!starts-with**: Does not start with.
- **=**: Equals.
- **case-sensitive**: Strings will be matched in case-sensitive manner.
- **contains**: Contains.
- **ends-with**: Ends with.
- **starts-with**: Starts with.

query_name

Specify the query name to match.

Must be a string of 1-127 characters.

Usage Guidelines Use this command to define rule expressions to match query name in DNS request messages.

Example

The following command defines a rule expression to match DNS query name "test":

```
dns query-name = test
```

active-charging service ruledef dns query-type

Configures rule expression to match the query type in the DNS request messages.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **`dns query-type`** *`operator query_type`*

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **=**: Equals.

query_type

Specify the DNS query type to match.

Must be one of the following:

- **a**: Support query-type A.
- **aaaa**: Support query-type AAAA.
- **cname**: Support query-type CNAME.
- **ns**: Support query-type NS.
- **null**: Support query-type NULL.
- **ptr**: Support query-type PTR.
- **srv**: Support query-type SRV.
- **txt**: Support query-type TXT.

Usage Guidelines Use this command to define rule expressions to match the query type in the DNS request messages.

Example

The following command defines a rule expression to match the DNS query type "txt":

```
dns query-type = txt
```

active-charging service ruledef dns return-code

Configures rule expression to match response code in DNS response messages.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description

dns return-code *operator return_code*

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **=**: Equals.

return_code

Specify the response code to match.

Must be one of the following:

- **format-error**: DNS response: Format Error.
- **name-error**: DNS response: Name Error.
- **no-error**: DNS response: No Error.
- **not-implemented**: DNS response: Name server does not support the requested query.
- **refused**: DNS response: Refused to perform specified operation.
- **server-failure**: DNS response: Server Failure.

Usage Guidelines

Use this command to define rule expressions to match response code in DNS response messages.

Example

The following command defines a rule expression to match a DNS response code "refused":

```
dns return-code = refused
```

active-charging service ruledef dns state

Configures rule expressions to match current state of DNS FSM.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **dns state** *operator current_state*

current_state

Specify the state to match.

Must be one of the following:

- **dns-timeout**
- **init**
- **req-sent**
- **resp-error**
- **resp-success**

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **=**: Equals.

Usage Guidelines Use this command to define rule expressions to match DNS FSM current state.

Example

The following command defines a rule expression to match DNS FSM current state of "req-sent":

```
dns state = req-sent
```

active-charging service ruledef dns tid

Configures rule expressions to match Transaction Identifier (TID) field in DNS messages.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **dns tid** *operator tid_value*

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **>=**: Greater than or equals.
- **<=**: Lesser than or equals.
- **=**: Equals.

tid_value

Specify the DNS TID field value to match.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to define rule expressions to match a TID field of DNS messages.

Example

The following command defines a rule expression to match DNS TID field value of "test":

```
dns tid = test
```

active-charging service ruledef http content type

Configures rule expression to match value in HTTP Content-Type entity-header field.

Syntax Description **`http content type [ case-sensitive ]`** *`operator content_type`*

case-sensitive

Specify the rule expression must be case-sensitive. By default, rule expressions are not case-sensitive.

content_type

Specify the content type to match.

Must be a string of 1-127 characters.

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **!contains**: Does not contain.
- **!ends-with**: Does not end with.

- **!starts-with**: Does not start with.
- =: Equals.
- **contains**: Contains.
- **ends-with**: Ends with.
- **starts-with**: Starts with.

Usage Guidelines Use this command to configure rule expressions to match HTTP content type.

active-charging service ruledef http host

Configures rule expression to match value in HTTP Host Request header field.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **`http host [ case-sensitive ]`** *`operator host_name`*

case-sensitive

Specify the rule expression must be case-sensitive. By default, rule expressions are not case-sensitive.

host_name

Specify the host name to match.

Must be a string of 1-127 characters.

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **!contains**: Does not contain.
- **!ends-with**: Does not end with.
- **!starts-with**: Does not start with.
- =: Equals.
- **contains**: Contains.
- **ends-with**: Ends with.
- **regex**: Regular expression.
- **starts-with**: Starts with.

Usage Guidelines Use this command to define rule expressions to match value in HTTP Host request-header field.

Example

The following command defines a rule expression to match "host1" in HTTP Host request-header field:

```
http host = host1
```

active-charging service ruledef http referer

Configures rule expression to match the value in the HTTP Referer request-header field.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **`http referer [ case-sensitive ]`** *`operator referer_name`*

case-sensitive

Specify the rule expression must be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **!contains**: Does not contain.
- **!ends-with**: Does not end with.
- **!present**: Not present.
- **!starts-with**: Does not start with.
- **=**: Equals.
- **contains**: Contains.
- **ends-with**: Ends with.
- **regex**: Regular expression.
- **starts-with**: Starts with.

referer_name

Specify the HTTP referer name to match.

Must be a string of 1-127 characters.

Usage Guidelines Use this command to define rule expressions to match value in HTTP Referer request-header field. This feature allows an operator to collect or track all URLs visited during a particular subscriber session. These URLs include the entire string of visited URLs, including all referral links. This information is output in an Event Data Record (EDR) format to support reporting or billing functions.

Example

The following command defines a rule expression to match the HTTP referer "cricket.espn.com":

```
http referer = cricket.espn.com
```

active-charging service ruledef http url

Configures rule expression to match HTTP URL.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **`http url [ case-sensitive ]`** *`operator url`*

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **!contains**: Does not contain.
- **!ends-with**: Does not end with.
- **!present**: Does not present.
- **!starts-with**: Does not start with.
- **=**: Equals.
- **case-sensitive**: Is case sensitive.
- **contains**: Contains.
- **ends-with**: Ends with.
- **regex**: Regular expression.
- **starts-with**: Starts with.

url

Specify the HTTP URL to match.

Must be a string of 1-127 characters.

Usage Guidelines Use this command to define rule expressions to match HTTP URL.

active-charging service ruledef http user-agent

Configures rule expressions to match the User-Agent.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **`http user-agent [ case-sensitive ]`** *`operator user_agent_value`*

case-sensitive

Specify the rule expression must be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **!contains**: Does not contain.
- **!ends-with**: Does not end with.
- **!present**: Not present.
- **!starts-with**: Does not start with.
- **=**: Equal.
- **contains**: Contains.
- **ends-with**: Ends with.
- **present**: Present.
- **regex**: Regular expression.
- **starts-with**: Starts with.

user_agent_value

Specify the HTTP user agent value to match.

Must be a string of 1-127 characters.

Usage Guidelines Use this command to configure rule expressions to match user agent.

active-charging service ruledef icmpv6 any-match

Configures rule expression to match all packets of the specified protocol.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **dns any-match** *operator condition*

Syntax Description **icmpv6 any-match** *operator condition*

Syntax Description **rtp any-match** *operator condition*

Syntax Description **rtsp any-match** *operator condition*

Syntax Description **secure-http any-match** *operator condition*

Syntax Description **tcp any-match** *operator condition*

Syntax Description **udp any-match** *operator condition*

Syntax Description **wsp any-match** *operator condition*

Syntax Description **wtp any-match** *operator condition*

condition

Specify the condition.

Must be one of the following:

- **FALSE**
- **TRUE**

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **=**: Equals.

Usage Guidelines Use this command to configure rule expression to match all packets of a specified protocol.

Example

The following command defines a rule expression to match all RTP packets:

```
rtp any-match = TRUE
```

active-charging service ruledef ip any-match

Configures rule expressions to match all IPv4/IPv6 packets.

Syntax Description **ip any-match** *operator condition*

condition

Specify the condition.

Must be one of the following:

- **FALSE**
- **TRUE**

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **=**: Equals.

Usage Guidelines Use this command to define rule expressions to match IPv4/IPv6 packets.

Example

The following command defines a rule expression to match IPv4/IPv6 packets:

```
ip any-match = TRUE
```

active-charging service ruledef ip dst-address

Configures rule expressions to match IP destination address field within IP headers.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **ip dst-address** *operator* **{** *ip_address* **|** *ip_prefix_length* **|** **address-group** *ipv6_address* **|** **host-pool** *host_pool_name* **}**

address-group *ipv6_address_group_name*

Specify a group of IPv6 addresses configured with wildcard input and/or specialized range input. Input is accepted as a string and parsed. Multiple wildcard characters can be accepted as input and only one 2-byte range input will be accepted. Both wildcard character input and 2-byte range input can be configured together within an IPv6 address. For example, 2607:7700:*:[2020-3040]::ce1d:b083/128. * is a wildcard input. [2020-3040] is a 2-byte specialized range input.

Must be a string of 1-56 characters.

host-pool *host_pool_name*

Specify name of the host pool.

Must be a string of 1-63 characters.

ip-address-prefix *prefix*

Specify the IP address prefix.

Must be a string in the ipv4-prefix pattern. For information on the ipv4-prefix pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-prefix pattern. For information on the ipv6-prefix pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

ip_address

Specify the destination IP address.

Must be one of the following:

- **dst-address**: DST address.

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **!range**: Not in the range.
- >=: Greater than or equal to.
- <=: Lesser than or equal to.
- =: Equals.
- **range**: In the range.

Usage Guidelines

Use this command to define rule expressions to match the IP destination address field within IP headers.

Example

The following command defines a rule expression to match user traffic based on the IPv4 destination address 10.1.1.1:

```
ip dst-address = 10.1.1.1
```

active-charging service ruledef ip protocol

Configures rule expression to match based on protocol being transported by IP packet.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description

ip protocol *operator protocol*

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **>=**: Greater than or equal to.
- **<=**: Lesser than or equal to.
- **=**: Equals.

protocol

Specify the protocol.

Must be an integer in the range of 0-255.

-Or-

Must be one of the following:

- **ah**
- **esp**
- **gre**
- **icmp**
- **icmpv6**
- **tcp**
- **udp**

Usage Guidelines

Use this command to define rule expressions to match based on protocol being transported by IP packet.

active-charging service ruledef ip server-ip-addr

Configure the server's IP address.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **ip server-ip-address** *operator* **{ { {** *ipv4_address* **|** *ipv6_address* **} ip-address-prefix** *prefix* **| address-group** *ipv6_address_group_name* **} | host-pool** *host_pool_name* **}**

address-group *ipv6_address_group_name*

Specify a group of IPv6 addresses configured with wildcard input and/or specialized range input. Input is accepted as a string and parsed. Multiple wildcard characters can be accepted as input and only one 2-byte range input will be accepted. Both wildcard character input and 2-byte range input can be configured together within an IPv6 address. For example, 2607:7700:*:[2020-3040]::ce1d:b083/128. * is a wildcard input. [2020-3040] is a 2-byte specialized range input.

Must be a string of 1-56 characters.

host-pool *host_pool_name*

Specify name of the host pool.

Must be a string of 1-63 characters.

ip-address-prefix *prefix*

Specify the IP address prefix.

Must be a string in the ipv4-prefix pattern. For information on the ipv4-prefix pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-prefix pattern. For information on the ipv6-prefix pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

{ ipv4_address | ipv6_address }

Specify IP address of the server.

Must be one of the following:

- **server-ip-address**: server-ip-address.

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.

- **!range**: Not in the range.
- **>=**: Greater than or equal to.
- **<=**: Lesser than or equal to.
- **=**: Equals.
- **range**: In the range.

Usage Guidelines Use this command to configure the server's IP address.

active-charging service ruledef ip uplink

Configures rule expression to match IP uplink packets.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **ip uplink** *operator condition*

condition

Specify the condition to match.

Must be one of the following:

- **FALSE**: Not analyzed.
- **TRUE**: Analyzed.

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **=**: Equals.

Usage Guidelines Use this command to configure matching IP uplink packets based on condition.

active-charging service ruledef ip version

Configures rule expression to match based on IP version.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **ip version** *operator ip_version*

ip_version

Specify the condition to match.

Must be one of the following:

- **ipv4**
- **ipv6**

operator

Specify how to match.

Must be one of the following:

- =: Equals.

Usage Guidelines Use this command to configure rule expression to match based on the IP version.

active-charging service ruledef multi-line-or

This command applies the OR operator to all lines in the current ruledef.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **`multi-line-or all-lines`**

all-lines

Applies the OR operator to all lines in the current ruledef.

Usage Guidelines When a ruledef is evaluated, if the multi-line-or all-lines command is configured, the logical OR operator is applied to all the rule expressions in the ruledef to decide if the ruledef matches or not. If the multi-line-or all-lines command is not configured, the logical AND operator is applied to all the rule expressions.

active-charging service ruledef p2p

This command allows you to define rule expressions to match P2P protocol. This command must be used for charging purposes. It must not be used for detection purposes.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **`p2p set-app-proto`** *`app_protocol_name`*

p2p set-app-proto *app_protocol_name*

Specify name of the custom-defined protocol (CDP). CDP name specifies the name of the custom defined protocol (CDP) for TLS/SSL flows, QUIC flows or any app-identifier matching the ruledef. If the flow/packet

matches the rule, the CDP name specified in the ruledef will be taken and the flow will be marked as CDP. If no CDP is configured in the rule, then the flow will be treated as TLS/SSL or QUIC flow.

Must be a string of 1-19 characters.

Usage Guidelines Use this command to define rule expressions to detect P2P protocols for charging purposes. For detection purposes use the "p2p-detection protocol" command in the ACS Configuration Mode.

active-charging service ruledef p2p app-identifier

Configures application identifiers populated from the plugin and mark the matching flows to a custom-defined protocol (CDP) name.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **`p2p app-identifier`** *`app_type operator app_identifier`*

app_identifier

Specify the app identifier.

Must be a string of 1-127 characters.

app_type

Specify the application type.

Must be one of the following:

- **quic-sni**: Specify the QUIC Server Name Indication (SNI) field value.
- **tls-cname**: Specify the common name in the Server Hello message of TLS. SSL renegotiation is supported for the flows that are marked using "tls-cname" rules.
- **tls-sni**: Specify the TLS/SSL Server Name Indication (SNI) field.

operator

Specify how to match.

Must be one of the following:

- **!=**: Not equals.
- **=**: Equals.
- **contains**: Contains.
- **ends-with**: Ends with.
- **starts-with**: Starts with.

Usage Guidelines Use this command to configure application identifiers populated from the plugin and mark the matching flows to a custom-defined protocol (CDP) name. The SNI ruledef supports multi-line-or all-lines or default multi-line-and rule lines. The rule lines configured with "!=" operator will not be optimized.

Example

The following command configures the QUIC SNI app-identifier that is set to fb.com:

```
p2p app-identifier quic-sni = fb.com
```

active-charging service ruledef p2p protocol

Configures the protocol to match parameter.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **p2p protocol** *operator p2p_protocol*

operator

Specify how to match.

Must be one of the following:

- =: Equals.

p2p_protocol

Specify the P2P protocol.

Must be one of the following:

- **8tracks**: P2P detection protocol for "8tracks" application.
- **actionvoip**: P2P detection protocol for "actionvoip" application.
- **actsync**: P2P detection protocol for "actsync" application.
- **adobeconnect**: P2P detection protocol for "adobeconnect" application.
- **aimini**: P2P detection protocol for "aimini" application.
- **amazoncloud**: P2P detection protocol for "amazoncloud" application.
- **amazonmusic**: P2P detection protocol for "amazonmusic" application.
- **amazonvideo**: P2P detection protocol for "amazonvideo" application.
- **antsp2p**: P2P detection protocol for "antsp2p" application.
- **apple-push**: P2P detection protocol for "apple-push" application.
- **apple-store**: P2P detection protocol for "apple-store" application.
- **applejuice**: P2P detection protocol for "applejuice" application.

- **applemaps**: P2P detection protocol for "applemaps" application.
- **ares**: P2P detection protocol for "ares" application.
- **armagettron**: P2P detection protocol for "armagettron" application.
- **avi**: P2P detection protocol for "avi" application.
- **badoo**: P2P detection protocol for "badoo" application.
- **baidumovie**: P2P detection protocol for "baidumovie" application.
- **battlefld**: P2P detection protocol for "battlefld" application.
- **bbm**: P2P detection protocol for "bbm" application.
- **beatport**: P2P detection protocol for "beatport" application.
- **bitcasa**: P2P detection protocol for "bitcasa" application.
- **bittorrent-sync**: P2P detection protocol for "bittorrent-sync" application.
- **bittorrent**: P2P detection protocol for "bittorrent" application.
- **blackberry-store**: P2P detection protocol for "blackberry-store" application.
- **blackberry**: P2P detection protocol for "blackberry" application.
- **blackdialer**: P2P detection protocol for "blackdialer" application.
- **box**: P2P detection protocol for "box" application.
- **callofduty**: P2P detection protocol for "callofduty" application.
- **chikka**: P2P detection protocol for "chikka" application.
- **cisco-jabber**: P2P detection protocol for "cisco-jabber" application.
- **citrix**: P2P detection protocol for "citrix" application.
- **clubbox**: P2P detection protocol for "clubbox" application.
- **clubpenguin**: P2P detection protocol for "clubpenguin" application.
- **comodounite**: P2P detection protocol for "comodounite" application.
- **crackle**: P2P detection protocol for "crackle" application.
- **crossfire**: P2P detection protocol for "crossfire" application.
- **curiosity-stream**: P2P detection protocol for "curiosity-stream" application.
- **cyberghost**: P2P detection protocol for "cyberghost" application.
- **ddlink**: P2P detection protocol for "ddlink" application.
- **didi**: P2P detection protocol for "didi" application.
- **directconnect**: P2P detection protocol for "directconnect" application.
- **dish-anywhere**: P2P detection protocol for "dish-anywhere" application.
- **dns-tunneling**: P2P detection protocol for "dns-tunneling" application.

- **dofus**: P2P detection protocol for "dofus" application.
- **dropbox**: P2P detection protocol for "dropbox" application.
- **ebuddy**: P2P detection protocol for "ebuddy" application.
- **edonkey**: P2P detection protocol for "edonkey" application.
- **espn**: P2P detection protocol for "espn" application.
- **facebook**: P2P detection protocol for "facebook" application.
- **facetime**: P2P detection protocol for "facetime" application.
- **fandor**: P2P detection protocol for "fandor" application.
- **fasttrack**: P2P detection protocol for "fasttrack" application.
- **feidian**: P2P detection protocol for "feidian" application.
- **ficall**: P2P detection protocol for "ficall" application.
- **fiesta**: P2P detection protocol for "fiesta" application.
- **filetopia**: P2P detection protocol for "filetopia" application.
- **flash**: P2P detection protocol for "flash" application.
- **flickr**: P2P detection protocol for "flickr" application.
- **florensia**: P2P detection protocol for "florensia" application.
- **foursquare**: P2P detection protocol for "foursquare" application.
- **fox-sports**: P2P detection protocol for "fox-sports" application.
- **freenet**: P2P detection protocol for "freenet" application.
- **friendster**: P2P detection protocol for "friendster" application.
- **fring**: P2P detection protocol for "fring" application.
- **fubotv**: P2P detection protocol for "fubotv" application.
- **funshion**: P2P detection protocol for "funshion" application.
- **gadugadu**: P2P detection protocol for "gadugadu" application.
- **gamekit**: P2P detection protocol for "gamekit" application.
- **gmail**: P2P detection protocol for "gmail" application.
- **gnutella**: P2P detection protocol for "gnutella" application.
- **go90**: P2P detection protocol for "go90" application.
- **goober**: P2P detection protocol for "goober" application.
- **google-music**: P2P detection protocol for "google-music" application.
- **google-push**: P2P detection protocol for "google-push" application.
- **google**: P2P detection protocol for "google" application.

- **googleplay**: P2P detection protocol for "googleplay" application.
- **googleplus**: P2P detection protocol for "googleplus" application.
- **gotomeeting**: P2P detection protocol for "gotomeeting" application.
- **gtalk**: P2P detection protocol for "gtalk" application.
- **guildwars**: P2P detection protocol for "guildwars" application.
- **halflife2**: P2P detection protocol for "halflife2" application.
- **hamachivpn**: P2P detection protocol for "hamachivpn" application.
- **hbogo**: P2P detection protocol for "hbogo" application.
- **hbonow**: P2P detection protocol for "hbonow" application.
- **heytell**: P2P detection protocol for "heytell" application.
- **hgtv**: P2P detection protocol for "hgtv" application.
- **hike-messenger**: P2P detection protocol for "hike-messenger" application.
- **hls**: P2P detection protocol for "hls" application.
- **hotspotvpn**: P2P detection protocol for "hotspotvpn" application.
- **http**: P2P detection protocol for "http" application.
- **hulu**: P2P detection protocol for "hulu" application.
- **hyves**: P2P detection protocol for "hyves" application.
- **iax**: P2P detection protocol for "iax" application.
- **icall**: P2P detection protocol for "icall" application.
- **icecast**: P2P detection protocol for "icecast" application.
- **icloud**: P2P detection protocol for "icloud" application.
- **idrive**: P2P detection protocol for "idrive" application.
- **igo**: P2P detection protocol for "igo" application.
- **iheartradio**: P2P detection protocol for "iheartradio" application.
- **imesh**: P2P detection protocol for "imesh" application.
- **imessage**: P2P detection protocol for "imessage" application.
- **imgur**: P2P detection protocol for "imgur" application.
- **imo**: P2P detection protocol for "imo" application.
- **implus**: P2P detection protocol for "implus" application.
- **instagram**: P2P detection protocol for "instagram" application.
- **iplayer**: P2P detection protocol for "iplayer" application.
- **iptv**: P2P detection protocol for "iptv" application.

- **irc**: P2P detection protocol for "irc" application.
- **isakmp**: P2P detection protocol for "isakmp" application.
- **iskoot**: P2P detection protocol for "iskoot" application.
- **itunes**: P2P detection protocol for "itunes" application.
- **jabber**: P2P detection protocol for "jabber" application.
- **jap**: P2P detection protocol for "jap" application.
- **jumblo**: P2P detection protocol for "jumblo" application.
- **kakaotalk**: P2P detection protocol for "kakaotalk" application.
- **kidoodle**: P2P detection protocol for "kidoodle" application.
- **kik-messenger**: P2P detection protocol for "kik-messenger" application.
- **kontiki**: P2P detection protocol for "kontiki" application.
- **kugou**: P2P detection protocol for "kugou" application.
- **kuro**: P2P detection protocol for "kuro" application.
- **linkedin**: P2P detection protocol for "linkedin" application.
- **lync**: P2P detection protocol for "lync" application.
- **magicjack**: P2P detection protocol for "magicjack" application.
- **manolito**: P2P detection protocol for "manolito" application.
- **mapfactor**: P2P detection protocol for "mapfactor" application.
- **mapi**: P2P detection protocol for "mapi" application.
- **maplestory**: P2P detection protocol for "maplestory" application.
- **meebo**: P2P detection protocol for "meebo" application.
- **mega**: P2P detection protocol for "mega" application.
- **mgcp**: P2P detection protocol for "mgcp" application.
- **mig33**: P2P detection protocol for "mig33" application.
- **mlb**: P2P detection protocol for "mlb" application.
- **mojo**: P2P detection protocol for "mojo" application.
- **monkey3**: P2P detection protocol for "monkey3" application.
- **mozy**: P2P detection protocol for "mozy" application.
- **msn**: P2P detection protocol for "msn" application.
- **msrp**: P2P detection protocol for "msrp" application.
- **mute**: P2P detection protocol for "mute" application.
- **mypeople**: P2P detection protocol for "mypeople" application.

- **myspace**: P2P detection protocol for "myspace" application.
- **nateontalk**: P2P detection protocol for "nateontalk" application.
- **naverline**: P2P detection protocol for "naverline" application.
- **navigon**: P2P detection protocol for "navigon" application.
- **nbc-sports**: P2P detection protocol for "nbc-sports" application.
- **netflix**: P2P detection protocol for "netflix" application.
- **netmotion**: P2P detection protocol for "netmotion" application.
- **newsy**: P2P detection protocol for "newsy" application.
- **nimbuzz**: P2P detection protocol for "nimbuzz" application.
- **nokia-store**: P2P detection protocol for "nokia-store" application.
- **octoshape**: P2P detection protocol for "octoshape" application.
- **odnoklassniki**: P2P detection protocol for "odnoklassniki" application.
- **off**: P2P detection protocol for "off" application.
- **ogg**: P2P detection protocol for "ogg" application.
- **oist**: P2P detection protocol for "oist" application.
- **oovoo**: P2P detection protocol for "oovoo" application.
- **opendrive**: P2P detection protocol for "opendrive" application.
- **openft**: P2P detection protocol for "openft" application.
- **openvpn**: P2P detection protocol for "openvpn" application.
- **operamini**: P2P detection protocol for "operamini" application.
- **orb**: P2P detection protocol for "orb" application.
- **oscar**: P2P detection protocol for "oscar" application.
- **outlook**: P2P detection protocol for "outlook" application.
- **paltalk**: P2P detection protocol for "paltalk" application.
- **pando**: P2P detection protocol for "pando" application.
- **pandora**: P2P detection protocol for "pandora" application.
- **path**: P2P detection protocol for "path" application.
- **pcanywhere**: P2P detection protocol for "pcanywhere" application.
- **periscope**: P2P detection protocol for "periscope" application.
- **pinterest**: P2P detection protocol for "pinterest" application.
- **plingm**: P2P detection protocol for "plingm" application.
- **poco**: P2P detection protocol for "poco" application.

- **popo**: P2P detection protocol for "popo" application.
- **pplive**: P2P detection protocol for "pplive" application.
- **ppstream**: P2P detection protocol for "ppstream" application.
- **ps3**: P2P detection protocol for "ps3" application.
- **qq**: P2P detection protocol for "qq" application.
- **qqgame**: P2P detection protocol for "qqgame" application.
- **qqlive**: P2P detection protocol for "qqlive" application.
- **quake**: P2P detection protocol for "quake" application.
- **quic**: P2P detection protocol for "quic" application.
- **quicktime**: P2P detection protocol for "quicktime" application.
- **radio-paradise**: P2P detection protocol for "radio-paradise" application.
- **rdp**: P2P detection protocol for "rdp" application.
- **rdt**: P2P detection protocol for "rdt" application.
- **regram**: P2P detection protocol for "regram" application.
- **rfactor**: P2P detection protocol for "rfactor" application.
- **rhapsody**: P2P detection protocol for "rhapsody" application.
- **rmstream**: P2P detection protocol for "rmstream" application.
- **rodi**: P2P detection protocol for "rodi" application.
- **rynga**: P2P detection protocol for "rynga" application.
- **samsung-store**: P2P detection protocol for "samsung-store" application.
- **scydo**: P2P detection protocol for "scydo" application.
- **secondlife**: P2P detection protocol for "secondlife" application.
- **shoutcast**: P2P detection protocol for "shoutcast" application.
- **showtime**: P2P detection protocol for "showtime" application.
- **silverlight**: P2P detection protocol for "silverlight" application.
- **siri**: P2P detection protocol for "siri" application.
- **skinny**: P2P detection protocol for "skinny" application.
- **skydrive**: P2P detection protocol for "skydrive" application.
- **skype**: P2P detection protocol for "Skype" application.
- **slacker-radio**: P2P detection protocol for "slacker-radio" application.
- **slingbox**: P2P detection protocol for "slingbox" application.
- **slingtv**: P2P detection protocol for "slingtv" application.

- **smartvoip**: P2P detection protocol for "smartvoip" application.
- **snapchat**: P2P detection protocol for "snapchat" application.
- **softether**: P2P detection protocol for "softether" application.
- **sopcast**: P2P detection protocol for "sopcast" application.
- **soribada**: P2P detection protocol for "soribada" application.
- **soulseek**: P2P detection protocol for "soulseek" application.
- **soundcloud**: P2P detection protocol for "soundcloud" application.
- **spdy**: P2P detection protocol for "spdy" application.
- **speedtest**: P2P detection protocol for "speedtest" application.
- **splashfighter**: P2P detection protocol for "splashfighter" application.
- **spotify**: P2P detection protocol for "spotify" application.
- **ssdp**: P2P detection protocol for "ssdp" application.
- **ssl**: P2P detection protocol for "ssl" application.
- **starz**: P2P detection protocol for "starz" application.
- **stealthnet**: P2P detection protocol for "stealthnet" application.
- **steam**: P2P detection protocol for "steam" application.
- **stun**: P2P detection protocol for "stun" application.
- **sudaphone**: P2P detection protocol for "sudaphone" application.
- **svtplay**: P2P detection protocol for "svtplay" application.
- **tagged**: P2P detection protocol for "tagged" application.
- **talkatone**: P2P detection protocol for "talkatone" application.
- **tango**: P2P detection protocol for "tango" application.
- **teamspeak**: P2P detection protocol for "teamspeak" application.
- **teamviewer**: P2P detection protocol for "teamviewer" application.
- **telegram**: P2P detection protocol for "telegram" application.
- **thunder**: P2P detection protocol for "thunder" application.
- **thunderhs**: P2P detection protocol for "thunderhs" application.
- **tmo-tv**: P2P detection protocol for "tmo-tv" application.
- **tor**: P2P detection protocol for "tor" application.
- **truecaller**: P2P detection protocol for "truecaller" application.
- **truphone**: P2P detection protocol for "truphone" application.
- **tumblr**: P2P detection protocol for "tumblr" application.

- **tunein-radio**: P2P detection protocol for "tunein-radio" application.
- **tunnelvoice**: P2P detection protocol for "tunnelvoice" application.
- **tvants**: P2P detection protocol for "tvants" application.
- **tvuplayer**: P2P detection protocol for "tvuplayer" application.
- **twitch**: P2P detection protocol for "twitch" application.
- **twitter**: P2P detection protocol for "twitter" application.
- **ultrabac**: P2P detection protocol for "ultrabac" application.
- **ultrasurf**: P2P detection protocol for "ultrasurf" application.
- **univision**: P2P detection protocol for "univision" application.
- **upc-phone**: P2P detection protocol for "upc-phone" application.
- **usenet**: P2P detection protocol for "usenet" application.
- **ustream**: P2P detection protocol for "ustream" application.
- **uusee**: P2P detection protocol for "uusee" application.
- **vchat**: P2P detection protocol for "vchat" application.
- **veohtv**: P2P detection protocol for "veohtv" application.
- **vessel**: P2P detection protocol for "vessel" application.
- **vevo**: P2P detection protocol for "vevo" application.
- **viber**: P2P detection protocol for "viber" application.
- **vine**: P2P detection protocol for "vine" application.
- **voipdiscount**: P2P detection protocol for "voipdiscount" application.
- **vopium**: P2P detection protocol for "vopium" application.
- **voxer**: P2P detection protocol for "voxer" application.
- **vpnx**: P2P detection protocol for "vpnx" application.
- **vtok**: P2P detection protocol for "vtok" application.
- **vtun**: P2P detection protocol for "vtun" application.
- **vudu**: P2P detection protocol for "vudu" application.
- **warcft3**: P2P detection protocol for "warcft3" application.
- **waze**: P2P detection protocol for "waze" application.
- **webex**: P2P detection protocol for "webex" application.
- **wechat**: P2P detection protocol for "wechat" application.
- **weibo**: P2P detection protocol for "weibo" application.
- **whatsapp**: P2P detection protocol for "whatsapp" application.

- **wii**: P2P detection protocol for "wii" application.
- **windows-azure**: P2P detection protocol for "windows-azure" application.
- **windows-store**: P2P detection protocol for "windows-store" application.
- **winmx**: P2P detection protocol for "winmx" application.
- **winny**: P2P detection protocol for "winny" application.
- **wmstream**: P2P detection protocol for "wmstream" application.
- **wofkungfu**: P2P detection protocol for "wofkungfu" application.
- **wofwarcraft**: P2P detection protocol for "wofwarcraft" application.
- **wuala**: P2P detection protocol for "wuala" application.
- **wwe**: P2P detection protocol for "wwe" application.
- **xbox**: P2P detection protocol for "xbox" application.
- **xdcc**: P2P detection protocol for "xdcc" application.
- **xing**: P2P detection protocol for "xing" application.
- **yahoo**: P2P detection protocol for "yahoo" application.
- **yahoomail**: P2P detection protocol for "yahoomail" application.
- **youku**: P2P detection protocol for "youku" application.
- **yourfreetunnel**: P2P detection protocol for "yourfreetunnel" application.
- **youtube**: P2P detection protocol for "youtube" application.
- **zattoo**: P2P detection protocol for "zattoo" application.

Usage Guidelines Use this command to specify the protocol to match.

active-charging service ruledef p2p traffic-type

Configures rule expression to match the traffic type.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **p2p traffic-type** *operator traffic_type*

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **=**: Equals.

traffic_type

Specify the traffic type to match.

Must be one of the following:

- **ads**
- **audio**
- **file-transfer**
- **im**
- **streaming-audio**
- **streaming-video**
- **tunnel**
- **unclassified**
- **video**
- **voipout**

Usage Guidelines Use this command to configure the system to detect voice or non-voice P2P traffic. When the detection of a protocol is enabled then the detection of sub-type is enabled by default.

Example

The following command configures the system to detect video traffic:

```
p2p traffic-type = video
```

active-charging service ruledef rtp any-match

Configures rule expression to match all packets of the specified protocol.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **dns any-match** *operator condition*

Syntax Description **icmpv6 any-match** *operator condition*

Syntax Description **rtp any-match** *operator condition*

Syntax Description **rtsp any-match** *operator condition*

Syntax Description **secure-http any-match** *operator condition*

Syntax Description **tcp any-match** *operator condition*

Syntax Description **udp any-match** *operator condition*

Syntax Description **wsp any-match** *operator condition*

Syntax Description **wtp any-match** *operator condition*

condition

Specify the condition.

Must be one of the following:

- **FALSE**
- **TRUE**

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **=**: Equals.

Usage Guidelines Use this command to configure rule expression to match all packets of a specified protocol.

Example

The following command defines a rule expression to match all RTP packets:

```
rtp any-match = TRUE
```

active-charging service ruledef rtsp any-match

Configures rule expression to match all packets of the specified protocol.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **dns any-match** *operator condition*

Syntax Description **icmpv6 any-match** *operator condition*

Syntax Description **rtp any-match** *operator condition*

Syntax Description **rtsp any-match** *operator condition*

Syntax Description **secure-http any-match** *operator condition*

Syntax Description **tcp any-match** *operator condition*

Syntax Description **udp any-match** *operator condition*

Syntax Description **wsp any-match** *operator condition*

Syntax Description **wtp any-match** *operator condition*

condition

Specify the condition.

Must be one of the following:

- **FALSE**
- **TRUE**

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **=**: Equals.

Usage Guidelines Use this command to configure rule expression to match all packets of a specified protocol.

Example

The following command defines a rule expression to match all RTP packets:

```
rtp any-match = TRUE
```

active-charging service ruledef secure-http any-match

Configures rule expression to match all packets of the specified protocol.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **dns any-match** *operator condition*

Syntax Description **icmpv6 any-match** *operator condition*

Syntax Description **rtp any-match** *operator condition*

Syntax Description **rtsp any-match** *operator condition*

Syntax Description **secure-http any-match** *operator condition*

Syntax Description **tcp any-match** *operator condition*

Syntax Description **udp any-match** *operator condition*

Syntax Description **wsp any-match** *operator condition*

Syntax Description **wtp any-match** *operator condition*

condition

Specify the condition.

Must be one of the following:

- **FALSE**
- **TRUE**

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **=**: Equals.

Usage Guidelines Use this command to configure rule expression to match all packets of a specified protocol.

Example

The following command defines a rule expression to match all RTP packets:

```
rtp any-match = TRUE
```

active-charging service ruledef secure-http uplink

Configures rule expression to match HTTPS uplink (subscriber to network) packets.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **secure-http uplink** *operator condition*

condition

Specify the condition to match.

Must be one of the following:

- **FALSE**
- **TRUE**

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **=**: Equals.

Usage Guidelines Use this command to specify the HTTPS uplink packets.

active-charging service ruledef tcp any-match

Configures rule expression to match all packets of the specified protocol.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **dns any-match** *operator condition*

Syntax Description **icmpv6 any-match** *operator condition*

Syntax Description **rtp any-match** *operator condition*

Syntax Description **rtsp any-match** *operator condition*

Syntax Description **secure-http any-match** *operator condition*

Syntax Description **tcp any-match** *operator condition*

Syntax Description **udp any-match** *operator condition*

Syntax Description **wsp any-match** *operator condition*

Syntax Description **wtp any-match** *operator condition*

condition

Specify the condition.

Must be one of the following:

- **FALSE**
- **TRUE**

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.

- **=**: Equals.

Usage Guidelines Use this command to configure rule expression to match all packets of a specified protocol.

Example

The following command defines a rule expression to match all RTP packets:

```
rtp any-match = TRUE
```

active-charging service ruledef tcp either-port with-portMap-range

Configures port selection with port map range.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **tcp either-port** *operator* **port-map** *port_map_name*

Syntax Description **udp either-port** *operator* **port-map** *port_map_name*

port-map *port_map_name*

Specify name of the port map.

Must be a string of 1-63 characters.

operator

Specify how to match.

Must be one of the following:

- **!range**: Not in the range of.
- **range**: In the range of.

Usage Guidelines Use this command to configure with port map range.

active-charging service ruledef tcp either-port with-range

Configures port configuration with range.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **tcp either-port** *operator start_range* **to** *end_range*

Syntax Description **udp either-port** *operator start_range* **to** *end_range*

to

Specify until node.

Must be one of the following:

- **to**

end_range

Specify the end range.

Must be an integer in the range of 1-65535.

operator

Specify how to match.

Must be one of the following:

- **!range**: Not in the range of.
- **range**: In the range of.

start_range

Specify the start range.

Must be an integer in the range of 1-65535.

Usage Guidelines Use this command to configure port configuration with range.

active-charging service ruledef tcp either-port without-range

Configures port configuration without range.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **tcp either-port** *operator* **port** *port_number*

Syntax Description **udp either-port** *operator* **port** *port_number*

port *port_number*

Specify the port number.

Must be an integer in the range of 1-65535.

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **>=**: Greater than or equal to.
- **<=**: Lesser than or equal to.
- **=**: Equals.

Usage Guidelines Use this command to configure port configuration without range.

active-charging service ruledef tcp flag

Configures rule expression to match bit within the Flag field of TCP headers.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **`tcp flag`** *`operator flag`*

flag

Specify the flag to match.

Must be one of the following:

- **ack**
- **fin**
- **push**
- **reset**
- **sync**

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **!contains**: Does not contain.
- **=**: Equals.
- **contains**: Contains.

Usage Guidelines Use this command to configure rule expression to match bit within the Flag field of TCP headers.

active-charging service ruledef tcp state

Configures rule expression to match current state of TCP connections.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description

tcp state *operator current_state*

current_state

Specify the state to match.

Must be one of the following:

- **close-wait**
- **close**
- **closing**
- **established**
- **fin-wait1**
- **fin-wait2**
- **last-ack**
- **listen**
- **syn-received**
- **syn-sent**
- **time-wait**

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **=**: Equals.

Usage Guidelines

Use this command to define rule expressions to match a current state of TCP connections.

Example

The following command defines a rule expression to match user traffic based on current state "close":

```
tcp state = close
```

active-charging service ruledef tethering-detection

Configures rule expression to match tethered or non-tethered flows.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description

tethering-detection *flow_option*

flow_option

Specify the flow option.

Must be one of the following:

- **flow-not-tethered**: If tethering is not detected on flow.
- **flow-tethered**: If tethering is detected on flow.

Usage Guidelines

Use this command to define rule expressions to match tethered/non-tethered flows. Note that in order for the rule containing the tethering-detection configuration to get matched, at least one valid rule line has to be present in it.

Example

The following command defines a rule expression to match tethered flows:

```
tethering-detection flow-tethered
```

active-charging service ruledef tethering-detection application

Configures application-based tethering detection.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description

tethering-detection application *flow_option*

flow_option

Specify the flow option.

Must be one of the following:

- **flow-not-tethered**: If tethering is not detected on flow.
- **flow-tethered**: If tethering is detected on flow.

Usage Guidelines

Use this command to select flows that were tethered or non-tethered based on application-based detection solution.

active-charging service ruledef tethering-detection dns-based

Configures DNS query pattern based tethering detection.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **tethering-detection dns-based** *flow_option*

flow_option

Specify the flow option.

Must be one of the following:

- **flow-not-tethered**: If tethering is not detected on flow.
- **flow-tethered**: If tethering is detected on flow.

Usage Guidelines Use this command to select flows that were tethered or non-tethered based on DNS-based detection solution.

active-charging service ruledef tethering-detection ip-ttl

Configures IP-TTL based tethering detection.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **tethering-detection ip-ttl** *flow_option*

flow_option

Specify the flow option.

Must be one of the following:

- **flow-not-tethered**: If tethering is not detected on flow.
- **flow-tethered**: If tethering is detected on flow.

Usage Guidelines Use this command to select flows that were tethered or non-tethered as per IP-TTL values.

active-charging service ruledef tethering-detection os-ua

Configures OS-UA based tethering detection.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **tethering-detection os-ua** *flow_option*

flow_option

Specify the flow option.

Must be one of the following:

- **flow-not-tethered**: If tethering is not detected on flow.
- **flow-tethered**: If tethering is detected on flow.

Usage Guidelines Use this command to select flows that were tethered or non-tethered as per OS-UA lookups.

active-charging service ruledef udp any-match

Configures rule expression to match all packets of the specified protocol.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **dns any-match** *operator condition*

Syntax Description **icmpv6 any-match** *operator condition*

Syntax Description **rtp any-match** *operator condition*

Syntax Description **rtsp any-match** *operator condition*

Syntax Description **secure-http any-match** *operator condition*

Syntax Description **tcp any-match** *operator condition*

Syntax Description **udp any-match** *operator condition*

Syntax Description **wsp any-match** *operator condition*

Syntax Description **wtp any-match** *operator condition*

condition

Specify the condition.

Must be one of the following:

- **FALSE**
- **TRUE**

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **=**: Equals.

Usage Guidelines Use this command to configure rule expression to match all packets of a specified protocol.

Example

The following command defines a rule expression to match all RTP packets:

```
rtp any-match = TRUE
```

active-charging service ruledef udp either-port with-portMap-range

Configures port selection with port map range.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **tcp either-port** *operator* **port-map** *port_map_name*

Syntax Description **udp either-port** *operator* **port-map** *port_map_name*

port-map *port_map_name*

Specify name of the port map.

Must be a string of 1-63 characters.

operator

Specify how to match.

Must be one of the following:

- **!range**: Not in the range of.
- **range**: In the range of.

Usage Guidelines Use this command to configure with port map range.

active-charging service ruledef udp either-port with-range

Configures port configuration with range.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **tcp either-port** *operator start_range* **to** *end_range*

Syntax Description **udp either-port** *operator start_range* **to** *end_range*

to

Specify until node.

Must be one of the following:

- **to**

end_range

Specify the end range.

Must be an integer in the range of 1-65535.

operator

Specify how to match.

Must be one of the following:

- **!range**: Not in the range of.
- **range**: In the range of.

start_range

Specify the start range.

Must be an integer in the range of 1-65535.

Usage Guidelines Use this command to configure port configuration with range.

active-charging service ruledef udp either-port without-range

Configures port configuration without range.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **tcp either-port** *operator* **port** *port_number*

Syntax Description **udp either-port** *operator* **port** *port_number*

port *port_number*

Specify the port number.

Must be an integer in the range of 1-65535.

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **>=**: Greater than or equal to.
- **<=**: Lesser than or equal to.
- **=**: Equals.

Usage Guidelines Use this command to configure port configuration without range.

active-charging service ruledef wsp any-match

Configures rule expression to match all packets of the specified protocol.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **dns any-match** *operator condition*

Syntax Description **icmpv6 any-match** *operator condition*

Syntax Description **rtp any-match** *operator condition*

Syntax Description **rtsp any-match** *operator condition*

Syntax Description **secure-http any-match** *operator condition*

Syntax Description **tcp any-match** *operator condition*

Syntax Description **udp any-match** *operator condition*

Syntax Description **wsp any-match** *operator condition*

Syntax Description **wtp any-match** *operator condition*

condition

Specify the condition.

Must be one of the following:

- **FALSE**
- **TRUE**

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **=**: Equals.

Usage Guidelines Use this command to configure rule expression to match all packets of a specified protocol.

Example

The following command defines a rule expression to match all RTP packets:

```
rtp any-match = TRUE
```

active-charging service ruledef wtp any-match

Configures rule expression to match all packets of the specified protocol.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **dns any-match** *operator condition*

Syntax Description **icmpv6 any-match** *operator condition*

Syntax Description **rtp any-match** *operator condition*

Syntax Description **rtsp any-match** *operator condition*

Syntax Description **secure-http any-match** *operator condition*

Syntax Description **tcp any-match** *operator condition*

Syntax Description **udp any-match** *operator condition*

Syntax Description **wsp any-match** *operator condition*

Syntax Description **wtp any-match** *operator condition*

condition

Specify the condition.

Must be one of the following:

- **FALSE**
- **TRUE**

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **=**: Equals.

Usage Guidelines Use this command to configure rule expression to match all packets of a specified protocol.

Example

The following command defines a rule expression to match all RTP packets:

```
rtp any-match = TRUE
```

active-charging service ruledef www any-match

Configures rule expression to match all WWW packets. It is true for HTTP, WAP1.x, and WAP2.0 protocols.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **www any-match** *operator condition*

condition

Specify the condition to match.

Must be one of the following:

- **FALSE**
- **TRUE**

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **=**: Equals.

Usage Guidelines Use this command to define rule expressions to match all WWW packets. This expression is true for HTTP, WAP1.x, and WAP2.0 protocols

Example

The following command defines a rule expression to match all WWW packets:

```
www any-match = TRUE
```

active-charging service ruledef www host

Configures rule expression to match the "host name" header field present in HTTP/WSP headers.

Command Modes

Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description

www host [case-sensitive] *operator host_name*

case-sensitive

Specify the rule expression must be case-sensitive. By default, rule expressions are not case-sensitive.

host_name

Specify the WWW host name to match.

Must be a string of 1-127 characters.

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **!contains**: Does not contain.
- **!ends-with**: Does not end with.
- **!starts-with**: Does not start with.
- **=**: Equals.
- **contains**: Contains.
- **ends-with**: Ends with.
- **regex**: Regular expression.
- **starts-with**: Starts with.

Usage Guidelines

Use this command to define rule expressions to match the host name header field present in HTTP/WSP headers.

Example

The following command defines a rule expression to match user traffic based on WWW host name "host1":

```
www host = host1
```

active-charging service ruledef www url

Configures rule expressions to match URL.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > Ruledef Configuration (config-ruledef-*ruledef_name*)

Syntax Description **`www url [ case-sensitive ]`** *`operator url`*

case-sensitive

Specify the rule expression must be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specify how to match.

Must be one of the following:

- **!=**: Does not equal.
- **!contains**: Does not contain.
- **!ends-with**: Does not end with.
- **!starts-with**: Does not start with.
- **=**: Equals.
- **contains**: Contains.
- **ends-with**: Ends with.
- **regex**: Regular expression.
- **starts-with**: Starts with.

url

Specify the URL to match.

Must be a string of 1-127 characters.

Usage Guidelines Use this command to configure the rule expressions to match URLsfor any Web protocol analyzer HTTP, WAP1.X, WAP2.0.

active-charging service url-blacklisting

Enable URL Blacklisting functionality.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*)

Syntax Description **`url-blacklisting match-method`** *`match_method`*

match-method *match_method*

Specify the match method to look up for URLs in the URL Blacklisting database.

Must be one of the following:

- **exact**: URL Blacklisting is performed only on exact match with a URL present in the URL.
- **generic**: URL Blacklisting is performed on a generic match with URLs present in the URL Blacklisting database.

Default Value: exact.

Usage Guidelines Use this command to enable URL Blacklisting functionality.

active-charging service urr-list

Configures ACS URR List configuration.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*)

Syntax Description **urr-list** *urr_list_name*

urr_list_name

Specify name of the URR list.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to configure the ACS URR List configuration. Enters the URR List Configuration mode (config-urr-list-<urr_list_name>). This mode allows mapping of URR-ID with Rating Group and Service-ID.

You can configure a maximum of one element with this command.

active-charging service urr-list urr-list-data

Configures URR list data.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > URR List Configuration (config-urr-list-*urr_list_name*)

Syntax Description **rating-group** *rating_id* **urr-id** *urr_id*

rating group *rating_id*

Specify the rating ID used in prepaid charging.

Must be an integer in the range of 0-2147483647.

urr-id *urr_id*

Specify the URR identifier for rating/service group.

Must be an integer in the range of 1-8388607.

Usage Guidelines Use this command to configure the URR list data.

active-charging service urr-list urr-list-data service-identifier

Configures the URR ID service identifier parameter.

Command Modes Exec > Global Configuration (config) > ACS Configuration (config-service-*acs_name*) > URR List Configuration (config-urr-list-*urr_list_name*)

Syntax Description **rating-group** *rating_id* **urr-id** *urr_id* **service-identifier** *service_id* **urr-id** *urr_id*

service-identifier *service_id*

Specify the service ID, the number given to the service.

Must be an integer in the range of 0-2147483647.

urr-id *urr_id*

Specify the URR identifier for rating/service group.

Must be an integer in the range of 1-8388607.

Usage Guidelines Use this command to configure the URR ID service identifier parameter.

apn

Configures Access Point Name (APN) templates.

Command Modes Exec > Global Configuration (config)

Syntax Description **apn** *apn_name*

apn *apn_name*

Specify name of the APN.

Must be a string in the pattern '[A-Za-z0-9]{1}[A-za-z0-9.-]{1,61}'.

Usage Guidelines Use this command to create and configure an APN.

Example

The following command creates an APN template named isp1:

```
apn isp1
```

apn active-charging

Enables a configured ACS rulebase.

Command Modes Exec > Global Configuration (config) > APN Configuration (config-apn-*apn_name*)

Syntax Description **active-charging rulebase** *rulebase_name*

rulebase *rulebase_name*

Specify name of the rulebase.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to enable a configured ACS rulebase.

apn authorize-with-hss

Configures S6b authentication.

Command Modes Exec > Global Configuration (config) > APN Configuration (config-apn-*apn_name*)

Syntax Description **authorize-with-hss [report-ipv6-addr]**

report-ipv6-addr

Specify to enable IPv6 reporting through AAR towards S6b interface.

Usage Guidelines Use this command to configure S6b authentication. Enables IPv6 reporting through AAR towards S6b interface.

apn authorize-with-hss egtp

Enables S6b authorization for all the interfaces of EGTP along with GN-GP Handover except 3G initial attach.

Command Modes Exec > Global Configuration (config) > APN Configuration (config-apn-*apn_name*)

Syntax Description **authorize-with-hss egtp [report-ipv6-addr]**

report-ipv6-addr

Specify to enable IPv6 reporting through AAR towards S6b interface.

Usage Guidelines Use this command to enable S6b authorization for all the interfaces of EGTP along with GN-GP Handover except 3G initial attach.

apn authorize-with-hss egtp gn-gp-enabled

Enables S6b authorization for 3G Initial Attach and GnGp Handover.

Command Modes Exec > Global Configuration (config) > APN Configuration (config-apn-*apn_name*)

Syntax Description **`authorize-with-hss egtp gn-gp-enabled report-ipv6-addr`**

report-ipv6-addr

Specify to enable IPv6 reporting through AAR towards S6b interface.

Usage Guidelines Use this command to enable S6b authorization for 3G Initial Attach and GnGp Handover.

apn authorize-with-hss egtp s2b

Enables S6b authorization for egtp-s2b.

Command Modes Exec > Global Configuration (config) > APN Configuration (config-apn-*apn_name*)

Syntax Description **`authorize-with-hss egtp s2b report-ipv6-addr`**

report-ipv6-addr

Specify to enable IPv6 reporting through AAR towards S6b interface.

Usage Guidelines Use this command to enable S6b authorization for egtp-s2b.

apn authorize-with-hss egtp s2b gn-gp-enabled

Enables S6b authorization for 3G Initial Attach and GnGp Handover.

Command Modes Exec > Global Configuration (config) > APN Configuration (config-apn-*apn_name*)

Syntax Description **`authorize-with-hss egtp s2b gn-gp-enabled report-ipv6-addr`**

report-ipv6-addr

Specify to enable IPv6 reporting through AAR towards S6b interface.

Usage Guidelines Use this command to enable S6b authorization for 3G Initial Attach and GnGp Handover.

apn authorize-with-hss egtp s2b s5-s8

Enables S6b authorization for egtp-s5s8.

Command Modes Exec > Global Configuration (config) > APN Configuration (config-apn-*apn_name*)

Syntax Description **authorize-with-hss egtp s2b s5-s8 [** *gn_gp_option* **| report-ipv6-addr]**

report-ipv6-addr

Specify to enable IPv6 reporting through AAR towards s6b interface.

gn_gp_option

Specify to enable or disable S6b authorization for 3G Initial Attach and GnGp Handover.

Must be one of the following:

- **gn-gp-disabled**: Disables S6b authorization for 3G Initial Attach and GnGp Handover.
- **gn-gp-enabled**: Enables S6b authorization for 3G Initial Attach and GnGp Handover.

Usage Guidelines Use this command to enable S6b authorization for egtp-s5s8.

apn authorize-with-hss egtp s5-s8

Enables S6b authorization for egtp-s5s8.

Command Modes Exec > Global Configuration (config) > APN Configuration (config-apn-*apn_name*)

Syntax Description **authorize-with-hss egtp s5-s8 [** *gn_gp_option* **] [report-ipv6-addr]**

report-ipv6-addr

Specify to enable IPv6 reporting through AAR towards s6b interface.

gn_gp_option

Specify to enable or disable S6b authorization for 3G Initial Attach and GnGp Handover.

Must be one of the following:

- **gn-gp-disabled**: Disables S6b authorization for 3G Initial Attach and GnGp Handover.
- **gn-gp-enabled**: Enables S6b authorization for 3G Initial Attach and GnGp Handover.

Usage Guidelines Use this command to enable S6b authorization for egtp-s5s8.

apn authorize-with-hss egtp s5-s8 s2b

Enables S6b authorization for egtp-s2b.

Command Modes Exec > Global Configuration (config) > APN Configuration (config-apn-*apn_name*)

Syntax Description **authorize-with-hss egtp s5-s8 s2b [** *gn_gp_option* **] [report-ipv6-addr]**

report-ipv6-addr

Specify to enable IPv6 reporting through AAR towards s6b interface.

gn_gp_option

Specify to enable or disable S6b authorization for 3G Initial Attach and GnGp Handover.

Must be one of the following:

- **gn-gp-disabled**: Disables S6b authorization for 3G Initial Attach and GnGp Handover.
- **gn-gp-enabled**: Enables S6b authorization for 3G Initial Attach and GnGp Handover.

Usage Guidelines Use this command to enable S6b authorization for egtp-s2b.

apn authorize-with-hss lma

Enables IPv6 reporting through AAR towards S6b.

Command Modes Exec > Global Configuration (config) > APN Configuration (config-apn-*apn_name*)

Syntax Description **`authorize-with-hss lma [ report-ipv6-addr | s6b-aaa-group`** *`group_name`* **`]`**

report-ipv6-addr

Specify to enable IPv6 reporting through AAR towards S6b interface.

s6b-aaa-group *group_name*

Specify the AAA group name for S6b authorization.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to enable IPv6 reporting through AAR towards S6b.

apn cc-profile

Configures the subscriber charging characteristics profile parameters.

Command Modes Exec > Global Configuration (config) > APN Configuration (config-apn-*apn_name*)

Syntax Description **`cc-profile`** *`index`* **`{ credit-control-group`** *`cc_group_name`* **`| prepaid-prohibited }`**

cc-profile *index*

Specify the charging characterstics profile index.

Must be an integer.

-Or-

Must be one of the following:

- **any**

credit-control-group *cc_group_name*

Specify name of the credit control group.

Must be a string of 1-63 characters.

prepaid-prohibited

Specify to disable prepaid for the configured profile index.

Usage Guidelines Use this command to configure the subscriber charging characteristics profile parameters.

apn content-filtering category

Configures Content Filtering category.

Command Modes Exec > Global Configuration (config) > APN Configuration (config-apn-*apn_name*)

Syntax Description **`content-filtering category policy-id`** *`policy_id`*

policy-id *policy_id*

Specify the Content Filtering Policy ID.

Must be an integer in the range of 1-4294967295.

Usage Guidelines Use this command to configure Content Filtering category.

apn data-tunnel

Configures the data tunnel MTU parameter.

Command Modes Exec > Global Configuration (config) > APN Configuration (config-apn-*apn_name*)

Syntax Description **`data-tunnel mtu`** *`max_transmission_unit`*

mtu *max_transmission_unit*

Specify the data tunnel MTU value, in octets.

Must be an integer.

Usage Guidelines Use this command to configure the data tunnel MTU parameter.

apn gtpp group

Enables and configures the GTPP group to be used by this APN.

Command Modes Exec > Global Configuration (config) > APN Configuration (config-apn-*apn_name*)

Syntax Description **gtpp group** *gtpp_group_name*

group *gtpp_group_name*

Specify name of the GTPP group.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to enable and configure the GTPP group to be used by this APN.

apn ip access-group

Configures an IPv4/IPv6 access group for the current APN profile.

Command Modes Exec > Global Configuration (config) > APN Configuration (config-apn-*apn_name*)

Syntax Description **ip access-group** *acl_group_name* **[in | out]**

access-group *acl_group_name*

Specify name of the IPv4/IPv6 access group.

Must be a string of 1-47 characters.

in

Specify the access group as inbound.

out

Specify the access group as outbound.

Usage Guidelines Use this command to apply a single IPv4/IPv6 access control list to multiple subscribers via this APN for inbound or outbound IPv4/IPv6 traffic. If no traffic direction is specified, the selected access control list will be applied to both directions.

You can configure a maximum of eight elements with this command.

apn ip source-violation

Enables or disables packet source validation for the current APN.

Command Modes Exec > Global Configuration (config) > APN Configuration (config-apn-*apn_name*)

Syntax Description **ip source-violation ignore**

ignore

Disables source address checking for the APN.

Usage Guidelines Use this command to enable packet 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.

Example

The following command enables source address validation for the APN and configures a drop-limit of 15:

```
ip source-violation check drop-limit 15
```

apn ppp

Configures PPP parameters for specified APN.

Command Modes Exec > Global Configuration (config) > APN Configuration (config-apn-*apn_name*)

Syntax Description **ppp mtu** *max_transmission_unit*

mtu *max_transmission_unit*

Specify the maximum transmission unit. Default Value: 1500.

Must be an integer.

Usage Guidelines Use this command to configure the PPP parameters for specified APN.

apn timeout

Configures session timeout parameters for the current APN.

Command Modes Exec > Global Configuration (config) > APN Configuration (config-apn-*apn_name*)

Syntax Description **timeout idle** *idle_timeout*

idle *idle_timeout*

Specify the session idle timeout period for the current APN.

Must be an integer in the range of 0-4294967295.

Usage Guidelines Use this command to configure the session timeout parameters for the current APN.

cd

Configures the change directory command.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **cd** *directory*.**ssh**

directory

Specify the directory path.

Must be an alphanumeric string.

Usage Guidelines Use this command to configure the change directory command.

cdl clear

Deletes the CDL database sessions.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **cdl clear sessions [db-name** *db_name* **| filter { condition { ends-with | match | starts-with } key** *key_value* **} | map-id** *map_id* **]**

db-name *db_name*

Specifies the database name to be queried for deleting the data.

Must be a string of 1 to 16 characters.

key *key_value*

Specifies the query value.

Must be a string of 0 to 512 characters.

map-id *map_id*

Specifies the map ID to delete the data for a map.

Must be an integer in the range of 0-1024.

filter condition { ends-with | match | starts-with }

Specify the query expression to filter the results of query.

Usage Guidelines Use this command to clear the CDL database sessions.

cdl show sessions

Displays the CDL session details.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **cdl show sessions count { detailed { db-name** *db_name* **| filter { condition { ends-with | match | starts-with } | key** *key_value* **} | limit** *limit* **| map-id** *map_id* **} | summary { db-name** *db_name* **| filter { condition { ends-with | match | starts-with } | key** *key_value* **} | limit** *limit* **| map-id** *map_id* **}**

count

Displays the session count information.

detailed

Displays the session details with data.

summary

Displays the session details without data.

db-name *db_name*

Specifies the database name to be queried for displaying the session details.

Must be a string of 1 to 16 characters.

key *key_value*

Specifies the query value.

Must be a string of 0 to 512 characters.

map-id *map_id*

Specifies the map ID to display the data for a map.

Must be an integer in the range of 0-1024.

limit *limit*

Specifies the maximum number of records to display.

Must be an integer in the range of 1 to 500 characters.

filter condition { ends-with | match | starts-with }

Specify the query expression to filter the results of query.

Usage Guidelines Use this command to display the session details.

cdl show status

Displays the status of the CDL database.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **cdl status db-name** *db_name*

db-name *db_name*

Specifies the database name for displaying the corresponding status.

Must be a string of 1 to 16 characters.

Usage Guidelines Use this command to display the status of the queried database.

clear diameter routes dynamic

Clears the dynamic routes.

Command Modes Exec

Syntax Description **clear diameter routes dynamic [interface** *interface_name* **profilename** *profile_name* **]**

Interface *interface_name*

Specify the diameter interface name, example: Gx or Gy. This is mandatory field.

profilename *profile_name*

Specify the profile name and is an optional field. If the profile-name is not provided, then it clears all the dynamic routes for the interface.

Usage Guidelines Use this command to clears the diameter dynamic routes.

clear ipam

Clears IPAM operational data.

Command Modes Exec

Syntax Description **clear ipam**

Usage Guidelines Use this command to clear IPAM operational data.

clear ipam

Clears the IPAM operational data.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **clear ipam**

Usage Guidelines Use this command to clear the IPAM operational data.

clear lawful-intercept stats

Clears Lawful Interception IRI Send and IRI Drop counters.

Command Modes Exec

Syntax Description **clear lawful-intercept stats**

Usage Guidelines Use this command to clear Lawful Interception IRI Send and IRI Drop counters.

clear subscriber

Clears subscriber data.

Command Modes Exec

Syntax Description **clear subscriber { all | gr-instance** *gr_instance* **| imei** *imei_id* **| namespace** *namespace* **| nf-service** *nf_service* **| supi** *supi_id* **|** *config_specific_options* **}**

all

Specify to remove all subscriber data.

gr-instance *gr_instance*

Specify the subscribers from the GR instance.

imei *imei_id*

Specify the International Mobile Equipment Identity.

Must be a string of 15-16 characters.

imsi *imsi*

Specify the International Mobile Subscriber Identifier (IMSI).

Must be a string.

msid *msid*

Specify the Mobile Station Identifier (MSID).

Must be a string.

namespace *namespace*

NOTE: This keyword is deprecated, use nf-service instead. Specifies the product namespace under which to search.

Default Value: cisco-mobile-infra:none.

nf-service *nf_service*

Specify the network function service under which to search.

Default Value: cisco-mobile-infra:none.

supi *supi_id*

Specify to remove subscriber data associated with the SUPI ID.

Must be a string of 1-63 characters.

clear subscriber supi-opt

Clears subscriber data based on SUPI.

Command Modes

Exec

Syntax Description

clear subscriber supi *supi_id* **[psid** *pdu_session_id* **| ebi** *eps_bearer_id* **| reactivation { false | true } }]**

all

Specify to remove all subscriber data.

ebi *eps_bearer_id*

Specify the EPS Bearer ID.

Must be a string.

gr-instance *gr_instance*

Specify the subscribers from the GR instance.

imei *imei_id*

Specify the International Mobile Equipment Identity.

Must be a string of 15-16 characters.

imsi *imsi*

Specify the International Mobile Subscriber Identifier (IMSI).

Must be a string.

msid *msid*

Specify the Mobile Station Identifier (MSID).

Must be a string.

namespace *namespace*

NOTE: This keyword is deprecated, use nf-service instead. Specifies the product namespace under which to search.

Default Value: cisco-mobile-infra:none.

nf-service *nf_service*

Specify the network function service under which to search.

Default Value: cisco-mobile-infra:none.

psid *pdu_session_id*

Specify the PDU Session ID.

Must be an integer in the range of 1-255.

reactivation { false | true }

Specify if reactivation is requested.

Must be one of the following:

- **false**
- **true**

supi *supi_id*

Specify to remove subscriber data associated with the SUPI ID.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to clear subscriber data.

Usage Guidelines Use this command to clear subscriber data based on SUPI.

clear subscriber imsi-opt

Clears subscriber data based on IMSI.

Command Modes Exec

Syntax Description **clear subscriber imsi-options** *imsi_option* **[ebi** *eps_bearer_id* **]**

ebi *eps_bearer_id*

Specify the EPS Bearer ID.

Must be a string.

Usage Guidelines Use this command to clear subscriber data based on IMSI.

clear subscriber supi-opt

Clears subscriber data based on SUPI.

Command Modes Exec

Syntax Description **`clear subscriber supi`** *`supi_id`* **`[ psid`** *`pdu_session_id`* **`| ebi`** *`eps_bearer_id`* **`| reactivation { false | true } } ]`**

ebi *eps_bearer_id*

Specify the EPS Bearer ID.

Must be a string.

psid *pdu_session_id*

Specify the PDU Session ID.

Must be an integer in the range of 1-255.

reactivation { false | true }

Specify if reactivation is requested.

Must be one of the following:

- **false**
- **true**

clear ipam

Clears IPAM operational data.

Command Modes Exec

Syntax Description **`clear ipam`**

clear lawful-intercept

Usage Guidelines Use this command to clear subscriber data based on SUPI.

Usage Guidelines Use this command to clear IPAM operational data.

client http header

Configures HTTP header parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **client http header user-agent** *user_agent_header*

user-agent *user_agent_header*

Specify the user agent header.

Must be one of the following:

- **app-name**
- **cluster-name**
- **disable**

Default Value: app-name.

Usage Guidelines Use this command to configure HTTP header parameters.

client http ping

Configures HTTP ping parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **client http ping { [timeout** *ping_timeout* **] [interval** *ping_interval* **] }**

interval *ping_interval*

Specify, in milliseconds, the time interval between two HTTP pings.

Must be an integer in the range of 0-30000.

Default Value: 10000.

timeout *ping_timeout*

Specify, in milliseconds, the ping timeout duration to detect if remote host is down.

Must be an integer in the range of 0-15000.

Default Value: 5000.

Usage Guidelines Use this command to configure HTTP ping parameters.

client inbound interface

Configures inbound client interface parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **`client inbound interface`** *`interface_name`*

interface *interface_name*

Specify name of the interface.



Note Specify *scp* interface to detect a dead SCP.

Usage Guidelines Use this command to configure inbound client interface parameters. The CLI prompt changes to the Interface Configuration mode (config-interface-<interface_name>).

client inbound interface limit overload

Configures Overload configuration parameters.

Command Modes Exec > Global Configuration (config) > Interface Configuration (config-interface-*interface_name*)

Syntax Description **`limit overload reject-code`** *`response_code`*

reject-code *response_code*

Specify the response code to be used when pending limit exceeds.

Must be an integer.

Usage Guidelines Use this command to configure Overload configuration parameters.

client inbound interface limit pending

Configures pending limit configuration.

Command Modes Exec > Global Configuration (config) > Interface Configuration (config-interface-*interface_name*)

Syntax Description **`limit pending request`** *`max_pending_request_limit`*

request *max_pending_request_limit*

Specify the maximum pending request limit to allow.

Must be an integer.

Default Value: 10240.

Usage Guidelines Use this command to configure pending limit configuration.

client inbound limit overload

Configures Overload configuration parameters.

Command Modes Exec > Global Configuration (config) > Interface Configuration (config-interface-*interface_name*)

Syntax Description **limit overload reject-code** *response_code*

reject-code *response_code*

Specify the response code to be used when pending limit exceeds.

Must be an integer.

Usage Guidelines Use this command to configure Overload configuration parameters.

client inbound limit pending

Configures pending limit configuration.

Command Modes Exec > Global Configuration (config) > Interface Configuration (config-interface-*interface_name*)

Syntax Description **limit pending request** *max_pending_request_limit*

request *max_pending_request_limit*

Specify the maximum pending request limit to allow.

Must be an integer.

Default Value: 10240.

Usage Guidelines Use this command to configure pending limit configuration.

client outbound host ping

Configures outbound host ping parameter.

Command Modes Exec > Global Configuration (config)

Syntax Description **client outbound host ping { [timeout** *ping_timeout* **] [interval** *ping_interval* **] [backoff** *backoff_interval* **] }**

Command Modes Exec > Global Configuration (config) > Interface Configuration (config-interface-*interface_name*)

Syntax Description **host ping { [timeout** *ping_timeout* **] [interval** *ping_interval* **] }**

backoff *backoff_interval*

Specify, in milliseconds, the backoff time interval to wait when remote host was detected down before start pinging again.

Must be an integer in the range of 0-3600000.

Default Value: 0.

interval *ping_interval*

Specify, in milliseconds, the time interval between two pings.

Must be an integer in the range of 0-30000.

Default Value: 0.

timeout *ping_timeout*

Specify, in milliseconds, the ping timeout duration to detect remote host down.

Must be an integer in the range of 0-15000.

Default Value: 0.

Usage Guidelines Use this command to configure outbound host ping parameter.

client outbound interface

Configures outbound client interface parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **client outbound interface** *interface_name*

interface *interface_name*

Specify the interface.

Usage Guidelines Use this command to configure outbound client interface parameters. The CLI prompt changes to the Interface Configuration mode (config-interface-<interface_name>).

client outbound interface host ping

Configures outbound host ping parameter.

Command Modes Exec > Global Configuration (config)

Syntax Description **client outbound host ping { [timeout** *ping_timeout* **] [interval** *ping_interval* **] [backoff** *backoff_interval* **] }**

Command Modes Exec > Global Configuration (config) > Interface Configuration (config-interface-*interface_name*)

Syntax Description **host ping { [timeout** *ping_timeout* **] [interval** *ping_interval* **] }**

backoff *backoff_interval*

Specify, in milliseconds, the backoff time interval to wait when remote host was detected down before start pinging again.

Must be an integer in the range of 0-3600000.

Default Value: 0.

interval *ping_interval*

Specify, in milliseconds, the time interval between two pings.

Must be an integer in the range of 0-30000.

Default Value: 0.

timeout *ping_timeout*

Specify, in milliseconds, the ping timeout duration to detect remote host down.

Must be an integer in the range of 0-15000.

Default Value: 0.

Usage Guidelines Use this command to configure outbound host ping parameter.

client outbound interface limit consecutive failure

Configures consecutive failure configuration parameters.

Command Modes Exec > Global Configuration

Syntax Description **consecutive failure count** *failure_limit_count* **codes** *failure_codes*

codes *failure_codes*

Specify the list of failure codes to be considered, such as timeout, 503, etc.

Must be a string.

You can configure a maximum of 10 elements with this keyword.

count *failure_limit_count*

Specify the consecutive failure limit count to detect remote host as down.

Must be an integer.

Default Value: 0.

Usage Guidelines Use this command to configure consecutive failure configuration parameters.

client outbound interface limit pending

Configures pending limit configuration.

Command Modes Exec > Global Configuration (config)

Syntax Description **`client outbound limit pending response`** *`response_message_limit`*

Command Modes Exec > Global Configuration (config) > Interface Configuration (config-interface-*interface_name*)

Syntax Description **`pending response`** *`response_message_limit`*

response *response_message_limit*

Specify the pending response message limit to detect remote host as down.

Must be an integer.

Default Value: 1024.

Usage Guidelines Use this command to configure pending limit configuration.

client outbound limit consecutive failure

Configures consecutive failure configuration parameters.

Command Modes Exec > Global Configuration

Syntax Description **`consecutive failure count`** *`failure_limit_count`* **`codes`** *`failure_codes`*

codes *failure_codes*

Specify the list of failure codes to be considered, such as timeout, 503, etc.

Must be a string.

You can configure a maximum of 10 elements with this keyword.

count *failure_limit_count*

Specify the consecutive failure limit count to detect remote host as down.

Must be an integer.

Default Value: 0.

Usage Guidelines Use this command to configure consecutive failure configuration parameters.

client outbound limit pending

Configures pending limit configuration.

Command Modes Exec > Global Configuration (config)

Syntax Description **client outbound limit pending response** *response_message_limit*

Command Modes Exec > Global Configuration (config) > Interface Configuration (config-interface-*interface_name*)

Syntax Description **pending response** *response_message_limit*

response *response_message_limit*

Specify the pending response message limit to detect remote host as down.

Must be an integer.

Default Value: 1024.

Usage Guidelines Use this command to configure pending limit configuration.

commit

Configures the commit parameters.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **commit [abort { persist-id** *persist_id* **} | confirm { persist-id** *persist_id* **} | persist-id** *persist_id* **]**

abort persist-id *persist_id*

Specify to abort commit. Specify the persistence ID for the commit operation.

Must be an integer.

confirm persist-id *persist_id*

Specify to confirm commit. Specify the persistence ID for the commit operation.

Must be an integer.

persist-id *persist_id*

Specify the persistence ID for the commit operation.

Must be an integer.

Usage Guidelines Use this command to configure the commit parameters.

compare

Compares the running configuration to another configuration or a file.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **compare file { *filename*[.kube | .ssh/] | *configuration* }**

***filename*[.kube | .ssh/]**

Specify the file name or the directory path of the file to be compared.

Must be a string.

configuration

Specify the desired configuration to be compared against.

Must be a string.

Usage Guidelines Use this command to compare the files.

config

Manipulates the software configuration information.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **config [exclusive | no-confirm | shared | terminal]**

exclusive

Specify to enter the exclusive configuration mode.

no-confirm

Specify to apply the command without asking for confirmation.

shared

Specify to enter the shared configuration mode.

terminal

Specify to enter the terminal configuration mode.

Usage Guidelines Use this command to manipulate the software configuration information.

config-error info

Displays configuration error information.

Command Modes Exec

Syntax Description **`show config-error [ info ]`**

Usage Guidelines Use this command to view configuration error information.

datastore dbs

Configures DBS parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **`datastore dbs`** *`dbs_name`*

dbs *dbs_name*

Specify name of the DBS.

Must be a string.

Usage Guidelines Use this command to configure the DBS parameters.

datastore dbs endpoints

Configures endpoint parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **`datastore session-db endpoints`** *`host_name`* **`port`** *`port_number`*

Command Modes Exec > Global Configuration (config) > DBS Configuration (config-dbs-*dbs_name*)

Syntax Description **`endpoints`** *`host_name`* **`port`** *`port_number`*

endpoints *host_name*

Specify name of the host.

Must be a string.

port *port_number*

Specify the port number.

Must be an integer.

Usage Guidelines Use this command to configure endpoint parameters.

datastore notification-ep

Configures notification endpoint parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **datastore notification-ep { [host** *host_name* **] [port** *port_number* **] }**

host *host_name*

Specify name of the host.

Must be a string.

port *port_number*

Specify the port number.

Must be an integer.

Usage Guidelines Use this command to configure notification endpoint parameters.

datastore session-db

Configures Session DB parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **datastore session-db slice-name** *slice_name*

slice-name *slice_name*

Specify name of the slice.

Must be a string.

Usage Guidelines Use this command to configure Session DB parameters.

datastore session-db endpoints

Configures endpoint parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **datastore session-db endpoints** *host_name* **port** *port_number*

Command Modes Exec > Global Configuration (config) > DBS Configuration (config-dbs-*dbs_name*)

Syntax Description **endpoints** *host_name* **port** *port_number*

endpoints *host_name*

Specify name of the host.

Must be a string.

port *port_number*

Specify the port number.

Must be an integer.

Usage Guidelines Use this command to configure endpoint parameters.

deployment

Configures the deployment parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **deployment [app-name** *application_name* **| cluster-name** *cluster_name* **| dc-name** *datacenter_name* **| logical-nf-instance-id** *logical_nf_instance_id* **| model** *deployment_model* **]**

app-name *application_name*

Specify name of the application.

Must be a string.

cluster-name *cluster_name*

Specify name of the cluster.

Must be a string.

dc-name *datacenter_name*

Specify name of the datacenter.

Must be a string.

logical-nf-instance-id *logical_nf_instance_id*

Specify the logical NF instance ID.

Must be an integer.

Default Value: 0.

model *deployment_model*

Specify the deployment model.

Must be one of the following:

- **small**

Usage Guidelines Use this command to configure the deployment parameters.

deployment resource

Configures the deployment CPU resource parameter.

Command Modes Exec > Global Configuration (config) > Deployment Configuration (config-deployment)

Syntax Description **resource cpu** *cpu_size*

cpu *cpu_size*

Specify the CPU size in millicores.

Must be an integer in the range of 2000-1000000.

Default Value: 18000.

Usage Guidelines Use this command to configure the deployment CPU resource parameter.

describe

Displays the command information.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **describe** *command*

command

Specify the command name to display detailed information about the command.

The command must be one of the following:

- **aaa**
- **cd**
- **cdl**
- **commit**
- **compare**
- **config**
- **describe**

- **dump**
- **exit**
- **help**
- **history**
- **id**
- **idle-timeout**
- **ignore-leading-space**
- **job**
- **leaf-prompting**
- **license**
- **logout**
- **monitor**
- **no**
- **paginate**
- **quit**
- **rcm**
- **screen-length**
- **screen-width**
- **send**
- **show**
- **show-defaults**
- **smiuser**
- **system**
- **terminal**
- **timestamp**
- **who**

Usage Guidelines Use this command to display the command specific information.

diagnostics info

Displays diagnostics information.

Command Modes Exec

Syntax Description **`show diagnostics [ info ]`**

Usage Guidelines Use this command to view diagnostics information.

dump

Removes the transaction history.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **`dump transactionhistory`**

Usage Guidelines Use this command to remove the transaction history.

dump core

Enables and configures inconsistency checks on session data.

Command Modes Exec > Global Configuration (config)

Syntax Description **`dump core [ [ count`** *`max_core_count_per_interval`* **`] [ expires`** *`expiration_time`* **`] [ file-detail`** *`file_name_line_number`* **`] [ interval`** *`interval_duration`* **`] [ pod-name`** *`pod_names`* **`] ]`**

count *max_core_count_per_interval*

Specify the maximum number of times core can be generated in an interval.

Must be an integer in the range of 0-50.

expires *expiration_time*

Specify the time after which the core agent will stop core dump generation. For example, 2020-03-24T23:15:00+05:30.

Must be a string in the date-and-time pattern. For information on the date-and-time pattern, see the *Input Pattern Types* chapter.

file-detail *file_name_line_number*

Specify the file name and line number to specific core dump. For example, procedures/pduim/procedure.go:1902.

Must be a string.

You can configure a maximum of 10 elements with this keyword.

interval *interval_duration*

Specify the duration of the interval in minutes.

Must be an integer in the range of 1-3600.

pod-name *pod_names*

Specify the names of the pods to enable core dump.

Must be a string.

Usage Guidelines Use this command to enable and configure inconsistency checks on session data.

dump transactionhistory

Creates dump of transaction history.

Command Modes Exec

Syntax Description **`dump transactionhistory`**

Usage Guidelines Use this command to create dump of transaction history.

edr

Configures EDR parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **`edr { [ reporting`** *`reporting_status`* **`] [ all | subscribers`** *`subscribers_for_edr_reporting`* **`] }`**

reporting *reporting_status*

Specify to enable or disable EDR reporting.

Must be one of the following:

- **disable**
- **enable**

Default Value: disable.

reporting all

Specify to enable EDR reporting for all subscribers.

subscribers *subscribers_for_edr_reporting*

Specify the subscribers for whom EDR reporting must be enabled.

Must be a string.

You can configure a maximum of 10 elements with this keyword.



Note The **edr reporting all** command takes precedence over the **edr reporting subscribers** command when enabled.

Usage Guidelines Use this command to configure EDR parameters.

edr file files

Configures EDR file parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **edr file { transaction | transaction-collision } [reporting** *reporting_status* **] [verbose** *verbosity_status* **]**

reporting *reporting_status*

Specify to enable or disable reporting of this file.

Must be one of the following:

- **disable**
- **enable**

Default Value: disable.

verbose *verbosity_status*

Specify to enable or disable field description or long names in the file.

Must be one of the following:

- **disable**
- **enable**

Default Value: disable.

{ transaction | transaction-collision }

Specify name of the EDR file.

Usage Guidelines Use this command to configure EDR file parameters.

edr file files disable

Disables procedure IDs.

Command Modes Exec > Global Configuration (config) > EDR File Configuration (config-file-*transaction_transaction-collision*)

Syntax Description **`disable procedure-id`** *`procedure_ids`*

procedure-id *procedure_ids*

Specify the procedure ID value(s)/name(s).

Must be a string.

Usage Guidelines Use this command to disable specific procedure IDs.

edr file files flush

Configures EDR file flush parameters.

Command Modes Exec > Global Configuration (config) > EDR File Configuration (config-file-*transaction_transaction-collision*)

Syntax Description **`flush interval`** *`file_flush_interval`*

interval *file_flush_interval*

Specify, in milliseconds, the file flush interval.

Must be an integer.

Default Value: 1000.

Usage Guidelines Use this command to configure the EDR file flush parameters.

edr file files limit

Configures EDR file limit parameters.

Command Modes Exec > Global Configuration (config) > EDR File Configuration (config-file-*transaction_transaction-collision*)

Syntax Description **`limit { [ count`** *`max_files_to_preserve`* **`] [ size`** *`max_single_file_size`* **`] }`**

count *max_files_to_preserve*

Specify the maximum number of files to be preserved.

Must be an integer.

Default Value: 10.

size *max_single_file_size*

Specify the maximum single file size limit in MB.

Must be an integer.

Default Value: 100.

Usage Guidelines Use this command to configure the EDR file limit parameters.

edr file files procedure-id disable-event-id

Disables transaction-level procedure ID configuration.

Command Modes Exec > Global Configuration (config) > EDR File Configuration (config-file-*transaction_transaction-collision*)

Syntax Description **`procedure-id`** *`procedure_id`*

procedure *procedure_id*

Specify the procedure ID value/name.

Must be a string.

Usage Guidelines Use this command to disable transaction-level procedure ID configuration.

edr file files procedure-id disable-event-id disable-inner disable

Disables event IDs.

Command Modes Exec > Global Configuration (config) > EDR File Configuration (config-file-*transaction_transaction-collision*) > Procedure ID Configuration (config-procedure-id-*procedure_id*)

Syntax Description **`disable event-id`** *`event_ids`*

event-id *event_ids*

Specify the event ID value(s)/name(s).

Must be a string.

Usage Guidelines Use this command to disable event IDs.

edr file files procedure-id disable-event-id disable-inner event-id disable-field-id

Disables procedure-level event ID configuration.

Command Modes Exec > Global Configuration (config) > EDR File Configuration (config-file-*transaction_transaction-collision*) > Procedure ID Configuration (config-procedure-id-*procedure_id*)

Syntax Description **`event-id`** *`event_id`*

event *event_id*

Specify the event ID value/name.

Must be a string.

Usage Guidelines Use this command to disable procedure-level event ID configuration.

edr file files procedure-id disable-event-id disable-inner event-id disable-field-id disable

Disables field IDs.

Command Modes Exec > Global Configuration (config) > EDR File Configuration (config-file-*transaction_transaction-collision*) > Procedure ID Configuration (config-procedure-id-*procedure_id*)

Syntax Description **`disable field-id`** *`field_ids`*

field-id *field_ids*

Specify the field ID value(s)/name(s).

Must be a string.

Usage Guidelines Use this command to disable field IDs.

edr file transaction field priorityClass

Configures the priority class of the transaction EDR file.

Command Modes Exec > Global Configuration (config)

Syntax Description **`[ no ] edr file transaction field priorityClass`**

field priorityClass

Specify the priority class of the message. The message can be a default priority message or a high-priority message. Enabling this CLI displays an additional field in the EDR transaction files with an additional field containing one of the following two values:

- DefaultPriority
- HighPriority

Usage Guidelines Use this command to configure the priority class of the transaction EDR file.

endpoint all

Displays endpoint status information.

Command Modes Exec

Syntax Description **show endpoint [all]**

Usage Guidelines Use this command to view endpoint status information.

endpoint info

Displays endpoint information.

Command Modes Exec

Syntax Description **show endpoint info [** *endpoint_name* **|** *endpoint_address* **| Interface** *interface_name* **| grInstance** *gr_instance_id* **| internal** *type_of_endpoint* **| startTime** *start_time* **| status** *endpoint_status* **| stoppedTime** *stop_time* **| type** *endpoint_type* **]**

Interface *interface_name*

Specify the interface name of the endpoint.

Must be a string.

grInstance *gr_instance_id*

Specify the GR instance ID.

Must be a string.

internal *type_of_endpoint*

Specify whether the endpoint is of internal or external type.

Must be a string.

startTime *start_time*

Specify the time at which the endpoint started.

Must be a string.

status *endpoint_status*

Specify the current status of the endpoint.

Must be a string.

stoppedTime *stop_time*

Specify the time at which the endpoint stopped.

Must be a string.

type *endpoint_type*

Specify the endpoint type.

Must be a string.

endpoint_address

Specify the host address and port number.

Must be a string.

endpoint_name

Specify the name of the endpoint.

Must be a string.

Usage Guidelines Use this command to view endpoint information.

exit

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

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `exit`

Usage Guidelines Use this command to exit the current configuration mode and return to the previous configuration mode. When used in the Exec mode, exits the management session.

geo maintenance

Configures Geo Admin Controller to enable or disable maintenance mode.

Command Modes Exec

Syntax Description `maintenance enable { false | true }`

enable { false | true }

Specify whether to enable or disable maintenance mode. To enable, set to true.

Must be one of the following:

- **false**
- **true**

Default Value: false.

Usage Guidelines Use this command to configure Geo Admin Controller to enable or disable maintenance mode.

geo replication-pull

geo replication-pull pulls the replication data from the peer rack and syncs it with the local rack.

Command Modes Exec

Syntax

geo replication-pull instance-id *gr_instanceId*

geo replication-pull

It pulls the replication data from the peer rack and syncs it with the local rack.

instance-id *instance_id*

Specify the instance ID for geo command.

Usage Guidelines Use this command to pull the replication data from the peer rack and sync it with the local rack.

geo reset-role

Configures Geo Admin Controller for reset role.

Command Modes Exec

Syntax Description **geo reset-role instance-id** *instance_id* **role** *new_role*

instance-id *instance_id*

Specify the instance ID for geo command.

role *new_role*

Specify the new role for the specified site.

Usage Guidelines Use this command to configure Geo Admin Controller for reset role.

geo switch-role

Geo switch-role switches the role to peer rack.

Command Modes Exec

Syntax Description **geo switch-role instance-id** *instance_id* **role** *new_role* **[failback-interval** *failback_interval* **]**

instance-id *instance_id*

Specify the instance ID for the geo command.

role *new_role*

Specify the new role for the specified site.

[failback-interval *failback_interval*]

The recommended value is 0.



Note The CLI **[failback-interval]** is an optional command to provide backward compatibility of upgrades between releases. It is deprecated from the current release and will be discontinued from the subsequent releases.

Usage Guidelines Use this command to switch the role to peer rack.

geomonitor podmonitor pods

Configures configuration of pods to be monitored.

Command Modes Exec > Global Configuration (config)

Syntax Description **geomonitor podmonitor pods** *pod_name* **retryCount** *retry_count* **retryInterval** *retry_interval* **retryFailOverInterval** *retry_interval* **failedReplicaPercent** *failed_replica_precentage*

failedReplicaPercent *failed_replica_precentage*

Specify the percentage of failed replica after which GR failover will get triggered.

Must be an integer in the range of 10-100.

pods *pod_name*

Specify the name of the pod to be monitored.

Must be a string.

retryCount *retry_count*

Specify the counter value to retry if pod failed to ping after which pod is marked as down.

Must be an integer in the range of 1-10.

retryFailOverInterval *retry_interval*

Specify, in milliseconds, the retry interval if pod ping fails.

Must be an integer in the range of 200-10000.

retryInterval *retry_interval*

Specify, in milliseconds, the retry interval if pod ping is successful.

Must be an integer in the range of 200-10000.

Usage Guidelines Use this command to configure configuration of pods to be monitored.

geomonitor remoteclustermonitor

Configures remote cluster monitoring parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **remoteclustermonitor retryCount** *retry_count* **retryInterval** *retry_interval*

retryCount *retry_count*

Specify the counter value to retry if remote clsuter is not reachable. To discable, set to 0.

Must be an integer in the range of 0-10.

Default Value: 3.

retryInterval *retry_interval*

Specify, in milliseconds, the retry interval after which the remote site's status will be fetched.

Must be an integer in the range of 200-50000.

Default Value: 3000.

Usage Guidelines Use this command to configure remote cluster monitoring parameters.

geomonitor trafficMonitor

Configures traffic monitoring parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **trafficMonitor thresholdCount** *threshold_count* **thresholdInterval** *threshold_interval*

thresholdCount *threshold_count*

Specify, in milliseconds, the maximum duration window to hit the threshold count value.

Must be an integer in the range of 0-10000.

Default Value: 0.

thresholdInterval *threshold_interval*

Specify, in milliseconds, the maximum duration window to hit the threshold count value.

Must be an integer in the range of 100-10000.

Default Value: 3000.

Usage Guidelines Use this command to configure traffic monitoring parameters.

geomonitor vipmonitor instance

Configures VIP monitoring parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **vipmonitor instance instance-id** *instance_id*

instance-id *instance_id*

Specify the instance ID.

Must be an integer in the range of 1-8.

Usage Guidelines Configuration of VIPs to be monitored. Use this command to configure the instance ID.

geomonitor vipmonitor instance vips

Configures VIP interface parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **vips vipInterface** *vip_interface* **vipIp** *vip_ip* **vipPort** *vip_port* **retryCount** *retry_count* **retryInterval** *retry_interval* **retryFailOverInterval** *retry_failover_interval*

retryCount *retry_count*

Specify the counter value to retry if VIP failed to ping after which VIP is marked as down.

Must be an integer in the range of 1-10.

retryFailOverInterval *retry_failover_interval*

Specify, in milliseconds, the retry interval if VIP ping fails.

Must be an integer in the range of 200-10000.

retryInterval *retry_interval*

Specify, in milliseconds, the retry interval if VIP ping is successful.

Must be an integer in the range of 200-10000.

vipInterface *vip_interface*

Specify the name of the interface to monitor.

Must be a string.

vipIp *vip_ip*

Specify the IPv4 address.

Must be a string.

vipPort *vip_port*

Specify the diagnostic port number.

Must be an integer.

Usage Guidelines Use this command to configure VIP interface parameters.

group nf-mgmt

Configures NF management group name.

Command Modes Exec > Global Configuration (config)

Syntax Description

```
nf-mgmt mgmt_group_name { nrf-mgmt-group nrf_mgmt_group_name |
failure-handling-profile fh_profile_name | nrf-auth-group nrf_auth_group_name |
locality locality_name | re-register { false | true } }
```

failure-handling-profile *fh_profile_name*

Specify name of the Failure Handling profile for the NRF Management functionality.

Must be a string.

locality *locality_name*

Specify the locality information.

Must be a string.

nf-mgmt *mgmt_group_name*

Specify name of the NRF management group.

Must be a string.

nrf-mgmt-group *nrf_mgmt_group_name*

Specify name of the NRF management group.

Must be a string.

Usage Guidelines Use this command to configure NF management group name.

group nf-mgmt heartbeat

Configures heartbeat interval.

Command Modes Exec > Global Configuration (config)

Syntax Description **heartbeat interval** *heartbeat_interval*

interval *heartbeat_interval*

Specify the heartbeat interval in seconds.

Must be an integer.

Usage Guidelines Use this command to configure the heartbeat interval.

group nrf discovery

Configures NRF discovery group parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **discovery** *group_name* **[nrf-type** *nrf_type* **]**

discovery *group_name*

Specify name of the NRF discovery group.

Must be a string.

nrf-type *nrf_type*

Specify the NRF type.

Must be one of the following:

- **PLMN**: PLMN.
- **SHARED**: SHARED.
- **SLICE-LOCAL**: SLICE-LOCAL.

Usage Guidelines Use this command to configure the NRF discovery group configuration.

group nrf discovery service type nrf

Configures the NRF discovery service name.

Command Modes Exec > Global Configuration (config)

Syntax Description **nrf** *nrf_service_name* **[responsetimeout** *response_timeout* **]**

nrf *nrf_service_name*

Specify name of the NRF discovery service.

Must be one of the following:

- **nnrf-disc**

responsetimeout *response_timeout*

Specify the response timeout interval in milliseconds.

Must be an integer.

Default Value: 2000.

Usage Guidelines Use this command to configure the NRF discovery service name.

group nrf discovery service type nrf endpoint-profile

Configures endpoint profile parameters.

Command Modes Exec > Global Configuration

Syntax Description **endpoint-profile** *endpoint_profile_name* **{ api-uri-prefix** *api_uri_prefix* **| api-root** *api_root* **| uri-scheme** *uri_scheme* **}**

api-root *api_root*

Specify the API root.

Must be a string.

api-uri-prefix *api_uri_prefix*

Specify the API URI prefix.

Must be a string.

endpoint-profile *endpoint_profile_name*

Specify name of the endpoint profile.

Must be a string.

uri-scheme *uri_scheme*

Specify the URI scheme.

Must be one of the following:

- **http**
- **https**

Usage Guidelines Use this command to configure endpoint profile parameters.

group nrf discovery service type nrf endpoint-profile endpoint-name

Configures endpoint parameters.

Command Modes Exec > Global Configuration

Syntax Description **endpoint-name** *endpoint_name* **[priority** *priority* **| capacity** *endpoint_capacity* **]**

capacity *endpoint_capacity*

Specify the endpoint capacity.

Must be an integer in the range of 0-65535.

Default Value: 10.

priority *priority*

Specify the node priority for endpoint.

Must be an integer in the range of 0-65535.

endpoint_name

Specify name of the endpoint.

Must be a string.

Usage Guidelines Use this command to configure endpoint parameters.

group nrf discovery service type nrf endpoint-profile endpoint-name primary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **ip-address { { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

group nrf discovery service type nrf endpoint-profile endpoint-name secondary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **`ip-address { { ipv4`** *`ipv4_address`* **`| ipv6`** *`ipv6_address`* **`} | port`** *`port_number`* **`}`**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

group nrf discovery service type nrf endpoint-profile endpoint-name tertiary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **ip-address { { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

group nrf discovery service type nrf endpoint-profile version uri-version

Configures URI version information.

Command Modes Exec > Global Configuration

Syntax Description **uri-version** *uri_version* **[full-version** *full_version* **]**

full-version *full_version*

Specify the full version in the format *major-version*.*minor-version*.*patch-version*.[alpha-*draft-number*]

Must be a string.

uri-version *uri_version*

Specify the URI version.

Must be a string in the pattern v\d.

Usage Guidelines Use this command to configure URI version information.

group nrf mgmt

Configures the NRF self-management group parameters.

Command Modes Exec > Global Configuration

Syntax Description **mgmt** *group_name* **[nrf-type** *nrf_type* **]**

mgmt *group_name*

Specify name of the NRF self-management group.

Must be a string.

nrf-type *nrf_type*

Specify the NRF type.

Must be one of the following:

- **PLMN**: PLMN.
- **SHARED**: SHARED.
- **SLICE-LOCAL**: SLICE-LOCAL.

Usage Guidelines Use this command to configure the NRF self-management group parameters.

group nrf mgmt service type nrf

Configures the NRF self-management service information.

Command Modes Exec > Global Configuration

Syntax Description **nrf nrf-service-name** *nrf_service_name* **[responsetimeout** *response_timeout* **]**

nrf-service-name *nrf_service_name*

Specify name of the NRF service.

Must be one of the following:

- **nnrf-nfm**

responsetimeout *response_timeout*

Specify the response timeout interval in milliseconds.

Must be an integer.

Default Value: 2000.

Usage Guidelines Use this command to configure the NRF self-management service information.

group nrf mgmt service type nrf endpoint-profile

Configures endpoint profile parameters.

Command Modes Exec > Global Configuration

Syntax Description **endpoint-profile** *endpoint_profile_name* **{ api-uri-prefix** *api_uri_prefix* **| api-root** *api_root* **| uri-scheme** *uri_scheme* **}**

api-root *api_root*

Specify the API root.

Must be a string.

api-uri-prefix *api_uri_prefix*

Specify the API URI prefix.

Must be a string.

endpoint-profile *endpoint_profile_name*

Specify name of the endpoint profile.

Must be a string.

uri-scheme *uri_scheme*

Specify the URI scheme.

Must be one of the following:

- **http**
- **https**

Usage Guidelines Use this command to configure endpoint profile parameters.

group nrf mgmt service type nrf endpoint-profile endpoint-name

Configures name of the endpoint.

Command Modes Exec > Global Configuration

Syntax Description **endpoint-name** *endpoint_name* **[priority** *endpoint_priority* **]**

max-retry-count *max_retry_count*

Specify the maximum retry count.

Must be an integer in the range of 0-10.

Default Value: 3.

priority *endpoint_priority*

Specify the node priority for endpoint.

Must be an integer in the range of 0-65535.

endpoint_name

Specify name of the endpoint.

Must be a string.

Usage Guidelines Use this command to configure the name of the endpoint.

group nrf mgmt service type nrf endpoint-profile endpoint-name primary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **ip-address { { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

group nrf mgmt service type nrf endpoint-profile endpoint-name secondary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **ip-address { { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 ***ipv4_address***

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 ***ipv6_address***

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port ***port_number***

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

group nrf mgmt service type nrf endpoint-profile endpoint-name tertiary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **ip-address { { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 ***ipv4_address***

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

group nrf mgmt service type nrf endpoint-profile version uri-version

Configures version information.

Command Modes Exec > Global Configuration

Syntax Description **uri-version** *uri_version* **[full-version** *full_version* **]**

full-version *full_version*

Specify the full version in the format *major-version.minor-version.patch-version*.[alpha-*draft-number*]

Must be a string.

uri-version *uri_version*

Specify the URI version.

Must be a string in the pattern v\d.

Usage Guidelines Use this command to configure the version information.

gtpp group

Configures GTPP group related parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **gtpp** *gtpp_group_name*

gtpp_group_name

Specify name of the GTPP group.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to configure GTPP group related parameters.

gtpp group gtpp egcdr final-record closing-cause

Configures closing cause for final EGCDR.

Command Modes Exec > Global Configuration (config) > GTPP Group Configuration (config-group-*gtpp_group_name*)

Syntax Description **`gtpp egcdr final-record closing-cause { same-in-all-partials | unique }`**

same-in-all-partials

Specify same closing cause for multiple final EGCDR(s).

unique

Specify unique closing cause for final EGCDR.

Usage Guidelines Use this command to configure closing cause for final EGCDR.

gtpp group gtpp egcdr losdv-max-containers

Configures maximum number of LoSDV containers in one EGCDR.

Command Modes Exec > Global Configuration (config) > GTPP Group Configuration (config-group-*gtpp_group_name*)

Syntax Description **`gtpp egcdr losdv-max-containers`** *`max_containers`*

losdv-max-containers *max_containers*

Specify the number of LOSDV containers.

Must be an integer in the range of 1-255.

Usage Guidelines Use this command to configure the maximum number of LoSDV containers in one EGCDR.

gtpp group gtpp egcdr service-data-flow threshold

Configures service data flow related parameters.

Command Modes Exec > Global Configuration (config) > GTPP Group Configuration (config-group-*gtpp_group_name*)

Syntax Description **`gtpp egcdr service-data-flow threshold interval`** *`duration`*

interval *duration*

Specify the time interval, in seconds, to close the eG-CDR/P-CDR if the minimum time duration thresholds for service data flow containers satisfied in flow-based charging. By default, this option is disabled.

Must be an integer in the range of 60-40000000.

Usage Guidelines Use this command to assign volume or interval values to the interim GCDRs.

gtpp group gtpp egcdr service-data-flow threshold volume

Configures the uplink/downlink volume octet counts for the generation of interim GCDRs.

Command Modes Exec > Global Configuration (config) > GTPP Group Configuration (config-group-*gtpp_group_name*)

Syntax Description **gtpp egcdr service-data-flow threshold volume { [downlink** *bytes* **] [total** *bytes* **] [uplink** *bytes* **] }**

downlink *bytes*

Specify the limit for the number of downlink octets after which the eG-CDR/P-CDR is closed.

Must be an integer in the range of 100000-4000000000.

total *bytes*

Specify the limit for the total number of octets (uplink+downlink) after which the eG-CDR/P-CDR is closed.

Must be an integer in the range of 100000-4000000000.

uplink *bytes*

Specify the limit for the number of uplink octets after which the eG-CDR/P-CDR is closed.

Must be an integer in the range of 100000-4000000000.

Usage Guidelines Use this command to configure the uplink/downlink volume octet counts for the generation of interim GCDRs.

gtpp group gtpp egcdr service-idle-timeout

Enables configuration for service idle out closure of LOSDV container.

Command Modes Exec > Global Configuration (config) > GTPP Group Configuration (config-group-*gtpp_group_name*)

Syntax Description **gtpp egcdr service-idle-timeout { 0 |** *service_idle_timeout* **}**

0

Specify no service-idle-timeout trigger.

Must be one of the following:

- **0**

service_idle_timeout

Specify time limit in seconds for service-idle-timeout.

Must be an integer in the range of 10-86400.

Usage Guidelines Use this command to enable configuration for service idle out closure.

gtpp group gtpp trigger

Configures triggers for CDR.

Command Modes Exec > Global Configuration (config) > GTPP Group Configuration (config-group-*gtpp_group_name*)

Syntax Description **`gtpp trigger { time-limit | volume-limit }`**

time-limit

When this trigger is disabled, no partial record closure occurs when the configured time limit is reached. Default: Enabled.

volume-limit

When this trigger is disabled no partial record closure occurs when volume limit is reached. Default: Enabled.

Usage Guidelines Use this command to configure triggers for CDR.

gtpp group gtpp trigger egcdr

Enables or disables and configures eGCDR-related parameters.

Command Modes Exec > Global Configuration (config) > GTPP Group Configuration (config-group-*gtpp_group_name*)

Syntax Description **`gtpp trigger egcdr max-losdv`**

max-losdv

Enable trigger for eGCDR release at MAX LoSDV containers.

Usage Guidelines Use this command to enable or disable and configure eGCDR-related parameters.

help

Displays help information for a specified command.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **`help`** *`command`*

command

Specify the command name to display the corresponding help information.

The command must be one of the following:

- **aaa**
- **cd**
- **cdl**
- **commit**
- **compare**
- **config**
- **describe**
- **dump**
- **exit**
- **help**
- **history**
- **id**
- **idle-timeout**
- **ignore-leading-space**
- **job**
- **leaf-prompting**
- **license**
- **logout**
- **monitor**
- **no**
- **paginate**
- **quit**
- **rcm**
- **screen-length**
- **screen-width**
- **send**
- **show**
- **show-defaults**
- **smiuser**

- **system**
- **terminal**
- **timestamp**
- **who**

Usage Guidelines Use this command to view help information for a specified command.

history

Configures the command history cache size.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **history** *history_size*

history_size

Specify the command history cache size.

Must be an integer in the range of 0-1000.

Usage Guidelines Use this command to configure the command history cache size.

id

Displays user ID information.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **id**

Usage Guidelines Use this command to view the user ID information.

idle-timeout

Configures the maximum duration a command can remain idle in seconds after which the system automatically terminates the connection.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `idle-timeout duration`

duration

Specify the idle timeout duration in seconds.

Must be an integer in the range of 1-8192.

Usage Guidelines Use this command to configure the maximum duration a command can remain idle.

ignore-leading-space

Configures whether to ignore or consider the leading whitespace at the beginning of a command.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `ignore-leading-space { false | true }`

{ false | true }

Specify false to ignore the leading whitespace, and true to consider it.

Must be either "false" or "true".

Usage Guidelines Use this command to configure whether to ignore or consider leading whitespace at the beginning of a command.

infra metrics experimental

Configures the experimental configuration parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description `infra metrics experimental version experimental_metrics_version`

version *experimental_metrics_version*

Specify the experimental metrics version to be enabled.

Must be an integer in the range of 0-4.

Default Value: 0.

Usage Guidelines Use this command to configure the experimental configuration parameters.

infra metrics verbose verboseLevels

Configures verbose configuration parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **infra metrics verbose podType** *pod_type* **level** *verbose_level*

level *verbose_level*

Specify the default verbosity level.

Must be one of the following:

- **debug**
- **off**
- **production**
- **trace**

Default Value: trace.

podType *pod_type*

Specify the pod type.

Must be one of the following:

- **application**
- **load-balancer**
- **protocol**
- **service**

Usage Guidelines Use this command to configure verbose configuration parameters.

infra metrics verbose verboseLevels metrics metricsList

Configures the metrics verbose level configuration.

Command Modes Exec > Global Configuration (config)

Syntax Description **metrics** *metric_name* **level** *metric_verbose_level* **granular-labels** *granular_labels*

granular-labels *granular_labels*

Specify the granular labels.

Must be a string.

level *metric_verbose_level*

Specify the metric verbosity level.

Must be one of the following:

- **debug**
- **off**
- **production**
- **trace**

Default Value: trace.

metric_name

Specify name of the metric.

Must be a string.

Usage Guidelines Use this command to configure the metrics verbose level configuration.

infra transaction limit

Configures the maximum stage limit per transaction.

Command Modes Exec > Global Configuration (config)

Syntax Description **infra transaction limit stage** *max_stage_limit*

stage *max_stage_limit*

Specify the maximum stage limit per transaction.

Must be an integer.

Default Value: 100.

Usage Guidelines Use this command to configure the maximum stage limit per transaction.

infra transaction limit consecutive same

Configures the maximum consecutive stage limit per transaction.

Command Modes Exec > Global Configuration (config)

Syntax Description **infra transaction limit consecutive same stage** *max_consecutive_stage_limit*

stage *max_consecutive_stage_limit*

Specify the maximum consecutive stage limit per transaction.

Must be an integer.

Default Value: 10.

Usage Guidelines Use this command to configure the maximum consecutive stage limit per transaction.

infra transaction loop

Configures the transaction loop detection parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **infra transaction loop detection** *detection_status*

detection *detection_status*

Specify to enable or disable loop detection.

Must be one of the following:

- **disable**
- **enable**

Default Value: disable.

Usage Guidelines Use this command to configure the transaction loop detection parameter.

infra transaction loop category

Configures the loop category.

Command Modes Exec > Global Configuration (config)

Syntax Description **infra transaction loop category** *loop_category*

category *loop_category*

Specify the category.

Usage Guidelines Use this command to configure the loop category.

infra transaction loop category threshold

Configures the loop detection interval parameter.

Command Modes Exec > Global Configuration (config)

Syntax Description **infra transaction threshold interval** *loop_detect_interval*

interval *loop_detect_interval*

Specify, in seconds, the loop detection interval.

Must be an integer.

Default Value: 5.

Usage Guidelines Use this command to configure the loop detection interval parameter.

infra transaction loop category threshold thresholds

Configures thresholds.

Command Modes Exec > Global Configuration

Syntax Description **thresholds** *threshold_level* **count** *max_transactions* **action** *threshold_action*

action *threshold_action*

Specify the action to take on threshold breach.

Must be one of the following:

- **kill-session**
- **log-event**
- **noop**

Default Value: noop.

count *max_transactions*

Specify the maximum number of transactions for the threshold interval.

Must be an integer.

Default Value: 100.

thresholds *threshold_level*

Specify the threshold level.

Must be one of the following:

- **high**
- **low**

Usage Guidelines Use this command to configure thresholds.

instance instance-id

Configures instance ID.

Command Modes Exec > Global Configuration (config)

Syntax Description **instance instance-id** *instance_id*

id *instance_id*

Specify the instance ID.

Usage Guidelines Use this command to configure the instance ID. The CLI prompt changes to the Instance ID Configuration mode (config-instance-id-<instance_id>).

endpoint-gtpprime

Sets the storage size limit (default 1 GB), which is applicable when **k8s use-volume-claim Pod** is set to true.

Command Modes Exec

Syntax Description

```
instance instance-id instance_id
  endpoint gtpprime
     storage storage_capacity
     replicas replicas_count
     nodes nodes_count
     interface Gz
       vip-ip   vip_ip vip-port
```

endpoint gtpprime

Specifiy the following parameters to configure an endpoint.

- **storage** *storage_capacity*—Specify the storage size of persistent volume in GB. Must be an integer in the range of 1-100.

Note CLI doesn't allow changing storage size while system is running. To change the storage size, bring the system down first.

- **replicas** *replicas_count*—Specify the number of replicas per node. Must be an integer.
- **nodes** *nodes_count*—This property is ignored. You may skip configuring it.
- **interface Gz** : Configure the Gz interface details, such as vip IPv4 address, vip port, vip interface, and VRF details.

Note When the system is active and under the Gz Interface, if there are any add or update **vip** configurations to use a new value, ensure to restart the **udp-proxy**.

Usage Guidelines Use this command to set the storage size limit (default 1 GB), which is applicable when **k8s use-volume-claim Pod** is set to true.

Ensure to configure GTPP profiles charging agent ip address and ports in the Endpoint under the Gz interface.

Note The **gtpp-ep** always ignores **nodes** config. When **k8s single-node** is set to false, it spawns 2 replicas of gtpp-ep in the Active or Standby mode independent of replicas and nodes configuration.

instance instance-id endpoint ep

Configures endpoint parameters.

Command Modes Exec > Global Configuration (config) > Instance ID Configuration (config-instance-id-*instance_id*)

Syntax Description **endpoint** *endpoint_type* **[instancetype** *instance_type* **| loopbackEth** *interface_name_host_ip* **| loopbackPort** *port_number* **| nodes** *node_replicas_for_resiliency* **| replicas** *replicas_per_node* **| internal-vip***{ smf_udp_proxy_internal_vip }***| vip-ip***{ client_ipv4_address }***]**

certificate-name *certificate_alias_name*

Specify the alias name for the certificate.

dscp *dscp_value*

Specify the DSCP value.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

enable-cpu-optimization { false | true }

Specify whether to enable CPU optimization in PFCP and GTP protocol message handling. By default, it is enabled.

Must be one of the following:

- **false**
- **true**

Default Value: true.

enable-go-encdec { false | true }

Specify whether to enable Go-based encoder-decoder in GTP protocol message handling or not. By default, it is disabled.

Must be one of the following:

- **false**
- **true**

Default Value: false.

endpoint *endpoint_type*

Specify the endpoint type.

instancetype *instance_type*

Specify the endpoint local interface type.

Must be one of the following:

- **Dual**
- **IPv4**
- **IPv6**

Default Value: IPv4.

internal-vip *{ smf_udp_proxy_internal_vip }*

Specify the internal VIP.

Must be a string.

vip-ip *{ client_ipv4_address }*

Specify the IP address of the dynamic authorization client. *ipv4_address* must be in standard IPv4 dotted decimal notation.

loopbackEth *interface_name_host_ip*

Specify the endpoint local interface name or host IP address.

Must be a string.

loopbackPort *port_number*

Specify the endpoint local port number.

Must be an integer.

nodes *node_replicas_for_resiliency*

Specify the number of node replicas for resiliency.

Must be an integer.

Default Value: 1.

replicas *replicas_per_node*

Specify the number of replicas per node.

Must be an integer.

Default Value: 1.

storage *persistent_volume_storage_size*

Specify the storage size of the persistent volume in gibibyte (GiB).

Must be an integer in the range of 1-20.

Default Value: 1.

uri-scheme *uri_scheme*

Specify the URI scheme.

Must be one of the following:

- **http**
- **https**

Default Value: http.

Usage Guidelines Use this command to configure endpoint parameters.

instance instance-id endpoint diameter

Configures the Diameter endpoint parameters.

Command Modes Exec > Global Configuration (config) > Instance ID Configuration (config-instance-id-*instance_id***endpoint diameter**)

Syntax Description

```
endpoint diameter [ interface { gx | gy }  [ vip-ip  ip_address [
vip-interface  interface_name| vip-port vip_port | vrf vrf_name ] ] ]
```

endpoint diameter

Specify the endpoint name as Diameter.

interface { gx | gy }

For Diameter endpoint, select **gx** or **gy** interface.

vip-ip *ip_address*

Specify the IPv4 address of the configured endpoint.

vip-interface *interface_name*

Specify the interface name.

Note **vip-interface** is a bonded interface which is associated with VRF.

vip-port *vip_port*

Specify the port number of endpoint.

vrf *vrf_name*

Specify the VRF name defined using global VRF configuration.

instance instance-id endpoint ep cpu

Configures K8 pod CPU configuration.

Command Modes Exec > Global Configuration

Syntax Description **`cpu request`** *`cpu_resource_request`* **`max-process`** *`max_processes`*

max-process *max_processes*

Specify the maximum number of parallel OS threads to use.

Must be an integer in the range of 1-32.

request *cpu_resource_request*

Specify the CPU resource request in millicores.

Must be an integer in the range of 100-1000000.

Usage Guidelines Use this command to configure the K8 pod CPU configuration.

instance instance-id endpoint ep extended-service

Enables service pod to run on Session VM.

Command Modes Exec > Global Configuration

Syntax Description **`extended-service replicas`** *`replicas_per_node`* **`nodes`** *`node_replicas`*

nodes *node_replicas*

Specify the number of node replicas for resiliency.

Must be an integer.

Default Value: 2.

replicas *replicas_per_node*

Specify the number of replicas per node.

Must be an integer.

Default Value: 2.

Usage Guidelines Use this command to enable service pod to run on session VM. Service pods are spawned in Session VM.

instance instance-id endpoint ep heartbeat

Configures PFCP path management.

Command Modes Exec > Global Configuration

Syntax Description **heartbeat interval** *heartbeat_interval* **max-retransmissions** *max_retransmissions* **retransmission-timeout** *retransmission_timeout*

interval *heartbeat_interval*

Specify the heartbeat interval in seconds.

Must be an integer from the following: 0, 60-360.

Default Value: 60.

max-retransmissions *max_retransmissions*

Specify the maximum number of retries for PFCP heartbeat request.

Must be an integer in the range of 0-10.

Default Value: 3.

retransmission-timeout *retransmission_timeout*

Specify the heartbeat retransmission timeout in seconds.

Must be an integer in the range of 1-20.

Default Value: 5.

Usage Guidelines Use this command to configure PFCP path management.

instance instance-id endpoint gtpprime

Configures GTP Prime endpoint parameters.

Command Modes Exec > Global Configuration (config) > Instance ID Configuration (config-instance-id-*instance_id***endpoint gtpprime**)

Syntax Description **endpoint gtpprime [storage** *storage_capacity***| replicas** *replicas_count***| nodes** *nodes_count* **| interface Gz [vip-ip** *vip_ip* **vip-port** *vip-port* **vip-interface** *vip-interface* **vrf** *vrf* **]]**

storage*storage_capacity*

Specify the storage size of persistent volume in GB. Must be an integer in the range of 1-100.

Note CLI doesn't allow changing storage size while system is running. To change the storage size, you must make the system inactive.

replicas *replicas_count*

Specify the number of replicas per node. Must be an integer.

nodes *nodes_count*

(Optional) This property is ignored. You may skip configuring it.

interface Gz [vip-ip *vip_ip* vip-port *vip-port* vip-interface *vip-interface* vrf *vrf*]

Configure the Gz interface details, such as vip IPv4 address, vip port, vip interface, and VRF details.

Note When the system is active and under the Gz interface, if there are any add or update **vip** configurations to use a new value, ensure to restart the **udp-proxy**.

instance instance-id endpoint ep interface

Configures the endpoint interface.

Command Modes Exec > Global Configuration (config) > Instance ID Configuration (config-instance-id-*instance_id*) > Endpoint *endpoint_type* Configuration (config-endpoint-*endpoint_type*)

Syntax Description **interface** *interface_type*

certificate-name *certificate_alias_name*

Specify the alias name for certificate.

dscp *dscp_value*

Specify the DSCP value.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

enable-go-encdec { false | true }

Specify whether to enable Go-based encoder-decoder in GTP protocol message handling. By default, it is enabled.

Must be one of the following:

- **false**
- **true**

Default Value: true.

instancetype *ep_local_interface_type*

Specify the endpoint local interface type.

Must be one of the following:

- **Dual**
- **IPv4**
- **IPv6**

Default Value: IPv4.

interface *interface_type*

Specify the interface type.

loopbackEth *pod_interface*

Specify the pod interface.

Must be a string.

loopbackPort *port_number*

Specify the port number.

Must be an integer.

uri-scheme *uri_scheme*

Specify the URI scheme.

Must be one of the following:

- **http**
- **https**

Default Value: http.

Usage Guidelines Use this command to configure the interface.

instance instance-id endpoint ep interface dispatcher

Displays the dispatcher queue support details for the interface.

Command Modes Exec > Global Configuration (config) > Instance ID Configuration (config-instance-id-*instance_id*) > Endpoint *endpoint_type* Configuration (config-endpoint-*endpoint_type*) > Interface *interface_type* Configuration (config-interface-*interface_type*)

Syntax Description

dispatcher { cache { false | true } | capacity *queue_capacity* **| count** *dispatcher_queues_count* **| expiry** *cache_entry_expiry_duration* **| nonresponsive** *cache_entry_expiry_duration* **| outbound { false | true } |rate-limit** *queue_rate_limit* **| threshold** *outstanding_requests_per_queue_cache* **}**

cache { false | true }

Specify to enable or disable disable retransmission cache support.

Must be one of the following:

- **false**
- **true**

Default Value: false.

capacity *queue_capacity*

Specify the capacity of each queue.

Must be an integer.

Default Value: 5000.

count *dispatcher_queues_count*

Specify the count of dispatcher queues.

Must be an integer.

Default Value: 0.

expiry *cache_entry_expiry_duration*

Specify, in milliseconds, the responded cache entry expiry duration.

Must be an integer.

Default Value: 60000.

nonresponsive *cache_entry_expiry_duration*

Specify, in milliseconds, the non-responsive cache entry expiry duration.

Must be an integer.

Default Value: 30000.

outbound { false | true }

Specify to enable or disable queue support for outbound messages.

Must be one of the following:

- **false**
- **true**

Default Value: true.

rate-limit *queue_rate_limit*

Specify the rate limit for each queue.

Must be an integer.

Default Value: 0.

threshold *outstanding_requests_per_queue_cache*

Specify the outstanding requests per queue cache.

Must be an integer.

Default Value: 30000.

Usage Guidelines Use this command to view dispatcher queue support details for the interface.

instance instance-id endpoint ep interface echo

Configures GTP-C path management.

Command Modes Exec > Global Configuration

Syntax Description **echo interval** *echo_interval* **retransmission-timeout** *retransmission_timeout* **max-retransmissions** *max_retransmissions*

interval *echo_interval*

Specify the echo interval in seconds.

max-retransmissions *max_retransmissions*

Specify the maximum number of retries for GTP echo request.

retransmission-timeout *retransmission_timeout*

Specify the echo retransmission timeout in seconds.

Usage Guidelines Use this command to configure GTP-C path management.

instance instance-id endpoint ep interface heartbeat

Enables PFCP path management.

Command Modes Exec > Global Configuration

Syntax Description **heartbeat interval** *heartbeat_interval* **retransmission-timeout** *retransmission_timeout* **max-retransmissions** *max_retransmissions*

interval *heartbeat_interval*

Specify the heartbeat interval in seconds. To disable, configure to 0.

Must be an integer from the following: 0, 1-3600.

Default Value: 60.

max-retransmissions *max_retransmissions*

Specify the maximum number of retries for PFCP heartbeat request.

Must be an integer in the range of 0-15.

Default Value: 4.

retransmission-timeout *retransmission_timeout*

Specify the heartbeat retransmission timeout in seconds.

Must be an integer in the range of 1-20.

Default Value: 5.

Usage Guidelines Use this command to enable PFCP path management.

instance instance-id endpoint ep interface internal base-port

Configures the internal base-port to start endpoint parameter.

Command Modes Exec > Global Configuration (config) > Instance ID Configuration (config-instance-id-*instance_id*) > Endpoint *endpoint_type* Configuration (config-endpoint-*endpoint_type*)

Syntax Description **`internal base-port start`** *`base_port_to_start_ep`*

start *base_port_to_start_ep*

Specify the base port to start endpoint.

Must be an integer in the range of 1024-65535.

Usage Guidelines Use this command to configure the internal base-port to start endpoint parameter.

instance instance-id endpoint ep interface overload-control client threshold critical

Configures critical threshold parameters for overload control protection.

Command Modes Exec > Global Configuration

Syntax Description **`critical`** *`critical_threshold`* **`action`** *`critical_threshold_action`*

action *critical_threshold_action*

Specify the action to be taken when critical threshold limit is hit.

critical *critical_threshold*

Specify the critical threshold limit for outstanding requests.

Must be an integer in the range of 10-100000.

drop

Specify to drop if threshold is hit.

exclude

Specify to not apply Overload Control Mechanism for priority messages.

message-priority *message_priority*

Specify message priorities higher or equal to the configured value.

Must be an integer in the range of 0-65535.

redirect-code *redirect_status_code*

Specify the redirect status code if threshold is hit.

Must be an integer in the range of 100-600.

redirect

Specify to redirect if threshold is hit.

reject-code *reject_status_code*

Specify reject status code if threshold is hit.

Must be an integer in the range of 100-600.

reject

Specify to reject if threshold is hit.

url *redirection_url*

Specify the redirection URL of new host.

Must be a string.

Usage Guidelines

Use this command to configure critical threshold parameters for overload control protection.

instance instance-id endpoint ep interface overload-control client threshold high

Configures high threshold parameters for overload control protection.

Command Modes

Exec > Global Configuration

Syntax Description

high *high_threshold* **action** *high_threshold_action*

action *high_threshold_action*

Specify the action to be taken when high threshold limit is hit.

drop

Specify to drop if threshold is hit.

exclude

Specify to not apply Overload Control Mechanism for priority messages.

high *high_threshold*

Specify the high threshold limit for outstanding requests.

Must be an integer in the range of 10-100000.

message-priority *message_priority*

Specify message priorities higher or equal to the configured value.

Must be an integer in the range of 0-65535.

redirect-code *redirect_status_code*

Specify the redirect status code if threshold is hit.

Must be an integer in the range of 100-600.

redirect

Specify to redirect if threshold is hit.

reject-code *reject_status_code*

Specify reject status code if threshold is hit.

Must be an integer in the range of 100-600.

reject

Specify to reject if threshold is hit.

url *redirection_url*

Specify the redirection URL of new host.

Must be a string.

Usage Guidelines Use this command to configure high threshold parameters for overload control protection.

instance instance-id endpoint ep interface overload-control client threshold low

Configures low threshold parameters for overload control protection.

Command Modes Exec > Global Configuration

Syntax Description **low** *low_threshold* **action** *low_threshold_action*

action *low_threshold_action*

Specify the action to be taken when low threshold limit is hit.

drop

Specify to drop if threshold is hit.

exclude

Specify to not apply Overload Control Mechanism for priority messages.

low *low_threshold*

Specify the low threshold limit for outstanding requests.

Must be an integer in the range of 10-100000.

message-priority *message_priority*

Specify message priorities higher or equal to the configured value.

Must be an integer in the range of 0-65535.

redirect-code *redirect_status_code*

Specify the redirect status code if threshold is hit.

Must be an integer in the range of 100-600.

redirect

Specify to redirect if threshold is hit.

reject-code *reject_status_code*

Specify reject status code if threshold is hit.

Must be an integer in the range of 100-600.

reject

Specify to reject if threshold is hit.

url *redirection_url*

Specify the redirection URL of new host.

Must be a string.

Usage Guidelines Use this command to configure low threshold parameters for overload control protection.

instance instance-id endpoint ep interface overload-control endpoint threshold critical

Configures critical threshold parameters for overload control protection.

Command Modes Exec > Global Configuration

Syntax Description **`critical`** *`critical_threshold`* **`action`** *`critical_threshold_action`*

action *critical_threshold_action*

Specify the action to be taken when critical threshold limit is hit.

critical *critical_threshold*

Specify the critical threshold limit for outstanding requests.

Must be an integer in the range of 10-100000.

drop

Specify to drop if threshold is hit.

exclude

Specify to not apply Overload Control Mechanism for priority messages.

message-priority *message_priority*

Specify message priorities higher or equal to the configured value.

Must be an integer in the range of 0-65535.

redirect-code *redirect_status_code*

Specify the redirect status code if threshold is hit.

Must be an integer in the range of 100-600.

redirect

Specify to redirect if threshold is hit.

reject-code *reject_status_code*

Specify reject status code if threshold is hit.

Must be an integer in the range of 100-600.

reject

Specify to reject if threshold is hit.

url *redirection_url*

Specify the redirection URL of new host.

Must be a string.

Usage Guidelines Use this command to configure critical threshold parameters for overload control protection.

instance instance-id endpoint ep interface overload-control endpoint threshold high

Configures high threshold parameters for overload control protection.

Command Modes Exec > Global Configuration

Syntax Description **high** *high_threshold* **action** *high_threshold_action*

action *high_threshold_action*

Specify the action to be taken when high threshold limit is hit.

drop

Specify to drop if threshold is hit.

exclude

Specify to not apply Overload Control Mechanism for priority messages.

high *high_threshold*

Specify the high threshold limit for outstanding requests.

Must be an integer in the range of 10-100000.

message-priority *message_priority*

Specify message priorities higher or equal to the configured value.

Must be an integer in the range of 0-65535.

redirect-code *redirect_status_code*

Specify the redirect status code if threshold is hit.

Must be an integer in the range of 100-600.

redirect

Specify to redirect if threshold is hit.

reject-code *reject_status_code*

Specify reject status code if threshold is hit.

Must be an integer in the range of 100-600.

reject

Specify to reject if threshold is hit.

url *redirection_url*

Specify the redirection URL of new host.

Must be a string.

Usage Guidelines Use this command to configure high threshold parameters for overload control protection.

instance instance-id endpoint ep interface overload-control endpoint threshold low

Configures low threshold parameters for overload control protection.

Command Modes Exec > Global Configuration

Syntax Description **low** *low_threshold* **action** *low_threshold_action*

action *low_threshold_action*

Specify the action to be taken when low threshold limit is hit.

drop

Specify to drop if threshold is hit.

exclude

Specify to not apply Overload Control Mechanism for priority messages.

low *low_threshold*

Specify the low threshold limit for outstanding requests.

Must be an integer in the range of 10-100000.

message-priority *message_priority*

Specify message priorities higher or equal to the configured value.

Must be an integer in the range of 0-65535.

redirect-code *redirect_status_code*

Specify the redirect status code if threshold is hit.

Must be an integer in the range of 100-600.

redirect

Specify to redirect if threshold is hit.

reject-code *reject_status_code*

Specify reject status code if threshold is hit.

Must be an integer in the range of 100-600.

reject

Specify to reject if threshold is hit.

url *redirection_url*

Specify the redirection URL of new host.

Must be a string.

Usage Guidelines Use this command to configure low threshold parameters for overload control protection.

instance instance-id endpoint ep interface overload-control msg-type messageConfigs

Configures the message configuration parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description

```
messageConfigs msg-type message_type msg-priority message_priority
pending-request pending_requests priority message_priority queue-size queue_size
```

rate-limit *rate_limit* **reject-threshold** *reject_threshold* **reject-action { drop-req | reject-req }**

msg-priority ***message_priority***

Specify the priority of the message.

Must be one of the following:

- **high**
- **low**

msg-type ***message_type***

Specify the message type.

Must be one of the following:

- **session-report**—This message type is applicable for PFCP endpoint and Sxa interface.
- **create-session-request**—This message type is applicable for GTP endpoint and S11 and S5 interfaces.

pending-request ***pending_requests***

Specify the pending requests count in virtual queue.

Must be an integer.

priority ***message_priority***

Specify the priority of messages to start rejecting if overload is reached.

Must be an integer.

queue-size ***queue_size***

Specify the capacity of each virtual queue.

Must be an integer.

rate-limit ***rate_limit***

Specify the rate limit for virtual queue.

Must be an integer.

reject-threshold ***reject_threshold***

Specify the limit to reject incoming messages if this threshold percentage of pending requests are present.

Must be an integer.

reject-action { drop-req | reject-req }

Specify to drop or reject the create session request messages when the threshold reached for requests in virtual queue.

Usage Guidelines Use this command to configure the message configuration parameters.

Important If the rate limiting configuration is enabled for S11 or S5 interface, it will also apply to emergency calls and WPS sessions, potentially causing Create Session Request messages for these calls to be rejected or dropped.

instance instance-id endpoint ep interface path-failure

Configures the GTP Path Failure Detection Policy profile.

Command Modes Exec > Global Configuration

Syntax Description **`path-failure detection-policy`** *`detection_policy_name`*

detection-policy *detection_policy_name*

Specify the failure detection policy name.

Must be a string.

Usage Guidelines Use this command to configure the GTP Path Failure Detection Policy profile.

instance instance-id endpoint ep interface retransmission

Configures retransmission parameters.

Command Modes Exec > Global Configuration

Syntax Description **`retransmission timeout`** *`retransmission_interval`* **`max-retry`** *`max_retry`*

max-retry *max_retry*

Specify the maximum number of times to request retry attempts. To disable retransmission, set to 0.

Must be an integer in the range of 0-5.

timeout *retransmission_interval*

Specify the retransmission interval in seconds. To disable retransmission, set to 0.

Must be an integer in the range of 0-10.

Usage Guidelines Use this command to configure retransmission parameters.

instance instance-id endpoint ep interface secondary-ip

Configures secondary IP address used in FTIED creation for new requests.

Command Modes Exec > Global Configuration

Syntax Description **`secondary-ip list-entry`** *`secondary_ip_addresses`*

list-entry *secondary_ip_addresses*

Specify the list of secondary IP addresses.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure secondary IP address used in FTIED creation for new requests.

instance instance-id endpoint ep interface sla

Configures the SLA parameters.

Command Modes Exec > Global Configuration

Syntax Description **`sla response`** *`response_time`* **`procedure`** *`procedure_time`*

procedure *procedure_time*

Specify, in milliseconds, the procedure time.

Must be an integer in the range of 1000-120000.

response *response_time*

Specify, in milliseconds, the response time.

Must be an integer in the range of 1000-180000.

Usage Guidelines Use this command to configure the SLA parameters.

instance instance-id endpoint ep interface supported-features

Enables supported features.

Command Modes Exec > Global Configuration

Syntax Description **`supported-features load-control overload-control`**

load-control

Specify to enable load control.

overload-control

Specify to enable overload control.

Usage Guidelines Use this command to enable supported features.

instance instance-id endpoint ep interface sx-path-failure

Configures the SX Path Failure Detection Policy profile.

Command Modes Exec > Global Configuration

Syntax Description **`sx-path-failure sx-detection-policy`** *`policy_profile_name`*

sx-detection-policy *policy_profile_name*

Specify name of the SX Path Failure Detection Policy profile.

Must be a string.

Usage Guidelines Use this command to configure the SX Path Failure Detection Policy profile.

instance instance-id endpoint ep interface vip

Configures the virtual IP address (VIP) parameters.

Command Modes Exec > Global Configuration

Syntax Description **`vip { vip-ip`** *`host_address`* **`| vip-port`** *`port_number`* **`} offline`**

offline

Specify when the virtual IP address (VIP) is offline.

vip-interface *interface_name*

Specify the interface name to advertise BGP router.

Must be a string.

vip-ip *host_address*

Specify the host address.

Must be a string.

vip-port *port_number*

Specify the port number.

Must be an integer.

Usage Guidelines Use this command to configure the VIP address parameters.

instance instance-id endpoint ep interface vip6

Configures VIP IP6 parameters.

Command Modes Exec > Global Configuration

Syntax Description **vip6 vip-ip6** *vip_ip6* **vip-ipv6-port** *port_number* **offline**

offline

Specify the VIP IP as offline.

vip-ip6 ***vip_ip6***

Specify the host detail.

Must be a string.

vip-ipv6-port ***port_number***

Specify the port number.

Must be an integer.

Usage Guidelines Use this command to configure VIP IP6 parameters.

instance instance-id endpoint ep internal base-port

Configures the internal base-port to start endpoint parameter.

Command Modes Exec > Global Configuration (config) > Instance ID Configuration (config-instance-id-*instance_id*) > Endpoint *endpoint_type* Configuration (config-endpoint-*endpoint_type*)

Syntax Description **internal base-port start** *base_port_to_start_ep*

start ***base_port_to_start_ep***

Specify the base port to start endpoint.

Must be an integer in the range of 1024-65535.

Usage Guidelines Use this command to configure the internal base-port to start endpoint parameter.

instance instance-id endpoint ep labels pod-config

Configures K8 node affinity label configuration.

Command Modes Exec > Global Configuration

Syntax Description **pod-config key** *label_key* **value** *label_value*

key *label_key*

Specify the key for the label.

Must be a string.

value *label_value*

Specify the value of the label.

Must be a string.

Usage Guidelines Use this command to configure the K8 node affinity label configuration.

instance instance-id endpoint ep memory

Configures K8 pod memory configuration.

Command Modes Exec > Global Configuration

Syntax Description **memory request** *memory_request* **limit** *memory_limit*

limit *memory_limit*

Specify the maximum memory resource in use, in megabytes.

Must be an integer in the range of 100-200000.

request *memory_request*

Specify the memory resource request, in megabytes.

Must be an integer in the range of 100-200000.

Usage Guidelines Use this command to configure the K8 pod memory configuration.

instance instance-id endpoint ep path-failure

Configures GTP path failure detection policy profile.

Command Modes Exec > Global Configuration

Syntax Description **path-failure detection-policy** *detection_policy*

detection-policy *detection_policy*

Specify the detection policy profile.

Must be a string.

Usage Guidelines Use this command to configure the GTP path failure detection policy profile.

instance instance-id endpoint ep retransmission

Configures retransmission parameters.

Command Modes Exec > Global Configuration

Syntax Description **`retransmission max-retry`** *`max_retry`* **`timeout`** *`retransmission_interval`*

max-retry *max_retry*

Specify the maximum number of times to request retry attempts. To disable retransmission, set to 0.

Must be an integer in the range of 0-5.

Default Value: 3.

timeout *retransmission_interval*

Specify the retransmission interval in seconds. To disable retransmission, set to 0.

Must be an integer in the range of 0-10.

Default Value: 2.

Usage Guidelines Use this command to configure retransmission parameters.

instance instance-id endpoint ep secondary-ip

Configures secondary IP address used in FTIED creation for new requests.

Command Modes Exec > Global Configuration

Syntax Description **`secondary-ip list-entry`** *`secondary_ip_addresses`*

list-entry *secondary_ip_addresses*

Specify the list of secondary IP addresses.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure secondary IP address used in FTIED creation for new requests.

instance instance-id endpoint ep sla

Configures the response and procedure duration parameters.

Command Modes Exec > Global Configuration

Syntax Description **sla response** *response_duration* **procedure** *procedure_duration*

procedure *procedure_duration*

Specify the procedure duration in milliseconds.

Must be an integer in the range of 1000-120000.

response *response_duration*

Specify the response duration in milliseconds.

Must be an integer in the range of 1000-120000.

Usage Guidelines Use this command to configure the response and procedure duration parameters.

instance instance-id endpoint ep sx-path-failure

Configures Sx Path Failure Detection Policy Profile parameter.

Command Modes Exec > Global Configuration

Syntax Description **sx-path-failure sx-detection-policy** *sx_detection_policy_name*

sx-detection-policy *sx_detection_policy_name*

Specify name of the Sx Path Failure Detection policy.

Must be a string.

Usage Guidelines Use this command to configure the Sx Path Failure Detection Policy Profile parameter.

instance instance-id endpoint ep system-health-level crash

Configures system health crash parameters.

Command Modes Exec > Global Configuration

Syntax Description **crash cpu-percent** *cpu_percentage* **memory-in-mbs** *memory* **num-of-goroutine** *goroutine_per_core*

cpu-percent *cpu_percentage*

Specify the CPU percentage.

Must be an integer.

Default Value: 80.

memory-in-mbs *memory*

Specify the memory in MBs.

Must be an integer.

Default Value: 2048.

num-of-goroutine *goroutine_per_core*

Specify the number of goroutine per core.

Must be an integer.

Default Value: 45000.

Usage Guidelines Use this command to configure system health crash parameters.

instance instance-id endpoint ep system-health-level critical

Configures system health critical parameters.

Command Modes Exec > Global Configuration

Syntax Description **`critical cpu-percent`** *`cpu_percentage`* **`memory-in-mbs`** *`memory`* **`num-of-goroutine`** *`goroutine_per_core`*

cpu-percent *cpu_percentage*

Specify the CPU percentage.

Must be an integer.

Default Value: 60.

memory-in-mbs *memory*

Specify the memory in MBs.

Must be an integer.

Default Value: 1024.

num-of-goroutine *goroutine_per_core*

Specify the number of goroutine per core.

Must be an integer.

Default Value: 35000.

Usage Guidelines Use this command to configure system health critical parameters.

instance instance-id endpoint ep system-health-level warn

Configures system health warning parameters.

Command Modes Exec > Global Configuration

Syntax Description **warn cpu-percent** *cpu_percentage* **memory-in-mbs** *memory* **num-of-goroutine** *goroutine_per_core*

cpu-percent *cpu_percentage*

Specify the CPU percentage.

Must be an integer.

Default Value: 50.

memory-in-mbs *memory*

Specify the memory in MBs.

Must be an integer.

Default Value: 512.

num-of-goroutine *goroutine_per_core*

Specify the number of goroutine per core.

Must be an integer.

Default Value: 25000.

Usage Guidelines Use this command to configure system health warning parameters.

instance instance-id endpoint ep vip

Configures virtual IP (VIP) parameters.

Command Modes Exec > Global Configuration (config) > Instance ID Configuration (config-instance-id-*instance_id*) > Endpoint *endpoint_type* Configuration (config-endpoint-*endpoint_type*)

Syntax Description **vip-ip** *vip_ipv4_detail* **[vip-port** *vip_port_number* **| vip-interface** *vip_interface_name* **| offline]**

offline

Specify the VIP-IP as offline.

vip-interface *vip_interface_name*

Specify the interface name to advertise BGP router.

Must be a string.

vip-ip *vip_ipv4_detail*

Specify the IPv4 detail.

Must be a string.

vip-port *vip_port_number*

Specify the VIP port number.

Must be an integer.

Usage Guidelines Use this command to configure VIP parameters.

instance instance-id endpoint ep vip6

Configures VIP IPv6 parameters.

Command Modes Exec > Global Configuration (config) > Instance ID Configuration (config-instance-id-*instance_id*) > Endpoint *endpoint_type* Configuration (config-endpoint-*endpoint_type*)

Syntax Description **vip-ipv6** *vip_ipv6_detail* **[vip-ipv6-port** *vip_ipv6_port_number* **| offline]**

offline

Specify the VIP-IP as offline.

vip-ipv6-port *vip_ipv6_port_number*

Specify the port number.

Must be an integer.

vip-ipv6 *vip_ipv6_detail*

Specify the IPv6 detail.

Must be a string.

Usage Guidelines Use this command to configure VIP IPv6 parameters.

instance instance-id endpoint fqdn

Configures the FQDN at endpoint level.

Command Modes Exec > Global Configuration (config) > Instance Configuration (config-instance-instance-id*instance_id*)

Syntax Description **endpoint** *endpoint_name* **{ fqdn** *fqdn_value* **}**

endpoint *endpoint_name* { fqdn *fqdn_value* }

- **endpoint** *endpoint_name* —Specify the endpoint name within the instance. For example: SBI interface.
- **fqdn** *fqdn_value* —Specify the FQDN value for the specified endpoint. FQDN value must be string.

Usage Guidelines Use this command to configure FQDN at endpoint level.

instance instance-id endpoint gtp interface interface-name

Configures encoder and decoder for the IEs that are associated with the GTPC endpoint pod.

Command Modes Exec > Global Configuration (config) > Instance ID Configuration (config-instance-id-*instance_id*)

Syntax Description **endpoint gtp interface** *interface_name* **enable-direct-encdec true | false**

interface *interface_name*

Specify the interface name, such as s5e and s11.

enable-direct-encdec { true | false } *dscp_value*

Specify whether to enable the encoder and decoder to optimize the encoding and decoding of the IEs that are associated with the GTPC endpoint pod. By default, it is disabled.

Must be one of the following:

- **false**
- **true**

Usage Guidelines Use this command to configure the encoder and decoder for the IEs that are associated with the GTPC endpoint pod.

instance instance-id endpoint pfcp interface n4 reactivate-peer condition

Reactivates the blocked UPF associated with the PFCP endpoint pod.

Command Modes Exec > Global Configuration (config) > Instance ID Configuration (config-instance-id-*instance_id*)

Syntax Description **endpoint pfcp interface** *interface_name* **reactivate-peer condition [blocked] attributes [frequency** *frequency_timer* **]**

reactivate-peer condition [blocked]

Specify the condition as blocked to reactivate the blocked UPF.

attributes

Specify the attributes to configure to reactivate the blocked UPF.

[frequency *frequency_timer*]

Configure the frequency timer to reactivate the blocked UPF once the timer is over.

The value of the command **frequency** ranges between 60 to 86400.

The frequency parameter does not have any default values.

Note It is mandatory to configure the frequency parameter within the defined range. If the frequency parameter is not configured within the range, the system by default takes zero as the input. As a result, the identified UPF does not get blocklisted even if the alarm is triggered.

Usage Guidelines Use this command to reactivate the blocked UPF once the timer is over.

instance instance-id endpoint radius

Configures the RADIUS endpoint parameters.

Command Modes Exec > Global Configuration (config) > Instance ID Configuration (config-instance-id-*instance_id***endpoint radius**)

Syntax Description `endpoint radius enable-async { false | true }`

endpoint radius

Specify the endpoint name as RADIUS.

enable-async { false | true }

Specify whether to enable asynchronous communication to send RADIUS Authentication and Accounting messages towards udp-proxy and CoA message towards smf-service. By default, it is disabled.

Must be one of the following:

- false
- true

Default value is false.

Note Any modifications to this configuration require a restart of the radius-ep pods.

instances instance

Configures SMF instance.

Command Modes Exec > Global Configuration (config)

Syntax Description **instances instance** *instance_id* **system-id** *system_id* **cluster-id** *cluster_id* **slice-name** *slice_name*

cluster-id *cluster_id*

Specify the instance cluster ID.

Must be a string.

instance-id *instance_id*

Specify the instance ID.

Must be an integer in the range of 1-8.

slice-name *slice_name*

Specify the CDL slice name associated with instance ID.

Must be a string.

system-id *system_id*

Specify the instance system ID.

Must be a string.

Usage Guidelines Use this command to configure SMF instance.

instance instance-id interface fqdn

Configures the FQDN at interface level.

Command Modes Exec > Global Configuration (config) > Instance Configuration (config-instance-instance-id*instance_id*)

Syntax Description **endpoint** *endpoint_name* **{ interface** *interface_name* **{ fqdn** *fqdn_value* **} }**

endpoint *endpoint_name*{ interface *interface_name*{ fqdn *fqdn_value*}}

- **endpoint** *endpoint_name* —Specify the endpoint name within the instance. For example: SBI interface.
- **interface** *interface_name* —Specify the interface for which the FQDN is being configured. For example: N7, N10, or N11 interface.
- **fqdn** *fqdn_value* —Specify the FQDN value for the specified endpoint. FQDN value must be string.

Usage Guidelines Use this command to configure FQDN at interface level.

instance instance-id smf-fqdn

instance instance-id interface fqdn

Configures the FQDN for SMF instance.

Command Modes Exec > Global Configuration (config) > SMF Profile Configuration (config-profile-smf-*profile_name*)

Syntax Description **instance** *instance_id* **smf-fqdn** *fqdn_value*

instance *instance_id* smf-fqdn *fqdn_value*

- **instance** *instance_id* —Specifiy the instance identifier for the SMF. Replace instance-id with the appropriate instance number, such as 1.
- **smf-fqdn** *fqdn_value* —Specify the FQDN for the SMF.

Usage Guidelines Use this command to configure SMF's FQDN under SMF profile for each instance.

ipam

Configures IP Address Management (IPAM) configuration parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **ipam**

Usage Guidelines Use this command to configure IPAM configuration parameters.

exec-ipam reclaim-chunk

Configures SMF to instantly reclaim under-utilized IP chunks.

Command Modes Exec

Syntax Description **exec-ipam reclaim-chunk { utilization-threshold** *utilization_threshold* **inactivity-threshold** *inactivity_threshold* **[instance** *grInstance* **] [pool-name** *poolName* **] [chunk-start-ip** *ip* **] }**

exec-ipam

Executes IPAM commands.

reclaim-chunk

Executes IP-chunk reclamation procedure.

utilization-threshold *utilization_threshold*

Configures the utilization threshold for reclamation.

inactivity-threshold *inactivity_threshold*

Configures inactivity threshold for reclamation in seconds.

instance *grInstance*

Configures the GR Instance for which the auto-reclamation process is to be executed.

pool-name *poolName*

Specifies the pool for which the auto-reclamation process is to be executed.

chunk-start-ip *ip*

Specifies the IP with which the chunk starts for which the auto-reclamation process is to be executed.

Usage Guidelines Use this command to instantly re-claim under-utilized IP chunks.

ipam dp

Displays IPAM data-plane allocations.

Command Modes Exec

Syntax Description **`show ipam dp`** *`dp_name`* **`[`** *`options`* **`]`**

Usage Guidelines Use this command to view IPAM data-plane allocations.

ipam instance

Configures the instance configuration parameters.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam)

Syntax Description **`instance`** *`instance_id`*

instance *instance_id*

Specify the instance ID.

Must be an integer in the range of 1-8.

Usage Guidelines Use this command to configure the instance configuration parameters.

ipam instance address-pool

Configures IPAM address pools.

Command Modes

Exec > Global Configuration > IPAM Configuration

Syntax Description

address-pool *address_pool_name* **[static | offline | dhcp | vrf-name** *vrf_name* **]**

address-pool *address_pool_name*

Specify name of the address pool.

Must be a string of 1-128 characters in the ipam-str pattern. For information on the ipam-str pattern, see the *Input Pattern Types* chapter.

address-quarantine-qsize *max_ips_in_quarantine_queue*

Specify the maximum number of IPs to be held in quarantine queue per-dp, per-af, per-instance.

Must be an integer.

address-quarantine-timer *address_quarantine_timer_interval*

Specify the address quarantine timer interval in seconds.

Must be an integer in the range of 4-3600.

Default Value: 4.

offline

Specify the pool as an offline pool.

static

Specify the pool as a static pool.

dhcp

Specify the pool as the DHCP pool.

vrf-name *vrf_name*

Specify name of the VRF.

Must be a string of 1-128 characters in the ipam-str pattern. For information on the ipam-str pattern, see the *Input Pattern Types* chapter.

Usage Guidelines

Use this command to configure IPAM address pools.

ipam instance address-pool ipv4

Configures IPv4 parameters.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*)

Syntax Description **`ipv4`**

Usage Guidelines Use this command to configure IPv4 parameters.

ipam instance address-pool ipv4 address-range

Configures IPv4 address ranges.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*) > IPv4 Configuration (config-ipv4)

Syntax Description **`address-range`** *`start_ipv4_address end_ipv4_address`* **`[ offline ]`**

address-range *start_ipv4_address*

Specify the start address of the IPv4 address range.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

nexthop-forwarding-address *nexthop_forwarding_address*

Specify the nexthop forwarding address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

offline

Specify the IPv4 address range as offline.

end_ipv4_address

Specify the end address of the IPv4 address range.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure IPv4 address ranges.

ipam instance address-pool ipv4 chunk-group

Configures IPv4 chunk group size for a pool.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*) > IPv4 Configuration (config-ipv4)

Syntax Description **chunk-group { chunks-per-group** *{ 2 | 4| 8 }* **reserve-contiguous-groups }**

chunk-group

Allows to configure chunk-groups for a pool.

chunks-per-group *{ 2 | 4| 8 }*

Defines the number of chunks in a chunk group. The values can be either 2, 4, or 8.

reserve-contiguous-groups

Allows reserving contiguous chunk-groups as per **max-upf-session** defined in the UPF or DNN profile.

Usage Guidelines Use this command to configure IPv4 chunk group.

ipam instance address-pool ipv4 prefix-range

Configures prefix range parameters.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*) > IPv4 Configuration (config-ipv4)

Syntax Description **prefix-range** *prefix_value* **length** *prefix_length* **[offline]**

length *prefix_length*

Specify the prefix length.

Must be an integer in the range of 1-31.

nexthop-forwarding-address *nexthop_forwarding_address*

Specify the nexthop forwarding address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

offline

Specify to set the IPv4 prefix to offline mode.

prefix *prefix_value*

Specify the prefix value.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure prefix range parameters.

ipam instance address-pool ipv4 split-size

Configures chunk split size.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*) > IPv4 Configuration (config-ipv4)

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*) > IPv6 Configuration (config-ipv6) > Address Range Configuration (config-address-ranges)

Syntax Description **`split-size [ [ no-split ] [ per-cache`** *`number_of_addresses`* **`] [ per-dp`** *`number_of_addresses`* **`] ]`**

no-split

Specify not to split the address range into smaller chunks.

per-cache *number_of_addresses*

Specify the number of addresses per chunk for IPAM cache allocation. Specify in power of 2.

Must be an integer in the range of 2-262144.

per-dp *number_of_addresses*

Specify the number of addresses per chunk for data-plane allocation. Specify in power of 2.

Must be an integer in the range of 2-262144.

Usage Guidelines Use this command to configure chunk split sizes.

ipam instance address-pool ipv4 threshold

Configures pool thresholds.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*) > IPv4 Configuration (config-ipv4) > Address Range Configuration (config-address-ranges)

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*) > IPv6 Configuration (config-ipv6) > Address Range Configuration (config-address-ranges)

Syntax Description **`threshold upper-threshold`** *`upper_threshold`*

upper-threshold *upper_threshold*

Specify the upper threshold in percentage.

Must be an integer in the range of 1-100.

Usage Guidelines Use this command to configure pool thresholds.

ipam instance address-pool ipv4 vlan

Configures the VLAN ID to receive the IPv4 addresses.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*) > IPv4 Configuration (config-ipv4)

Syntax Description **`vlan`** *`vlan_id`*

vlan *vlan_id*

Configure the VLAN ID to receive the IPv4 address.

Usage Guidelines Use this CLI to configure VLAN ID.

ipam instance address-pool ipv6

Configures IPv6 parameters.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*)

Syntax Description **`address-range`**

Usage Guidelines Use this command to configure IPv6 parameters.

ipam instance address-pool ipv6 address-ranges address-range

Configures IPv6 address ranges.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*) > IPv6 Configuration (config-ipv6)

Syntax Description **address-ranges address-range** *start_ipv6_address end_ipv6_address* **[offline]**

offline

Specify the IPv6 address range as offline.

end_ipv6_address

Specify the end address of the IPv6 address range.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

start_ipv6_address

Specify the start address of the IPv6 address range.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure IPv6 address ranges.

ipam instance address-pool ipv6 address-ranges prefix-range

Configures prefix range parameters.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*) > IPv6 Configuration (config-ipv6)

Syntax Description **prefix-ranges prefix-range [prefix** *prefix_value* **] [length** *prefix_length* **] [offline]**

length *prefix_length*

Specify the prefix length.

Must be an integer in the range of 96-127.

offline

Specify to set the IPv6 prefix to offline mode.

prefix *prefix_value*

Specify the prefix value.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure prefix range parameters.

ipam instance address-pool ipv6 prefix-ranges prefix-length

Configures IPv6 prefix length that should be used for IP allocation.

Command Modes Exec > Global Configuration > IPAM Configuration > Address Pool Configuration > Prefix Ranges Configuration

Syntax Description **`prefix-length`** *`prefix_length`*

prefix-length *prefix_length*

Specify the prefix length for IP allocation. The system will always allocate IPs from the pool with the specified prefix.

Must be an integer in the range of 2-64.

Usage Guidelines Use this command to configure IPv6 prefix length.

ipam instance address-pool ipv6 address-ranges chunk-group

Configures chunk group for IPv6 address ranges.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*) > IPv6 Configuration (config-ipv6)

Syntax Description **`chunk-group { chunks-per-group`** *`{ 2 | 4| 8 }`* **`reserve-contiguous-groups }`**

chunk-group

This CLI allows to configure chunk-groups for a pool.

chunks-per-group *{ 2 | 4| 8 }*

Defines the number of chunks in a chunk group. The values can be either 2, 4, or 8.

reserve-contiguous-groups

Allows reserving contiguous chunk-groups as per **max-upf-session** defined in the UPF or DNN profile.

Usage Guidelines Use this command to configure IPv6 chunk group size for address range.

ipam instance address-pool ipv6 address-ranges split-size

Configures chunk split size.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*) > IPv4 Configuration (config-ipv4)

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*) > IPv6 Configuration (config-ipv6) > Address Range Configuration (config-address-ranges)

Syntax Description **`split-size [ [ no-split ] [ per-cache`** *`number_of_addresses`* **`] [ per-dp`** *`number_of_addresses`* **`] ]`**

no-split

Specify not to split the address range into smaller chunks.

per-cache *number_of_addresses*

Specify the number of addresses per chunk for IPAM cache allocation. Specify in power of 2.

Must be an integer in the range of 2-262144.

per-dp *number_of_addresses*

Specify the number of addresses per chunk for data-plane allocation. Specify in power of 2.

Must be an integer in the range of 2-262144.

Usage Guidelines Use this command to configure chunk split sizes.

ipam instance address-pool ipv6 address-ranges threshold

Configures pool thresholds.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*) > IPv4 Configuration (config-ipv4) > Address Range Configuration (config-address-ranges)

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*) > IPv6 Configuration (config-ipv6) > Address Range Configuration (config-address-ranges)

Syntax Description **`threshold upper-threshold`** *`upper_threshold`*

upper-threshold *upper_threshold*

Specify the upper threshold in percentage.

Must be an integer in the range of 1-100.

Usage Guidelines Use this command to configure pool thresholds.

ipam instance address-pool ipv6 vlan

Configures the VLAN ID to receive the IPv6 addresses.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*) > IPv6 Configuration (config-ipv6)

Syntax Description **vlan** *vlan_id*

vlan *vlan_id*

Configure the VLAN ID to receive the IPv6 address.

Usage Guidelines Use this CLI to configure VLAN ID.

ipam instance address-pool ipv6 prefix-ranges prefix-range

Configures IPv6 prefix ranges.

Command Modes Exec > Global Configuration > IPAM Configuration > Address Pool Configuration > Prefix Ranges Configuration

Syntax Description **prefix-range** *prefix_value* **length** *prefix_length* **[offline]**

length *prefix_length*

Specify the prefix length.

Must be an integer in the range of 1-63.

offline

Specify the IPv6 prefix range as offline.

prefix-range *prefix_value*

Specify the IPv6 prefix range.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure IPv6 prefix ranges.

ipam instance address-pool ipv6 prefix-ranges chunk-group

Configures chunk group for IPv6 prefix ranges.

Command Modes Exec > Global Configuration > IPAM Configuration > Address Pool Configuration > Prefix Ranges Configuration

Syntax Description **chunk-group { chunks-per-group** *{ 2 | 4| 8 }* **reserve-contiguous-groups }**

chunk-group

This CLI allows to configure chunk-groups for a pool.

chunks-per-group *{ 2 | 4| 8 }*

Defines the number of chunks in a chunk group. The values can be either 2, 4, or 8.

reserve-contiguous-groups

Allows reserving contiguous chunk-groups as per **max-upf-session** defined in the UPF or DNN profile.

Usage Guidelines Use this command to configure IPv6 chunk group size for prefix range.

ipam instance address-pool ipv6 prefix-ranges split-size

Configures chunk split size.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*) > IPv4 Configuration (config-ipv4)

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*) > IPv6 Configuration (config-ipv6) > Address Range Configuration (config-address-ranges)

Syntax Description **split-size [[no-split] [per-cache** *number_of_addresses* **] [per-dp** *number_of_addresses* **]]**

no-split

Specify not to split the address range into smaller chunks.

per-cache *number_of_addresses*

Specify the number of addresses per chunk for IPAM cache allocation. Specify in power of 2.

Must be an integer in the range of 2-262144.

per-dp *number_of_addresses*

Specify the number of addresses per chunk for data-plane allocation. Specify in power of 2.

Must be an integer in the range of 2-262144.

Usage Guidelines Use this command to configure chunk split sizes.

ipam instance address-pool ipv6 prefix-ranges threshold

Configures pool thresholds.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*) > IPv4 Configuration (config-ipv4) > Address Range Configuration (config-address-ranges)

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*) > IPv6 Configuration (config-ipv6) > Address Range Configuration (config-address-ranges)

Syntax Description **`threshold upper-threshold`** *`upper_threshold`*

upper-threshold *upper_threshold*

Specify the upper threshold in percentage.

Must be an integer in the range of 1-100.

Usage Guidelines Use this command to configure pool thresholds.

ipam instance address-pool tags

Configures address pool tags.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*) > Address Pool Configuration (config-address-pool-*address_pool_name*)

Syntax Description **`tags [ [ dnn`** *`dnn`* **`] [ nssai`** *`nssai`* **`] [ serving-area`** *`serving_area`* **`] ]`**

dnn *dnn*

Specify the DNN.

Must be a string.

nssai *nssai*

Specify the NSSAI.

Must be a string.

serving-area *serving_area*

Specify the serving area.

Must be a string.

Usage Guidelines Use this command to configure address pool tags.

ipam instance audit chunk

Configures IPAM to enable or disable the reconciliation of IP chunks between SMF and UPF.

Command Modes Exec > Global Configuration > IPAM Configuration

Syntax Description **`audit chunk`** *`[ local | none ]`*

audit chunk *[local | none]*

Configures audit activity on IPAM. It has two possible values:

- *local* —Enables the feature.
- *none* —Disables the feature.

Default value is *none*.

Usage Guidelines Use this command to enable or disable the reconciliation of IP chunks between SMF and UPF.

ipam instance chunk throttling

Configure the IP chunk allocation throttling feature.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*)

Syntax Description **`chunk-throttling { false | true }`**

chunk-throttling { false | true }

Specify to enable or disable the IP chunk throttling. To disable the throttling, set to false.

Default value: true

The IP chunk allocation throttle feature triggers throttling checks based on the maximum UPF sessions supported. However, throttling checks occur even if the maximum UPF sessions are not configured, causing unnecessary processing overhead. To address this issue, you shoud disable the IP throttling explicitly.

Usage Guidelines Use this command to enable or disable IP chunk throttling.

ipam instance chunk-reclamation

Configures SMF to auto re-claim under-utilized IP chunks.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*)

Syntax Description **chunk-reclamation { schedule tod-hour** *tod_hour_value* **schedule tod-minute** *tod_min_value* **utilization-threshold** *utilization_threshold* **inactivity-threshold** *inactivity_threshold* **}**

chunk-reclamation

Configures periodic IP chunk reclamation process.

schedule

Configure the Time-of-day values for the chunk-reclamation process.

tod-hour *tod_hour_value*

Configure the Time-of-day hour value for the chunk-reclamation process. The value range for **schedule tod-hour** is <0-23>.

tod-minute *tod_min_value*

This CLI configures the Time-of-day minute value for the chunk-reclamation process. The value range for **tod-minute** is <0-59>.

utilization-threshold *utilization_threshold*

This CLI configures the utilization threshold for reclamation. The value range for **utilization-threshold** is <0-20>. The default value is 2.

inactivity-threshold *inactivity_threshold*

This CLI configures the inactivity threshold for reclamation. The value range for **inactivity-threshold** is <0-3600>. The default value is 1800.

Usage Guidelines Use this command to auto re-claim under-utilized IP chunks.

ipam instance data-sharding

Enable IPAM cache data sharding.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*)

Syntax Description **data-sharding num-shards** *shards_number*

num-shards *shards_number*

Specify the number of shards for IPAM cache data. The value of *shards_number* must be an integer between 2 and 16.

To disable data sharding, use the **no data-sharding** command. By default, the data sharding is disabled.

Important You must restart SMF for the configuration to take effect.

Usage Guidelines Use this command to enable IPAM cache data sharding and configure the number of shards based on the number of IP pools, UPFs, and address types deployed. This configuration improves the IPAM performance and scalability.

ipam instance min-dp-addr-size

Configures the minimum number of addresses to reserve per upf, per nm, per pool/tag.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*)

Syntax Description **`min-dp-addr-size [ [ ipv4-addr`** *`min_to_reserve`* **`] [ ipv6-addr`** *`min_to_reserve`* **`] [ ipv6-prefix`** *`min_to_reserve`* **`] ]`**

ipv4-addr *min_to_reserve*

Specify the minimum number of IPv4 address to reserve.

Must be an integer in the range of 16-262144.

ipv6-addr *min_to_reserve*

Specify the minimum number of IPv6 address to reserve.

Must be an integer in the range of 32-262144.

ipv6-prefix *min_to_reserve*

Specify the minimum number of IPv6 prefix to reserve.

Must be an integer in the range of 32-262144.

Usage Guidelines Use this command to configure the minimum number of addresses to reserve per upf, per nm, per pool/tag.

ipam instance source

Configures pool-datastore source selection.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*)

Syntax Description **`source local`**

local

Specify to use local address pool datastore.

Usage Guidelines Use this command to configure pool-datastore source selection.

ipam instance source external ipam

Configures external IPAM server for pool information.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*)

Syntax Description **source external ipam [[host** *ip_address* **] [port** *port_number* **] [vendor** *vendor_id* **]]**

host *ip_address*

Specify IP address of the IPAM server.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify port number of the IPAM server.

Must be an integer in the range of 1-65535.

vendor *vendor_id*

Specify the IPAM server's vendor ID. Default: cisco.

Must be one of the following:

- **cisco**

Usage Guidelines Use this command to configure external IPAM server for pool information.

ipam instance threshold

Configures global upper thresholds.

Command Modes Exec > Global Configuration (config) > IPAM Configuration (config-ipam) > Instance Configuration (config-instance-*instance_id*)

Syntax Description **threshold [[ipv4-addr** *ipv4_address_threshold* **] | [ipv6-addr** *ipv6_address_threshold* **] | [ipv6-prefix** *ipv6_prefix_threshold* **]]**

ipv4-addr ***ipv4_address_threshold***

Specify the IPv4 address threshold in percentage.

Must be an integer in the range of 1-100.

ipv6-addr ***ipv6_address_threshold***

Specify the IPv6 address threshold in percentage.

Must be an integer in the range of 1-100.

ipv6-prefix ***ipv6_prefix_threshold***

Specify the IPv6 prefix threshold in percentage.

Must be an integer in the range of 1-100.

Usage Guidelines Use this command to configure global upper thresholds.

ipam pool

Displays IPAM pool allocation information.

Command Modes Exec

Syntax Description **show ipam pool** *pool_name*

Usage Guidelines Use this command to view IPAM pool allocation information.

ipam pool ipv4-addr

Displays IPAM pool IPv4 address information.

Command Modes Exec

Syntax Description **show ipam pool** *pool_name* **ipv4-addr**

Usage Guidelines Use this command to view IPAM pool IPv4 address information.

ipam pool ipv6-addr

Displays IPAM pool IPv6 address information.

Command Modes Exec

Syntax Description **show ipam pool** *pool_name* **ipv6-addr**

Usage Guidelines Use this command to view IPAM pool IPv6 address information.

job

Suspends the jobs that are running in the background.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **`job stop`** *`job_id`*

job_id

Specify the job ID for suspending the corresponding job.

Must be an integer.

Usage Guidelines Use this command to suspend the jobs that are running in the background.

k8 ccg

Configures coverage build parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **`k8 ccg coverage-build { false | true }`**

coverage-build { false | true }

Specify whether to enable or disable coverage build.

Must be one of the following:

- **false**
- **true**

Default Value: false.

Usage Guidelines Use this command to configure the coverage build parameters.

k8 ccg coverage

Configures Code Coverage Utils parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **`k8 ccg coverage container-stop`** *`container_stop`*

container-stop *container_stop*

Specify container stop.

Must be a string.

Default Value: false.

Usage Guidelines Use this command to configure the Code Coverage Utils parameters.

k8 label pod-group-config

Configures the K8 node affinity label parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **k8 label** *vm_group* **key** *label_key* **value** *label_value*

key *label_key*

Specify the label key.

Must be a string.

value *label_value*

Specify the label value.

Must be a string.

vm_group

Specify the VM group.

Must be one of the following:

- **cdl-layer**
- **oam-layer**
- **protocol-layer**
- **service-layer**

Usage Guidelines Use this command to configure the K8 node affinity label parameters.

leaf-prompting

Enables or disables automatic querying for leaf values.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `leaf-prompting { false | true }`

{ false | true }

Specify false to disable leaf prompting, and true to enable.

Must be either "false" or "true".

Usage Guidelines Use this command to automatically query for leaf values.

license smart deregister

Configures the license parameters for the VNF deregistration.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `license smart deregister`

deregister

Specify to deregister the VNF for smart licensing.

Usage Guidelines Use this command to configure the license parameters for the VNF deregistration.

license smart register

Configures the license parameters for the VNF registration.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `license smart register force idtoken` *`token_id`*

register

Specify to register the VNF for Smart Licensing.

force

Specify to enable the force registration of the agent.

idtoken *token_id*

Specify the ID token to register the agent with.

Must be an integer.

Usage Guidelines Use this command to configure the license parameters for the VNF registration.

license smart renew

Configures the license parameters for the VNF renewal.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **`license smart renew { ID | auth }`**

renew

Renew the smart agent IDs and authentication.

ID

Specify to renew the smart agent license registration information.

auth

Initiate the manual update of the license usage information with Cisco.

Usage Guidelines Use this command to configure the license parameters for the VNF renewal.

local-instance

Configures local instance parameters.

Command Modes Exec > Global Configuration

Syntax Description **`local-instance instance`** *`instance_id`*

instance *instance_id*

Specify the local instance ID.

Usage Guidelines Use this command to configure local instance parameters.

load factor

Configures the load factor frequency calculation parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **`load factor { calc-frequency`** *`calc_frequency_time`* **`| exclude-pods`** *`exclude_pod_name`* **`}`**

load factor

Configures the load factor calculation parameters.

{ calc-frequency *calc_frequency_time*

Configures the load factor frequency time.

Must be an integer.

| exclude-pods *exclude_pod_name*

Configures the specific service pods to be excluded. It must be one of the following:

- bfdmgr
- bgpspeaker-pod
- cache-pod
- edr-monitor
- georeplication-pod

Usage Guidelines Use this command to configure the load factor for the system.

logging async application enable

Enables async logging.

Command Modes Exec > Global Configuration

Syntax Description **enable buffer-size** *buffer_size*

buffer-size *buffer_size*

Specify the buffer size for async logging.

Must be an integer.

Usage Guidelines Use this command to enable async logging.

logging async monitor-subscriber enable

Enables async logging.

Command Modes Exec > Global Configuration

Syntax Description **enable buffer-size** *buffer_size*

buffer-size *buffer_size*

Specify the buffer size for async logging.

Must be an integer.

Usage Guidelines Use this command to enable async logging.

logging async tracing enable

Enables async logging.

Command Modes Exec > Global Configuration

Syntax Description **enable buffer-size** *buffer_size*

buffer-size *buffer_size*

Specify the buffer size for async logging.

Must be an integer.

Usage Guidelines Use this command to enable async logging.

logging async transaction enable

Enables async logging.

Command Modes Exec > Global Configuration

Syntax Description **enable buffer-size** *buffer_size*

buffer-size *buffer_size*

Specify the buffer size for async logging.

Must be an integer.

Usage Guidelines Use this command to enable async logging.

logging error

Configures error logging parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **logging error stack** *status*

stack *status*

Specify to enable or disable error stack.

Must be one of the following:

- **disable**
- **enable**

Default Value: enable.

Usage Guidelines Use this command to configure error logging parameters.

logging json-logging

Configures JSON logging in pod logs.

Command Modes Exec > Global Configuration (config)

Syntax Description **`[no] logging json-logging [ application | monitor-subscriber | transaction ]`**

logging json-logging [

no

Disables the JSON logging in the pod logs.

logging json-logging [application | monitor-subscriber | transaction]

Enables the SMF-based application pods to start logging in the JSON format for the **application**, **monitor-subscriber**, and **transaction** log types.

Usage Guidelines Use this command to enable or disable the JSON logging in pod logs.

logging level

Configures the logging level.

Command Modes Exec > Global Configuration (config)

Syntax Description **`logging level { application`** *`application_log_level`* **`| monitor-subscriber`** *`monitor_subscriber_log_level`* **`| tracing`** *`tracing_log_level`* **`| transaction`** *`transaction_log_level`* **`}`**

application *application_log_level*

Specify the log level for application log type.

Must be one of the following:

- **debug**
- **error**
- **info**
- **off**
- **trace**
- **warn**

monitor-subscriber *monitor_subscriber_log_level*

Specify the log level for subscriber monitoring.

Must be one of the following:

- **debug**
- **error**
- **info**
- **off**
- **trace**
- **warn**

tracing *tracing_log_level*

Specify the log level for tracing log type.

Must be one of the following:

- **debug**
- **error**
- **info**
- **off**
- **trace**
- **warn**

transaction *transaction_log_level*

Specify the log level for transaction log type.

Must be one of the following:

- **debug**
- **error**
- **info**

- **off**
- **trace**
- **warn**

Usage Guidelines Configures logging parameters. Use this command to configure the logging level.

logging logger

Configures logger parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **logging name** *logger_name*

logger_name

Specify the logger name in the format "module.component.interface".

Must be a string.

Usage Guidelines Use this command to configure logger parameters.

logging logger level

Configures the logging level.

Command Modes Exec > Global Configuration

Syntax Description **logging name** *logger_name* **level { application** *application_log_level* **| tracing** *tracing_log_level* **| transaction** *transaction_log_level* **}**

application *application_log_level*

Specify the log level for application log type.

Must be one of the following:

- **debug**
- **error**
- **info**
- **off**
- **trace**
- **warn**

monitor-subscriber *monitor_subscriber_log_level*

Specify the log level for subscriber monitoring.

Must be one of the following:

- **debug**
- **error**
- **info**
- **off**
- **trace**
- **warn**

tracing *tracing_log_level*

Specify the log level for tracing log type.

Must be one of the following:

- **debug**
- **error**
- **info**
- **off**
- **trace**
- **warn**

transaction *transaction_log_level*

Specify the log level for transaction log type.

Must be one of the following:

- **debug**
- **error**
- **info**
- **off**
- **trace**
- **warn**

Usage Guidelines

Use this command to configure the logging level type.

logging transaction

Configures the transaction logging parameters.

Command Modes

Exec > Global Configuration (config)

Syntax Description

logging transaction { duplicate { enable | disable } | max-file-size *max_file_size* **| max-rotation** *max_rotations* **| message { enable | disable } | persist { enable | disable } }**

duplicate { enable | disable }

Specify whether to enable or disable duplicate logs in transaction logging.

Must be one of the following:

- **disable**
- **enable**

Default Value: disable.

max-file-size *max_file_size*

Specify the maximum transaction file size in MB.

Must be an integer in the range of 1-10000.

Default Value: 50.

max-rotation *max_max_rotations*

Specify the maximum number of file rotations.

Must be an integer in the range of 2-1000.

Default Value: 10.

message { enable | disable }

Specify whether to enable or disable messages in transaction logging.

Must be one of the following:

- **disable**
- **enable**

Default Value: disable.

persist { enable | disable }

Specify whether to enable or disable file-based transaction logging.

Must be one of the following:

- **disable**

- **enable**

Default Value: disable.

Usage Guidelines Use this command to configure the transaction logging parameters.

logout

Logout a specific session or a specific user from all sessions.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **logout [session** *session_id* **| user** *user_name* **]**

session *session_id*

Specify the session ID from the possible completion options.

Must be a string.

user *user_name*

Specify the user name or the user process from the possible completion options.

Must be a string.

Usage Guidelines Use this command to log out a specific session or a specific user from all sessions.

message type

Configures the UDM message types.

Command Modes Exec > UDM Service Configuration (config)

Syntax Description **message type { UdmRegistrationReq | UdmSdmGetUESMSubscriptionData | UdmSdmSubscribeToNotification | UdmSdmUnsubscribeToNotification | UdmSubscriptionReq | UdmUecmRegisterSMF skip optional-ies [epdgInd | registrationTime] | UdmUecmUnregisterSMF }**

message type { UdmRegistrationReq | UdmSdmGetUESMSubscriptionData | UdmSdmSubscribeToNotification | UdmSdmUnsubscribeToNotification | UdmSubscriptionReq | UdmUecmRegisterSMF skip optional-ies [epdgInd | registrationTime] | UdmUecmUnregisterSMF }

Configures any one of the following udm subscription message types:

- **UdmRegistrationReq**
- **UdmSdmGetUESMSubscriptionData**

- **UdmSdmSubscribeToNotification**
- **UdmSdmUnsubscribeToNotificationUdmSubscriptionReq**
- **UdmUecmRegisterSMF**

skip optional-ies [epdgInd | registrationTime]—Skips ePDG indication or Resgistration Time in the N10 Registration Request.



Note The **skip optional-ies [epdgInd | registrationTime]** command is available only with UdmUecmRegisterSMF message.

Usage Guidelines Use this command to configure the UDM message types.

mode debug exec action release-resource

Triggers the resource releasing process for N4 interface per UPF from SMF.

Command Modes Exec

Syntax Description **`mode debug exec  action release-resource attributes { interface n4 peer { ip`** *`upf_ip`* **`} } condition { dnn matches`** *`dnn-name`* **`}`**

debug

This keyword indicates that this is a debug mode operational CLI.

exec

This command executes the command to trigger N4 release per UPF from SMF.

action

Triggers an action to be performed.

release-resource

This is an optional command. Upon executing **release-resource**, the SMF triggers clean-up of subscriber/pool resources to the peer provided.

attributes

Defines the attributes to perform an action.

peer

The UPF peer can be defined using UPF IP address.

interface

Specifies the interface name to trigger the operation for.

condition

Specifies the additional condition to filter the data for selected operation. This is an optional filter.

dnn

Pools associated to this dnn-name will be cleared based on the given operator.

matches

This command verifies the DNN that matches the output modifiers.

Usage Guidelines Use this command to trigger N4 resources or associations release process per UPF from the SMF.

monitor protocol

Configures the SMF to monitor the protocol.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **monitor protocol { interface** *interface_name* **[capture-duration** *duration* **| gr-instance** *gr_instance* **| pcacp yes | |] | list [|] }**



Warning Use the **monitor protocol interface** command cautiously, as it may disrupt user services. When used in a live network, it can cause session delays, call drops, and degrade system performance.

interface *interface_name*

Specifies the name of interface on which PCAP is captured.

interface_name must be a string of possible values sbi, pfcp, gtpu, gtpc, gtp, radius, and diameter.



Note For the Diameter interface, SMF uses the Monitor Protocol for packets.

capture-duration *duration*

duration Specifies the duration, in seconds, during which PCAP is captured.

Must be an integer.

The default value is 300 seconds.

gr-instance *gr_instance*

Specifies the monitor protocol for given gr-instance only.

grinstance_monitorprotocol must be a string.

pcap yes

Enables PCAP file generation.

The default value is no.

list

Lists monitor protocol files.

[|]

Specifies output options:

- append
- begin
- count
- exclude
- include
- linnum
- more
- nomore
- save
- until

monitor active-instance-traffic

Configures the SMF to monitor the traffic on an active GR instance.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration (config)

Syntax Description

`active-instance-traffic { no-traffic-duration` *`no_traffic_duration`*
`session-threshold` *`session_threshold`* **`action {`** *`pod-restart | trigger-switch-over`* **`} }`**

active-instance-traffic

It is the CLI to configure active traffic monitoring on the pod.

no-traffic-duration *no_traffic_duration*

Specifies the maximum allowed time (in seconds) of no traffic on an active instance. The value range is 10-300.

session-threshold *session_threshold*

Minimum session count to start the active instance traffic monitoring. The value range is 10-10000000. The default value is 1000.

action *{ pod-restart | trigger-switch-over }*

Action to take on condition fulfillment. The possible values for this command are *pod-restart* or *trigger-switch-over*. The default value is *pod-restart*.

Usage Guidelines Use this command to monitor the traffic on an active GR instance.

monitor-protocol cpu-limit

Configures the CPU utilization of pods.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration (config)

Syntax Description **monitor protocol cpu-limit** *threshold_percentage*

cpu-limit *threshold_percentage*

Specifies the CPU utilization threshold percentage, based on which the **monitor ptotocol** command in the Exec mode is restricted.

Must be an integer in the range of 1 - 100.

The default value is 70%.

monitor subscriber

Configures the SMF to monitor the subscribers.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **monitor subscriber [supi** *supi* **| imsi** *imsi* **| imei** *imei* **[capture-duration** *duration* **| gr-instance***gr_instance* **| internal-messages yes | namespace** *namespace* **| nf-service** *nf-service* **| transaction-logs yes internal-messages yes | [|]]]**

supi *supi*

Specify the subscriber identifier.

Must be a string.

imsi *imsi*

Specifyes the subscriber IMSI.

Must be a string.

imei *imei*

Specifyes the subscriber IMEI.

Must be a string.

capture-duration *duration*

Specifyes the duration in seconds during which PCAP is captured.

Must be an integer.

The default value is 300 seconds.

gr-instance *gr_instance*

Specifyes the monitor subscriber for given gr-instance only.

Must be an integer.

internal-messages yes |

Specifyes yes in order to enable internal messages.

By default it is disabled.

namespace *namespace*

Specify sgw or smf.

nf-service *nf-service*

Specify sgw or smf.

transaction-logs yes internal-messages

Sets to yes in order to enable internal messages.

By default it is disabled.

msid-opt

Clears subscriber data based on MSID.

Command Modes Exec

Syntax Description **clear subscriber msid** *msid* **[ebi** *eps_bearer_id* **| reactivation { false | true }]**

ebi *eps_bearer_id*

Specify the EPS Bearer ID.

Must be a string.

reactivation { false | true }

Specify if reactivation is requested.

Must be one of the following:

- **false**
- **true**

Usage Guidelines Use this command to subscriber data based on MSID.

nf-tls ca-certificates

Configures NF TLS certificate name and data configuration parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **nf-tls ca-certificates** *certificate_alias_name* **[cert-data** *certificate_data* **]**

ca-certificates *certificate_alias_name*

Specify the alias name for the certificate.

Must be a string.

cert-data *certificate_data*

Specify the certificate data in PEM format.

Must be a string.

Usage Guidelines Use this command to configure certificate name and data configuration parameters.

nf-tls certificate-status

Displays NF TLS certificate status.

Command Modes Exec

Syntax Description **show nf-tls certificate-status [[** *certificate_name* **] [days** *days_to_expire* **] [podInstance** *pod_instance* **]]**

days *days_to_expire*

Specify the number of days for the certificate to expire.

Must be a string.

podInstance *pod_instance*

Specify the Pod instance.

Must be a string.

certificate_name

Specify name of the certificate.

Must be a string.

Usage Guidelines Use this command to view certificate status.

nf-tls certificates

Configures NF TLS certificate parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **nf-tls certificates** *certificate_alias_name* **[[cert-data** *certificate_data* **] [private-key** *private_key* **]]**

cert-data *certificate_data*

Specify the certificate data in PEM format.

Must be a string.

certificates *certificate_alias_name*

Specify the alias name for the certificate.

Must be a string.

private-key *private_key*

Specify the certificate private key in PEM format.

Must be a string.

Usage Guidelines Use this command to configure NF TLS certificate parameters.

no

Restores the command history cache size to its default setting. See the history command.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `no history`

Usage Guidelines Use this command to configure the command history cache size to its default setting. For more details, see the history command.

nodemonitor

Configures the nodemonitor pod to periodically check the operating state of other nodes.

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration (config)

Syntax Description `nodemonitor mode { 0 | 1 | 2 | 3 interval` *wait_time* `}`

mode { 0 | 1 | 2 | 3 interval *wait_time*}

Enable the node monitoring pod to switch to different modes depending on the operating state of nodes.

- **mode 0**—Disables the node monitoring functionality.
- **mode 1**—Enables the node monitoring and performs self-reboot only after reaching a hardcoded value of 2 seconds when two or more nodes are not reachable. This is the default setting.
- **mode 2**—Enables the node monitoring and performs self-reboot when two or more nodes are not reachable but not all the nodes.
- **mode 3 interval** *wait_time*—Specify the time interval in seconds, after which the node monitoring pod is rebooted when two or more nodes are not reachable.

  wait_time must be an integer in the range of 5–300.

Usage Guidelines Use this command to configure nodemonitor pod to periodically check the operating state of other nodes.

nrf discovery-info discovery-filter

Displays NF discovery filter information.

Command Modes Exec > Global Configuration

Syntax Description `show discovery-filter`

Usage Guidelines Use this command to view NF discovery filter information.

nrf discovery-info discovery-filter nf-discovery-profile

Displays discovery profile information.

Command Modes Exec > Global Configuration

Syntax Description `show nf-discovery-profile`

Usage Guidelines Use this command to view NF discovery profile information.

nrf discovery-info discovery-filter nf-discovery-profile nf-service

Displays NF service information.

Command Modes Exec > Global Configuration

Syntax Description `show nf-service`

Usage Guidelines Use this command to view NF service information.

nrf registration-info

Displays NRF registration information.

Command Modes Exec

Syntax Description `show nrf [ registration-info [ gr-instance gr_instance ] ]`

gr-instance *gr_instance*

Specify the GR instance ID.

Must be a string.

Usage Guidelines Use this command to view registration information.

nrf subscription-info

Displays NF subscription information.

Command Modes Exec > Global Configuration

Syntax Description `show nrf subscription-info`

Usage Guidelines Use this command to view NF subscription information.

nssai

Configures the list of DNN profile names.

Command Modes Exec > Global Configuration (config)

Syntax Description `nssai name slice_name [ [ dnn profile_names_list ] [ sdt slice_differentiator_type ] [ sst slice_service_type ] [ tai-group-list tai_group_list ] ]`

dnn *profile_names_list*

Specify the list of actual DNN profile names configured.

Must be a string.

name *slice_name*

Specify name of the slice.

Must be a string.

sdt *slice_differentiator_type*

Specify the Slice Differentiator Type (SDT).

Must be a string in the octet-string24 pattern. For information on the octet-string24 pattern, see the *Input Pattern Types* chapter.

sst *slice_service_type*

Specify the Slice/Service Type (SST).

Must be a string in the sst-string255 pattern. For information on the sst-string255 pattern, see the *Input Pattern Types* chapter.

tai-group-list *tai_group_list*

Specify the list of TAI groups for this NSSAI.

Must be a string.

Usage Guidelines Use this command to configure the list of actual DNN profile names.

paginate

Configures whether or not to paginate CLI command output.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `paginate { false | true }`

{ false | true }

Specify false to disable paginating CLI command output, and true to enable.

Must be either "false" or "true".

Usage Guidelines Use this command to paginate the command output.

pcscf mark-online

Marks the failed P-CSCF addresses online.

Command Modes Exec

Syntax Description **`pcscf mark-online [ all | fqdn`** *`fqdn`* **`| mw-ipv4`** *`IPv4_address`* **`| mw-ipv6`** *`IPv6_address`* **`]`**

pcscf mark-online

Allows marking the failed P-CSCF address online. It has four possible values:

- **all**— This command marks all the P-CSCF addresses online.
- **fqdn** *fqdn*— This command specifies the FQDN to mark online.
- **mw-ipv4** *IPv4_address*— This command specifies the failed P-CSCF IPv4 address to mark online.
- **| mw-ipv6** *IPv6_address*— This command specifies the failed P-CSCF IPv6 address to mark online.

Usage Guidelines Use this command to activate the failed P-CSCF addresses.

peers all

Displays the peer configuration information.

Command Modes Exec

Syntax Description `show peers [ all ]`

Usage Guidelines Use this command to view peer configuration information.

policy

Configures the policy for PCF interaction or the N7 optimization.

Syntax Description **policy [local | optimized] rat-type [nr | wlan | eutra]**

[local|optimized]

policy [local | optimized]

Specify the policy.

Must be one of the following:

- **local**
- **optimized**



Note In case you configure both **policy local** and **policy optimized** together, then **policy local** takes the precendence.

rat-type [nr | wlan | eutra]

Specify the RAT type.

Must be one of the following:

- **nr**
- **wlan**
- **eutra**



Note This keyword is optional. If **rat-type** is not configured then the **policy local** or **policy optimized** is valid for all the three RAT types, which are NR, WLAN, and EUTRA.

Usage Guidelines Use this command to configure the policy for PCF interaction or the N7 optimization.

policy actionmgmt

This configuration adds action definition policies.

Command Modes Exec > Global Configuration (config)

Syntax Description **policy actionmgmt** *policy_actionmgmt_name* **{ actiondef** *actiondef_name* **{ priority** *priority_number* **action** *action_name* **[attributes { rulebase** *rulebase_name* **[rules** *rules_name* **] }]**

actionmgmt *policy_actionmgmt_name*

Configures the action to be executed.

actiondef *actiondef_name*

Defines the action attributes to be executed.

priority *priority_number*

Defines the priority in which the actions are to be executed. *priority_number* must be an integer from 1 to 127.

action *action_name*

Defines the actions associated with an actiondef in the order of priority. The action name can be one of the following:

- activate-rulebase
- continue-session
- create-bearer
- release-flow
- release-flow-ho
- release-session
- terminate-session

For sematic and syntactic error handling, it supports **release-session**, **release-flow**, and **release-flow-ho** as actions.

attributes

Defines the attributes of a particular action. This is an optional command.

rulebase *rulebase_name*

Defines a collection of protocol rules to match a flow and associated actions to be taken for matching flow.

rules *rules_name*

Defines a list of rules to be executed.

Usage Guidelines This configuration is used to add action definition policies.

policy call-control-profile

Configures SGW call control profile for operator policy.

Syntax Description **`call-control-profile`** *`sgw_cc_profile_name`* **`charging-mode`** *`sgw_charging_mode`*
`sgw-charging-profile` *`sgw_charging_profile_name`*

call-control-profile *sgw_cc_profile_name*

Specify name of the SGW Call Control Profile for operator policy.

Must be a string.

charging-mode *sgw_charging_mode*

Specify the SGW charging mode.

Must be one of the following:

- **gtpp**
- **none**

sgw-charging-profile *sgw_charging_profile_name*

Specify name of the associated SGW charging profile.

Usage Guidelines Use this command to configure SGW call control profile for operator policy.

policy call-control-profile cc

Configures charging characteristics selection preference parameter.

Syntax Description **`cc prefer`** *`cc_selection_preference`*

prefer *cc_selection_preference*

Specify the preference for selecting charging characteristics.

Must be one of the following:

- **hlr-hss-value**: Specify hlr-hss-value - value received from serving node.
- **local-value**: Specify local-value - value defined locally.

Default Value: hlr-hss-value.

Usage Guidelines Use this command to configure charging characteristics selection preference parameter.

policy call-control-profile cc local-value

Configures local value for charging characteristics.

Syntax Description **`local-value profile`** *`profile_index`*

profile *profile_index*

Specify the local profile index.

Must be an integer in the range of 1-15.

Default Value: 8.

Usage Guidelines Use this command to configure local value for charging characteristics.

policy dnn

Configures the virtual DNN to operator DNN mapping.

Command Modes Exec > Global Configuration (config)

Syntax Description **dnn** *dnn_policy_name* **[profile** *dnn_profile_name* **]**

dnn *dnn_policy_name*

Specify name of the DNN policy.

Must be a string.

profile *dnn_profile_name*

Specify name of the DNN profile.

Must be a string.

Usage Guidelines Use this command to configure the virtual DNN to operator DNN mapping.

policy dnn dnn dnn

Configures the virtual DNN to a network DNN.

Syntax Description **dnn** *dnn_name* **[profile** *dnn_profile_name* **] dnn-list** *dnn_list*

dnn-list *dnn_list*

Specify the additional list of DNNs to be associated for the DNN profile.

Must be a string.

dnn *dnn_name*

Specify name of the DNN.

Must be a string.

profile *dnn_profile_name*

Specify name of the DNN profile.

Must be a string.

Usage Guidelines Use this command to configure the virtual DNN to a network DNN.

policy dnn dnn network-identifier

Configures the network identifier.

Command Modes Exec > Global Configuration (config) > DNN Configuration (config-dnn-*policy_name*)

Syntax Description **dnn network-identifier** *network_identifier* **[profile** *profile_name* **] [dnn-list** *dnn_list* **]**

network-identifier *network_identifier*

Specify the network identifier.

Must be a string.

profile *profile_name*

Specify name of the profile.

Must be a string.

Usage Guidelines Use this command to configure the network identifier.

policy dnn dnn network-identifier operator-identifier

Configures the operator identifier.

Command Modes Exec > Global Configuration (config) > DNN Configuration (config-dnn-*policy_name*)

Syntax Description **dnn network-identifier** *network_identifier* **operator-identifier** *operator_identifier* **[profile** *profile_name* **]**

operator-identifier *operator_identifier*

Specify the operator identifier.

Must be a string.

profile *profile_name*

Specify name of the profile.

Must be a string.

Usage Guidelines Use this command to configure the operator identifier.

policy dnn dnn operator-identifier

Configures the operator identifier.

Command Modes Exec > Global Configuration (config) > DNN Configuration (config-dnn-*policy_name*)

Syntax Description **dnn operator-identifier** *operator_identifier* **[profile** *profile_name* **] [dnn-list** *dnn_list* **]**

operator-identifier *operator_identifier*

Specify the operator identifier.

Must be a string.

profile *profile_name*

Specify name of the profile.

Must be a string.

Usage Guidelines Use this command to configure the operator identifier.

policy eventmgmt

Configures the event management policies and defines the attributes.

Command Modes Exec > Global Configuration (config)

Syntax Description **policy eventmgmt** *eventmgmt_name* **priority** *event_priority*

eventmgmt *policy_eventmgmt_name*

Configures the event management policies and attributes.

priority *event_priority*

Defines the priority of a particular event management policy.

ruledef *ruledef_name*

Defines a rule for a local policy that when matched an action is performed.

actiondef *actiondef_name*

Configures the action name to be executed.

event *event_type*

Defines an event for which a particular action is to be performed. It supports the following events:

- cb-resp
- imexit
- n1-modify
- new-call

- plmn-ch
- subscription-change
- ub-resp
- xnho

For sematic and syntactic error handling, it supports **n1-modify**, **cbr-resp**, and **ubr-resp** event names.

For UDM data change notification, it supports **subscription-change** event name.

Usage Guidelines This configuration is used for adding the event management policy.

policy network-capability

Configures Network Capability Policy configuration.

Command Modes Exec > Global Configuration (config)

Syntax Description

```
policy network-capability policy_name [ link-mtu link_mtu |
max-supported-pkt-filter max_supported_pkt_filter | nw-support-local-address-tft
 { false | true } ]
```

link-mtu *link_mtu*

Specify name of the Network Capability Policy.

Must be an integer in the range of 1280-2000.

Default Value: 1500.

max-supported-pkt-filter *max_supported_pkt_filter*

Specify the maximum supported packet filters.

Must be an integer in the range of 16-256.

Default Value: 16.

network-capability *policy_name*

Specify name of the Network Capability Policy.

Must be a string.

nw-support-local-address-tft { false | true }

Enable or disable network support for local address in TFT.

Must be one of the following:

- **false**
- **true**

Default Value: false.

Usage Guidelines Use this command to configure Network Capability Policy configuration.

policy operator

Configures the operator policy configuration.

Command Modes Exec > Global Configuration (config)

Syntax Description **policy operator** *policy_name* **call-control-profile** *sgw_cc_profile_name* **roaming-status** *roaming_status*

call-control-profile *sgw_cc_profile_name*

Specify name of the associated SGW Call Control profile.

operator *policy_name*

Specify name of the operator policy.

Must be a string.

roaming-status *roaming_status*

Specify the roaming status.

Must be one of the following:

- **roamer**
- **visitor-lbo**

Usage Guidelines Use this command to configure the operator policy specific configuration.

policy operator policy

Configures DNN policy parameters.

Command Modes Exec > Global Configuration (config) > Operator Policy Configuration (config-operator-*policy_name*)

Syntax Description **policy dnn** *dnn_policy_name* **[network-capability** *network_capability* **]**

dnn *dnn_policy_name*

Specify name of the DNN policy.

Must be a string.

network-capability *network_capability*

Specify the network capability.

Must be a string.

secondary *secondary*

Specify the secondary.

Must be a string.

Usage Guidelines Use this command to configure DNN policy parameters.

policy path-failure-detection

Configures path failure detection policy-specific configuration.

Command Modes Exec > Global Configuration (config)

Syntax Description **`policy path-failure-detection`** *`policy_name`* **`max-remote-rc-change`** *`max_remote_rc_change`*

max-remote-rc-change *max_remote_rc_change*

Specify the maximum remote restart counter change.

Must be an integer in the range of 1-255.

path-failure-detection *policy_name*

Specify name of the Path Failure Detection policy.

Must be a string.

Usage Guidelines Use this command to configure path failure detection policy-specific configuration.

policy path-failure-detection ignore

Configures to ignore counter values, echo timeouts, or echo failures.

Command Modes Exec > Global Configuration (config) > Path Failure Detection Policy Configuration (config-path-failure-detection-*policy_name*)

Syntax Description **`ignore type`** *`ignore_type`*

type *ignore_type*

Specify to ignore restart counter values, echo timeouts, or echo failures.

Must be one of the following:

- **control-rc-change**

- **echo-failure**
- **echo-rc-change**

Usage Guidelines Use this command to configure ignoring counter values, echo timeouts, or echo failures.

policy rulemgmt

This configuration allows adding rule definition policies.

Command Modes Exec > Global Configuration (config)

Syntax Description **policy rulemgmt** *policy_rulemgmt_name* **ruledef** *rule_def* **condition** *condition_string*

rulemgmt *policy_rulemgmt_name*

Defines a rule to be added in the policies.

ruledef *rule_def*

Configures a rule attribute. A ruledef is declared when the conditions match.

condition *condition_string*

Defines the use cases for a rule. It supports the following conditions:

- an-type
- any
- cause
- duplicate-ip
- sarea

For sematic and syntactic error handling, it supports **cause-value matches** and **cause-source matches** conditions.

Use the condition **duplicate-ip** to detect duplicate static IP addresses received from AAA or UDM.

Usage Guidelines This configuration allows adding rule definition policies.

policy subscriber

Configures SMF policy parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **policy subscriber** *policy_name*

policy subscriber *policy_name*

Specify name of the subscriber policy.

Must be a string.

Usage Guidelines Use this command to configure SMF policy parameters.

policy subscriber list-entry

Configures operator policy selection match criteria definition.

Command Modes Exec > Global Configuration (config) > Subscriber Policy Configuration (config-subscriber-*policy_name*)

Syntax Description **precedence** *precedence_number* **[sst** *slice_service_type* **| sdt** *slice_differentiator_type* **| supi-start-range** *supi_start_range* **| supi-stop-range** *supi_stop_range* **| instance-start-range** *instance_start_range* **| instance-stop-range** *instance_stop_range* **| gpsi-start-range** *gpsi_start_range* **| gpsi-stop-range** *gpsi_stop_range* **| pei-start-range** *pei_start_range* **| pei-stop-range** *pei_stop_range* **| operator-policy** *operator_policy_name* **]**

gpsi-start-range *gpsi_start_range*

Specify the GPSI start range.

Must be an integer in the range of 1000000000-999999999999999.

gpsi-stop-range *gpsi_stop_range*

Specify the GPSI stop range.

Must be an integer in the range of 1000000000-999999999999999.

imsi-start-range *imsi_start_range*

Specify the IMSI start range.

Must be an integer in the range of 100000000000000-9999999999999999.

imsi-stop-range *imsi_stop_range*

Specify the IMSI stop range.

Must be an integer in the range of 100000000000000-9999999999999999.

operator-policy *operator_policy_name*

Specify name of the operator policy.

Must be a string.

pei-start-range *pei_start_range*

Specify the PEI start range.

Must be an integer in the range of 1000000000000-9999999999999999.

pei-stop-range *pei_stop_range*

Specify the PEI stop range.

Must be an integer in the range of 1000000000000-9999999999999999.

precedence *precedence_number*

Specify the precedence for entry.

Must be an integer in the range of 1-2048.

sdt *slice_differentiator_type*

Specify the Slice Differentiator Type (SDT).

Must be a string in the octet-string24 pattern. For information on the octet-string24 pattern, see the *Input Pattern Types* chapter.

sst *slice_service_type*

Specify the Slice/Service Type (SST).

Must be a string in the octet-string8 pattern. For information on the octet-string8 pattern, see the *Input Pattern Types* chapter.

supi-start-range *supi_start_range*

Specify the SUPI start range.

Must be an integer in the range of 100000000000000-999999999999999.

supi-stop-range *supi_stop_range*

Specify the SUPI stop range.

Must be an integer in the range of 100000000000000-999999999999999.

instance-start-range *instance_start_range*

Specify the SMF instance start range for the DNN profile selection. Must be an integer in the range of 1 to 8.

instance-stop-range *instance_stop_range*

Specify the SMF instance stop range for the DNN profile selection. Must be an integer in the range of 1 to 8.

Usage Guidelines

Use this command to configure operator policy selection match criteria definition.

policy subscriber list-entry imsi

Configures subscriber International Mobile Station Identification (IMSI).

Command Modes Exec > Global Configuration (config) > Subscriber Policy Configuration (config-subscriber-*policy_name*) > Subscriber Policy Precedence Configuration (config-subscriber-*precedence*)

Syntax Description **imsi mcc** *mobile_country_code* **mnc** *mobile_network_code*

mcc *mobile_country_code*

Specify the Mobile Country Code (MCC).

Must be a string in the three-digit pattern. For information on the three-digit pattern, see the *Input Pattern Types* chapter.

mnc *mobile_network_code*

Specify the Mobile Network Code (MNC).

Must be a string in the two-or-three-digit pattern. For information on the two-or-three-digit pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure subscriber IMSI.

policy subscriber list-entry imsi msin

Configures MSIN range for mobile subscriber identification number.

Command Modes Exec > Global Configuration (config) > Subscriber Policy Configuration (config-subscriber-*policy_name*) > Subscriber Policy Precedence Configuration (config-subscriber-*precedence*)

Syntax Description **imsi msin first** *start_msin_range* **last** *end_msin_range*

first *start_msin_range*

Specify starting value of the MSIN range.

Must be an integer in the range of 1-9999999999.

last *end_msin_range*

Specify the ending value of the MSIN range.

Must be an integer in the range of 1-9999999999.

Usage Guidelines Use this command to configure MSIN range for mobile subscriber identification number.

policy subscriber list-entry serving-plmn

Configures serving PLMN parameters.

Command Modes Exec > Global Configuration (config) > Subscriber Policy Configuration (config-subscriber-*policy_name*) > Subscriber Policy Precedence Configuration (config-subscriber-*precedence*)

Syntax Description **serving-plmn [mcc** *mobile_country_code* **| mnc** *mobile_network_code* **| mnc-list** *mnc_list* **]**

mcc *mobile_country_code*

Specify the Mobile Country Code (MCC) portion of the PLMN ID.

Must be a string in the three-digit pattern. For information on the three-digit pattern, see the *Input Pattern Types* chapter.

mnc-list *mnc_list*

Specify the MNC list.

Must be a string in the two-or-three-digit pattern. For information on the two-or-three-digit pattern, see the *Input Pattern Types* chapter.

mnc *mobile_network_code*

Specify the Mobile Network Code (MNC) portion of the PLMN ID.

Must be a string in the two-or-three-digit pattern. For information on the two-or-three-digit pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure serving PLMN parameters.

policy sx-path-failure-detection

Configures Sx Path Failure Detection Policy-specific configuration.

Command Modes Exec > Global Configuration (config)

Syntax Description **policy sx-path-failure-detection** *policy_name*

sx-path-failure-detection *policy_name*

Specify name of the Sx Path Failure Detection policy.

Must be a string.

Usage Guidelines Use this command to configure Sx Path Failure Detection Policy-specific configuration.

policy sx-path-failure-detection ignore

Configures to ignore heartbeat-retry-failure or the heartbeat-recovery-timestamp-change configuration.

Command Modes Exec > Global Configuration (config) > Sx Path Failure Detection Policy Configuration (config-sx-path-failure-detection-*policy_name*)

Syntax Description **ignore** *ignore_type*

ignore *ignore_type*

Specify to ignore heartbeat-retry-failure or the heartbeat-recovery-timestamp-change configuration.

Must be one of the following:

- **heartbeat-recovery-timestamp-change**
- **heartbeat-retry-failure**

Usage Guidelines Use this command to configure ignoring the heartbeat-retry-failure or the heartbeat-recovery-timestamp-change configuration.

policy upf-selection

Configures UPF selection policy parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **policy upf-selection** *policy_name*

upf-selection *policy_name*

Specify name of the UPF selection policy.

Must be a string.

Usage Guidelines Use this command to configure UPF selection policy parameters.

policy upf-selection list-entry

Configures UPF selection match criteria definition.

Command Modes Exec > Global Configuration (config) > UPF Selection Policy Configuration (config-upf-selection-*policy_name*)

Syntax Description **precedence** *entry_precedence*

precedence *entry_precedence*

Specify the precedence for entry.

Must be an integer in the range of 1-4.

Usage Guidelines Use this command to configure UPF selection match criteria definition.

policy upf-selection list-entry query-params

Configures the query parameter for UPF selection.

Command Modes Exec > Global Configuration (config) > UPF Selection Policy Configuration (config-upf-selection-*policy_name*) > UPF Selection Policy Precedence Configuration (config-upf-selection-*precedence*)

Syntax Description **query-params** *query_params*

query-params *query_params*

Specify the query parameters. If both pdn-type-subscription and pdn-type-session are configured, pdn-type-subscription will be considered.

Must be one of the following:

- **dcnr**
- **dnn**
- **location**
- **pdn-type-session**
- **pdn-type-subscription**
- **slice**

Usage Guidelines Use this command to configure the query parameter for UPF selection.

profile access

Configures the access profile.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile access** *access_profile_name*

access *access_profile_name*

Specify name of the access profile.

Must be a string.

Usage Guidelines Use this command to configure the access profile.

profile access eps-fallback cbr

Configures Create Dedicated Bearer parameters.

Command Modes Exec > Global Configuration (config) > Access Profile Configuration (config-access-*profile_name*)

Syntax Description **eps-fallback cbr delay** *delay_duration* **max-retry** *max_retry* **timeout** *timeout_interval*

delay *delay_duration*

Specify the Create Dedicated Bearer delay duration in milliseconds.

Must be an integer in the range of 0-10000.

Default Value: 0.

max-retry *max_retry*

Specify the Create Dedicated Bearer maximum retry count.

Must be an integer in the range of 0-10.

Default Value: 0.

timeout *timeout_interval*

Specify the Create Dedicated Bearer Retry interval in seconds.

Must be an integer in the range of 1-3.

Default Value: 1.

Usage Guidelines Use this command to configure Create Dedicated Bearer parameters.

profile access eps-fallback guard

Configures handling EPS fallback expiry.

Command Modes Exec > Global Configuration (config) > Access Profile Configuration (config-access-*profile_name*)

Syntax Description **eps-fallback guard timeout** *eps_fallback_timer*

timeout *eps_fallback_timer*

Specify the EPS fallback guard timer in milliseconds.

Must be an integer in the range of 500-15000.

Default Value: 10000.

Usage Guidelines Use this command to configure handling EPS fallback expiry.

profile access eps-fallback trigger-cause group

Configures the cause to trigger EPSFallback.

Command Modes Exec > Global Configuration (config)

Syntax Description **trigger-cause group cause-group** *cause_group* **value** *cause_types*

cause-group *cause_group*

Specify the cause group.

Must be one of the following:

- **misc**
- **nas**
- **protocol**
- **radioNetwork**
- **transport**

value *cause_types*

Specify the list of cause types for which EPSFallback can be triggered.

Must be an integer in the range of 0-46.

You can configure a maximum of four elements with this keyword.

Usage Guidelines Use this command to configure the cause to trigger EPSFallback.

profile access erir

Configures the ERIR parameters.

Command Modes Exec > Global Configuration (config) > Access Profile Configuration (config-access-*profile_name*)

Syntax Description **erir delay** *erir_delay*

delay *erir_delay*

Specify the ERIR delay duration for 4G/WIFI sessions in milliseconds.

Must be an integer in the range of 0-3000.

Default Value: 0.

Usage Guidelines Use this command to configure the ERIR parameters.

profile access gtpc

Configures the GTPC Failure Handling profile.

Command Modes Exec > Global Configuration (config) > Access Profile Configuration (config-access-*profile_name*)

Syntax Description **gtpc { class-map-cause-profile** *profile_name* **| gtpc-failure-profile** *profile_name* **}**

class-map-cause-profile *profile_name*

Specify name of the Class Map Cause profile.

Must be a string.

gtpc-failure-profile *profile_name*

Specify name of the GTPC Failure Handling profile.

Usage Guidelines Use this command to configure the GTPC Failure Handling profile.

profile access gtpc message-handling create-session-request ho-ind

Configures handling of Create Session Request received with HO Indicator.

Command Modes Exec > Global Configuration (config) > Access Profile Configuration (config-access-*profile_name*)

Syntax Description **`gtpc message-handling create-session-request ho-ind [ new-call-reject ]`**

create-session-request ho-ind new-call-reject

Specify to reject Create Session Request received with HO Indicator, if session is not present.

Usage Guidelines Use this command to configure handling of Create Session Request received with HO Indicator.

profile access gtpc message-handling create-session-response action

Configures action for GTPC message.

Command Modes Exec > Global Configuration (config) > Access Profile Configuration (config-access-*profile_name*)

Syntax Description **`gtpc message-handling create-session-response action [ apn-ambr ]`**

apn-ambr

Specify APN Aggregate Maximum Bit Rate (APN-AMBR).

Usage Guidelines Use this command to configure action for GTPC message.

profile access gtpc message-handling create-session-response condition

Configures IP Exhaust condition.

Command Modes Exec > Global Configuration (config) > Access Profile Configuration (config-access-*profile_name*)

Syntax Description **n1 message-handling pdu-establishment condition [ip-exhaust [action** *action* **[cause** *cause_in_response* **]]]**

action *action*

Specify the action.

Must be one of the following:

- **backoff**

cause *cause_in_response*

Specify the cause in response. Check the specification for the integer value.

Must be an integer in the range of 0-255.

Default Value: 0.

ip-exhaust

Specify the IP exhaust condition.

Usage Guidelines Use this command to configure IP Exhaust condition.

profile access n1 message-handling pdu-establishment condition

Configures IP Exhaust condition.

Command Modes Exec > Global Configuration (config) > Access Profile Configuration (config-access-*profile_name*)

Syntax Description **gtpc message-handling create-session-response condition [ip-exhaust [action** *action* **[cause** *cause_in_response* **]]]**

action *action*

Specify the action.

Must be one of the following:

- **backoff**

cause *cause_in_response*

Specify the cause in response. Check the specification for the integer value.

Must be an integer in the range of 0-40.

Default Value: 0.

ip-exhaust

Specify the IP exhaust condition.

Usage Guidelines Use this command to configure IP Exhaust condition.

profile access n1 message-handling pdu-release condition

Configures N4 Path Fail condition.

Command Modes Exec > Global Configuration (config) > Access Profile Configuration (config-access-*profile_name*)

Syntax Description **n1 message-handling pdu-release condition [n4-pathfail [action** *action* **[cause** *cause_in_response* **]]]**

action *action*

Specify the action.

Must be one of the following:

- **backoff**

cause *cause_in_response*

Specify the cause in response. Check the specification for the integer value.

Must be an integer in the range of 0-40.

n4-pathfail

Specify the N4 Path Fail condition.

Usage Guidelines Use this command to configure N4 Path Fail condition.

profile access n1 t3591-pdu-mod-cmd

Configures the N1 timer t3591 - PDU Session Modify Command Retransmission Timer.

Command Modes Exec > Global Configuration (config) > Access Profile Configuration (config-access-*profile_name*)

Syntax Description **n1 t3591-pdu-mod-cmd timeout** *timeout_period* **max-retry** *max_retries*

max-retry *max_retries*

Specify the PDU Modify Command maximum retry count.

Must be an integer in the range of 0-10.

Default Value: 2.

timeout *timeout_period*

Specify the PDU Modify Command timer in seconds.

Must be an integer in the range of 1-16.

Default Value: 2.

Usage Guidelines Use this command to configure the n1 timer t3591 - PDU Session Modify Command Retransmission Timer.

profile access n1 t3592-pdu-rel-cmd

Configures the N1 timer t3592 - PDU Sess Rel Command retransmission timer for cause 39 - retransmission required.

Command Modes Exec > Global Configuration (config) > Access Profile Configuration (config-access-*profile_name*)

Syntax Description **`n1 t3592-pdu-rel-cmd timeout`** *`timeout`* **`max-retry`** *`max_retry`*

max-retry *max_retry*

Specify the PDU Release Command Max Retry Count.

Must be an integer in the range of 0-10.

Default Value: 4.

timeout *timeout*

Specify the PDU Release Command timer in seconds for cause 39.

Must be an integer in the range of 1-16.

Default Value: 4.

Usage Guidelines Use this command to configure the n1 timer t3592 - PDU Sess Rel Command retransmission timer for cause 39 - retransmission required.

profile access n1

Configures the N1 interface.

Command Modes Exec > Global Configuration (config) > Access Profile Configuration (config-access-*profile_name*)

Syntax Description **`n1 n1-failure-profile`** *`n1_failure_profile`* **`[ class-map-cause-profile`** *`class_map_cause_profile`* **`]`**

class-map-cause-profile *class_map_cause_profile*

Specify the class map cause profile.

Must be a string.

n1-failure-profile *n1_failure_profile*

Specify the N1 failure profile.

Usage Guidelines Use this command to configure the N1 interface.

profile access n2

Configures the N2 interface.

Command Modes Exec > Global Configuration (config) > Access Profile Configuration (config-access-*profile_name*)

Syntax Description **n2 n2-failure-profile** *n2_failure_profile* **[class-map-cause-profile** *class_map_cause_profile* **]**

class-map-cause-profile *class_map_cause_profile*

Specify the class map cause profile.

Must be a string.

n2-failure-profile *n2_failure_profile*

Specify the N2 failure profile.

Usage Guidelines Use this command to configure the N2 interface.

profile access n11

Configures the N11 interface.

Command Modes Exec > Global Configuration (config) > Access Profile Configuration (config-access-*profile_name*)

Syntax Description **n11 n11-failure-profile** *n11_failure_profile* **[class-map-cause-profile** *class_map_cause_profile* **]**

class-map-cause-profile *class_map_cause_profile*

Specify the class map cause profile.

Must be a string.

n11-failure-profile *n11_failure_profile*

Specify the N11 failure profile.

Usage Guidelines Use this command to configure the N11 interface.

profile access n2 idft

Configures N2 or N26 Indirect Data Forwarding Tunnel (IDFT) support.

Command Modes Exec > Global Configuration (config) > Access Profile Configuration (config-access-*profile_name*)

Syntax Description **`n2 idft enable timeout`** *`idft_timeout`*

Syntax Description **`n26 idft enable timeout`** *`idft_timeout`*

enable

Specify to enable IDFT support.

timeout *idft_timeout*

Specify the IDFT timeout period in seconds.

Must be an integer in the range of 15-60.

Usage Guidelines Use this command to configure N2 or N26 IDFT support.

profile access n26 idft

Configures N2 or N26 Indirect Data Forwarding Tunnel (IDFT) support.

Command Modes Exec > Global Configuration (config) > Access Profile Configuration (config-access-*profile_name*)

Syntax Description **`n2 idft enable timeout`** *`idft_timeout`*

Syntax Description **`n26 idft enable timeout`** *`idft_timeout`*

enable

Specify to enable IDFT support.

timeout *idft_timeout*

Specify the IDFT timeout period in seconds.

Must be an integer in the range of 15-60.

Usage Guidelines Use this command to configure N2 or N26 IDFT support.

profile charging

Configures the charging profile.

Command Modes

Exec > Global Configuration (config)

Syntax Description

profile charging *profile_name* **[max-charging-condition** *max_changes* **| max-deferred-urr** *max_deferred_urr* **| max-secondary-rat-reports** *max_secondary_rat_reports* **| metering-method** *metering_method* **| method** *charging_method* **| offline-interim-timer** *timer_duration* **| ooo-retry-interval** *ooo_report_retry_interval* **| query-all-urr { false | true } | tight-interworking-mode { false | true }]**

charging *profile_name*

Specify the charging profile configuration.

Must be a string.

max-charging-condition *max_changes*

Specify the maximum number of charging condition changes.

Must be an integer in the range of 0-500.

Default Value: 20.

max-deferred-urr *max_deferred_urr*

Specify the maximum number of deferred USU containers.

Must be an integer in the range of 1-200.

Default Value: 50.

max-secondary-rat-reports *max_secondary_rat_reports*

Specify the maximum number of secondaryRatDataUsageReports to trigger CHF update.

Must be an integer in the range of 0-50.

Default Value: 0.

metering-method *metering_method*

Specify the parameters to be metered.

Must be one of the following:

- **duration-volume**
- **duration**
- **volume**

Default Value: duration-volume.

method *charging_method*

Specify the charging method. Default Value: offline.

Must be one of the following:

- **none**
- **offline**
- **online**

offline-interim-timer *timer_duration*

Specify the offline interim timer duration in seconds.

Must be an integer.

Default Value: 60.

ooo-retry-interval *ooo_report_retry_interval*

Specify the interval, in milliseconds, at which OOO report will be retried.

Must be an integer in the range of 5-5000.

You can configure a maximum of five elements with this keyword.

query-all-urr { false | true }

Specify to enable or disable query all URRs.

Must be one of the following:

- **false**
- **true**

Default Value: true.

tight-interworking-mode { false | true }

Specify to enable or disable tight interworking mode for online/offline charging methods.

Must be one of the following:

- **false**
- **true**

Default Value: false.

Usage Guidelines Use this command to configure the charging profile.

profile charging accounting limit

Configures the duration threshold for accounting.

Command Modes Exec > Global Configuration (config) > Charging Profile Configuration (config-charging-*profile_name*)

Syntax Description **`accounting limit duration`** *`threshold`*

duration *threshold*

Specify the duration threshold for accounting.

Must be an integer in the range of 0-2147483647.

Usage Guidelines Use this command to configure the duration threshold for accounting.

profile charging accounting limit volume

Configures the volume threshold for accounting.

Command Modes Exec > Global Configuration (config) > Charging Profile Configuration (config-charging-*profile_name*)

Syntax Description **accounting limit volume { downlink** *downlink_volume_limit* **| total** *total_volume_limit* **| uplink** *uplink_volume_limit* **}**

downlink *downlink_volume_limit*

Specify the downlink volume limit in bytes for interim generation.

Must be an integer in the range of 100000-4000000000.

total *total_volume_limit*

Specify the total volume limit in bytes for interim generation.

Must be an integer in the range of 100000-4000000000.

uplink *uplink_volume_limit*

Specify the uplink volume limit in bytes for interim generation.

Must be an integer in the range of 100000-4000000000.

Usage Guidelines Use this command to configure the volume threshold for accounting.

profile charging dynamic-rules request-quota

Configures the dynamic rules request quota.

Command Modes Exec > Global Configuration (config) > Charging Profile Configuration (config-charging-*profile_name*)

Syntax Description **dynamic-rules request-quota { on-receiving-rule | on-traffic-match }**

on-receiving-rule

Specify this value to send CCR-I message with RSU on receiving the dynamic rule.

on-traffic-match

Specify this value to send CCR-I message with RSU on receiving the start of traffic.

Default Value: **on-receiving-rule**.

Usage Guidelines Use this command to configure dynamic rules request quota.

profile charging failure-handling error-type

Configures the failure handling error type for Rating Group-level and application-level errors.

Command Modes Exec > Global Configuration (config) > Charging Profile Configuration (config-charging-*profile_name*)

Syntax Description **`failure-handling error-type [ rg | app ] error-value`** *`error_value`* **`action`** *`action_value`*

failure-handling error-type [rg | app]

Specify this value to configure the failure handling error type as Rating Group or Application.

error-value *error_value* action *action_value*

For the application-level errors, specify one of the following values for *action_value*

- **drop-data**—Specify this value to drop data corresponding to the charging ID.
- **terminate**—Specify this value to release the PDU session.
- **continue**—Specify this value to disable charging.

For the Rating Group-level errors, enter one of the following values for *action_value*:

- **convert-offline**—Specify this value to convert to offline charging.
- **delete-flow**—Specify this value to delete the flow or rule associated with the Rating Group.
- **drop-data**—Specify this value to drop data corresponding to the Rating Group.
- **terminate**—Specify this value to release the PDU session.

Note

- If you haven't configured an action for the Rating Group-level and application-level errors, the SMF continues with the default behavior.
- SMF doesn’t allow mapping of multiple QoS flows to the same Rating Group for dynamic rules.
- The **drop-data** action is applicable to all the flows that are associated to the Rating Group.

Usage Guidelines Use this command to configure failure handling error type for Rating Group-level and application-level errors.

profile charging limit

Configures the duration and volume thresholds.

Command Modes Exec > Global Configuration (config) > Charging Profile Configuration (config-charging-*profile_name*)

Syntax Description **limit { duration** *duration_threshold* **| volume** *volume_threshold* **}**

duration *duration_threshold*

Specify the duration threshold for charging.

Must be an integer in the range of 60-40000000.

volume *volume_threshold*

Specify the volume threshold for charging.

Must be an integer in the range of 10000-4000000000.

Usage Guidelines Use this command to configure the duration and volume thresholds.

profile charging limit rating-group

Configures the rating group volume and duration thresholds.

Command Modes Exec > Global Configuration (config) > Charging Profile Configuration (config-charging-*profile_name*)

Syntax Description **limit rating-group { duration** *duration_threshold* **| volume** *volume_threshold* **}**

duration *duration_threshold*

Specify the duration threshold for charging.

Must be an integer in the range of 60-40000000.

volume *volume_threshold*

Specify the volume threshold for charging.

Must be an integer in the range of 10000-4000000000.

Usage Guidelines Use this command to configure the rating group duration and volume thresholds.

profile charging mscc-final-unit-action terminate session

Terminates the session when MSCC final unit action is terminate.

.

Command Modes Exec > Global Configuration (config) > Charging Profile Configuration (config-charging-*profile_name*)

Syntax Description **mscc-final-unit-action terminate session**

mscc-final-unit-action terminate session

Terminate the session when MSCC final unit action is terminate.

Usage Guidelines Use this command to terminate the session when the MSCC final unit action is terminate.

profile charging offline zero-usage

Configures offline charging zero-usage parameters.

Command Modes Exec > Global Configuration (config) > Charging Profile Configuration (config-charging-*profile_name*)

Syntax Description **offline zero-usage [drop** *suppress_for_zero_usage* **| measurement** *parameters_to_suppress* **| trigger** *triggers_to_suppress* **]**

drop *suppress_for_zero_usage*

Specify the parameters to suppress for zero usage.

Must be one of the following:

- **cdr**
- **uuc**

measurement *parameters_to_suppress*

Specify the parameters to be suppressed.

Must be one of the following:

- **duration**
- **volume**

trigger *triggers_to_suppress*

Specify the list of triggers to be suppressed.

Must be one of the following:

- **external**
- **final**
- **internal**

Usage Guidelines Use this command to configure offline charging zero-usage parameters.

profile charging quota

Configures the charging quota parameters.

Command Modes Exec > Global Configuration (config) > Charging Profile Configuration (config-charging-*profile_name*)

Syntax Description **quota request** *request_quota*

request *request_quota*

Specify the request quota from CHF.

Must be one of the following:

- **always**
- **standard**

Default Value: standard.

Usage Guidelines Use this command to configure the charging quota parameters.

profile charging quota suppress

Configures the list of triggers to be suppressed.

Command Modes Exec > Global Configuration (config) > Charging Profile Configuration (config-charging-*profile_name*)

Syntax Description **quota suppress triggers** *triggers_to_suppress*

triggers *triggers_to_suppress*

Specify the list of triggers to be suppressed.

Must be one of the following:

- **qht**

Usage Guidelines Use this command to configure the list of triggers to be suppressed.

profile charging quota validity-time

Configures the validity lifetime of the quota.

Command Modes Exec > Global Configuration (config) > Charging Profile Configuration (config-charging-*profile_name*)

Syntax Description **quota validity-time** *validity_time*

validity-time *validity-time*

Specify the validity lifetime of the quota.

Must be an integer in the range of 1 through 4000000 seconds.

Usage Guidelines Use this command to configure the charging validity lifetime of the quota.

profile charging quota volume-threshold percent

Configures the volume threshold value as a percentage of the volume quota.

Command Modes Exec > Global Configuration (config) > Charging Profile Configuration (config-charging-*profile_name*)

Syntax Description **`quota volume-threshold percent`** *`volume-threshold percent`*

volume-threshold percent *volume-threshold percent*

Specify the volume threshold value as a percentage of the volume quota.

Must be an integer in the range of 1 through 100.

Usage Guidelines Use this command to configure the charging volume threshold value as a percentage of the volume quota.

profile charging reporting-level

Configures the usage reporting level to be used if not sent by the PCF.

Command Modes Exec > Global Configuration (config) > Charging Profile Configuration (config-charging-*profile_name*)

Syntax Description **`reporting-level { offline`** *`reporting_level`* **`| online`** *`reporting_level`* **`}`**

offline *reporting_level*

Specify the reporting level configuration for offline.

Must be one of the following:

- **rating-group**
- **service-id**

Default Value: rating-group.

online *reporting_level*

Specify the reporting level configuration for online.

Must be one of the following:

- **rating-group**
- **service-id**

Default Value: rating-group.

Usage Guidelines Use this command to configure the usage reporting level to be used if not sent by the PCF.

profile charging requested-service-unit

Configures the Requested Service Unit time parameter.

Command Modes Exec > Global Configuration (config) > Charging Profile Configuration (config-charging-*profile_name*)

Syntax Description **requested-service-unit time** *rsu_time*

time *rsu_time*

Specify the Requested Service Unit time value in seconds.

Must be an integer in the range of 1-4000000000.

Usage Guidelines Use this command to configure the Requested Service Unit time parameter.

profile charging requested-service-unit volume

Configures the Requested Service Unit Volume parameters.

Command Modes Exec > Global Configuration (config) > Charging Profile Configuration (config-charging-*profile_name*)

Syntax Description **requested-service-unit volume { uplink** *uplink_volume* **| downlink** *downlink_volume* **| total** *total_volume* **}**

downlink *downlink_volume*

Specify the downlink volume in bytes.

Must be an integer in the range of 1-4000000000.

total *total_volume*

Specify the total volume in bytes.

Must be an integer in the range of 1-4000000000.

uplink *uplink_volume*

Specify the uplink volume in bytes.

Must be an integer in the range of 1-4000000000.

Usage Guidelines Use this command to configure the Requested Service Unit Volume parameters.

profile charging send charging-initial

Configures the option to send CCR-I message towards OCS when dynamic and predefined rules are received or when the usage report is received with the start of traffic.

Command Modes Exec > Global Configuration (config) > Charging Profile Configuration (config-charging-*profile_name*)

Syntax Description **`send charging-initial { session-start | traffic-start }`**

session-start

Specify whether to send CCR-I message towards OCS on receiving the dynamic and predefined rules.

traffic-start

Specify whether to send the CCR-I message towards OCS on receiving the usage report with the start of traffic.

The default value is **session-start**.

Usage Guidelines Use this command to configure an option for sending CCR-I message towards OCS when dynamic and predefined rules are received or when the usage report is received with the start of traffic.

profile charging session-failover

Configure the Diameter session failover for the Gy interface.

Command Modes Exec > Global Configuration (config) > Charging Profile Configuration (config-charging-*profile_name*)

Syntax Description **`session-failover { false | true }`**

false

Disable the Diameter session failover for Gy.

true

Enable the Diameter session failover for Gy.

Default Value: **false**

Usage Guidelines Use this command to configure Diameter session failover for Gy.

profile charging tariff-time-change

Configures timestamps for tariff-time change.

Command Modes Exec > Global Configuration (config) > Charging Profile Configuration (config-charging-*profile_name*)

Syntax Description **`tariff-time-change { hour`** *`hour`* **`| minute`** *`minute`* **`}`**

hour *hour*

Specify the hour timestamp for tariff-time change.

Must be an integer in the range of 0-23.

minute *minute*

Specify the minute timestamp for tariff-time change.

Must be an integer in the range of 0-59.

Usage Guidelines Use this command to configure timestamps for tariff-time change.

profile charging triggers

Configures the list of triggers.

Command Modes Exec > Global Configuration (config) > Charging Profile Configuration (config-charging-*profile_name*)

Syntax Description **triggers session** *triggers*

session *triggers*

Specify the list of session-level triggers.

Must be one of the following:

- **3gpp-ps-change**
- **ambr-change**
- **max-number-of-changes-in-charging-conditions**
- **plmn-change**
- **qos-change**
- **rat-change**
- **serv-node-change**
- **tarrif-time-change**
- **ue-pra-change**
- **ue-time-change**
- **upf-add**
- **upf-rem**
- **user-loc-change**

Usage Guidelines Use this command to configure the list of triggers.

profile charging-characteristics

Configures the charging characteristics profile.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile charging-characteristics** *cc_profile_name* **[[charging-profile** *charging_profile_name* **] [charging-qbc-profile** *charging_qbc_profile_name* **]]**

charging-characteristics *cc_profile_name*

Specify name of the charging characteristics profile. For example, 1, 2, 3, 12, 14, till 16.

Must be a string of 1-2 characters in the pattern '[0-9]*'.

charging-profile *charging_profile_name*

Specify name of the Charging profile.

Must be a string.

charging-qbc-profile *charging_qbc_profile_name*

Specify name of the Charging QBC profile.

Must be a string.

Usage Guidelines Use this command to configure the charging characteristics profile.

profile charging-characteristics network-element-profile-list

Configures the network elements profile list.

Command Modes Exec > Global Configuration (config) > Charging Characteristics Profile Configuration (config-charging-characteristics-*profile_name*)

Syntax Description **network-element-profile-list chf** *charging_server*

chf *charging_server*

Specify the list of charging servers.

Must be a string.

Usage Guidelines Use this command to configure the network elements profile list.

profile charging-qbc

Configures the Charging QBC profile.

Command Modes Exec > Global Configuration (config) > Charging Characteristics Profile Configuration (config-charging-characteristics-*profile_name*)

Syntax Description **charging-qbc** *charging_qbc_profile_name* **[[max-charging-condition** *max_charging_condition_changes* **] [max-deferred-urr** *max_deferred_urr* **] [**

ooo-retry-interval *ooo_report_retry_interval* **] [triggers** *bearer_level_triggers* **]]**

charging-qbc ***charging_qbc_profile_name***

Specify name of the Charging QBC profile.

Must be a string.

max-charging-condition ***max_charging_condition_changes***

Specify the maximum number of charging condition changes.

Must be an integer in the range of 0-500.

Default Value: 20.

max-deferred-urr ***max_deferred_urr***

Specify the maximum number of deferred USU containers.

Must be an integer in the range of 1-200.

Default Value: 50.

ooo-retry-interval ***ooo_report_retry_interval***

Specify the list intervals at which OOO report will be retried in miliseconds. Default: 5 50 2000.

Must be an integer in the range of 5-5000.

You can configure a maximum of five elements with this keyword.

triggers ***bearer_level_triggers***

Specify the list of bearer level triggers.

Must be one of the following:

- **3gpp-ps-change**
- **ambr-change**
- **max-number-of-changes-in-charging-conditions**
- **plmn-change**
- **qos-change**
- **rat-change**
- **serv-node-change**
- **tarrif-time-change**
- **ue-pra-change**
- **ue-time-change**
- **upf-add**

- **upf-rem**
- **user-loc-change**

Usage Guidelines Use this command to configure the Charging QBC profile.

profile charging-qbc limit

Configures the thresholds.

Command Modes Exec > Global Configuration (config) > Charging Characteristics Profile Configuration (config-charging-characteristics-*profile_name*)

Syntax Description **limit { duration** *duration_threshold* **| volume** *volume_threshold* **}**

duration *duration_threshold*

Specify the duration threshold for charging.

Must be an integer in the range of 60-40000000.

volume *volume_threshold*

Specify the volume threshold for charging.

Must be an integer in the range of 10000-4000000000.

Usage Guidelines Use this command to configure the thresholds.

profile charging usage-reporting quota-to-report based-on-grant

Configures the charging usage reporting quota to report volume or duration in Used Service Unit to OCS if it is granted in Granted Service Unit by OCS server.

Command Modes Exec > Global Configuration (config) > Charging Profile Configuration (config-charging-*profile_name*)

Syntax Description **usage-reporting quota-to-report based-on-grant { report-only-granted-volume }**

quota-to-report based-on-grant {report-only-granted-volume}

The **based-on-grant** option specifies the report volume or duration in Used Service Unit to OCS if only it is granted in Granted Service Unit by OCS server. The **report-only-granted-volume** option specifies the filter for sending Used Volume quota to OCS base on Input, Output, or Total Octets granted in Granted Service Unit by OCS server.

Usage Guidelines Use this command to configure the charging usage reporting quota to report volume or duration in Used Service Unit to OCS if it is granted in Granted Service Unit by OCS server.

profile compliance

Configures 3GPP compliance configuration.

Command Modes Exec > Global Configuration (config)

Syntax Description **compliance** *profile_name*

compliance *profile_name*

Specify name of the compliance profile.

Must be a string.

Usage Guidelines Use this command to configure the 3GPP compliance configuration.

profile compliance service

Configures the SMF service names.

Command Modes Exec > Global Configuration (config) > Compliance Profile Configuration (config-compliance-*profile_name*)

Syntax Description **service** *service_name*

service_name

Specify the service names.

Must be one of the following:

- **n1**
- **n2**
- **namf-comm**
- **nchf-convergedcharging**
- **nnrf-disc**
- **nnrf-nfm**
- **npcf-smpolicycontrol**
- **nsmf-pdusession**
- **nudm-sdm**
- **nudm-uecm**
- **threegpp23502**

Usage Guidelines Use this command to configure the SMF service names. The service names are specified in 3GPPTS 29.510 V15.2.0, Section 6.1.6.3.11.

profile compliance service n1

Configures the 3GPP n1 specification version number.

Command Modes Exec > Global Configuration (config) > Compliance Profile Configuration (config-compliance-*profile_name*)

Syntax Description **service n1 version { full** *full_version* **| spec** *3gpp_spec_version* **| uri** *version_uri* **} | version-list version** *version_name* **{ full** *full_version* **| mode { active | offline } | spec** *3gpp_spec_version* **| uri** *version_uri* **}**

version

Specify the 3GPP compliance version to configure. It allows only one compliance version to be configured at a time.

full *full_version*

Specify the full version in the format *major-version*.*minor-version*.*patch-version*.[alpha-*draft-number*].

Must be a string in the pattern '\d+.\d+.\d+^?(.alpha-\d+)?'.

spec *3gpp_spec_version*

Specify the 3GPP N1 specification version number.

Must be one of the following:

- **15.2.0**
- **15.4.0**

Default Value: 15.2.0.

uri *version_uri*

Specify the version URI.

Must be a string in the pattern 'v\d'.

version-list version *version_name*

Specify the 3GPP compliance versions to configure. It allows a maximum of two compliance versions to be configured at a time.

mode { active | offline }

Specify the status of configured 3GPP compliance versions. **mode** is an optional configuration. The default value is **active**. If **version-list version** is configured with two versions, then at least one version should be **active**.

Usage Guidelines Use this command to configure the 3GPP n1 specification version number.

profile compliance service n2

Configures the 3GPP n2 service specification version number.

Command Modes Exec > Global Configuration (config) > Compliance Profile Configuration (config-compliance-*profile_name*)

Syntax Description **service n2 version { full** *full_version* **| spec** *3gpp_spec_version* **| uri** *version_uri* **} | version-list version** *version_name* **{ full** *full_version* **| mode { active | offline } | spec** *3gpp_spec_version* **| uri** *version_uri* **}**

version

Specify the 3GPP compliance version to configure. It allows only one compliance version to be configured at a time.

full *full_version*

Specify the full version in the format *major-version*.*minor-version*.*patch-version*.[alpha-*draft-number*].

Must be a string in the pattern '\d+.\d+.\d+^?(.alpha-\d+)?'.

spec *3gpp_spec_version*

Specify the 3GPP n2 service specification version number.

Must be one of the following:

- **15.0.0**
- **15.2.0**
- **15.4.0**

Default Value: 15.0.0.

uri *version_uri*

Specify the version URI.

Must be a string in the pattern 'v\d'.

version-list version *version_name*

Specify the 3GPP compliance versions to configure. It allows a maximum of two compliance versions to be configured at a time.

mode { active | offline }

Specify the status of configured 3GPP compliance versions. **mode** is an optional configuration. The default value is **active**. If **version-list version** is configured with two versions, then at least one version should be **active**.

Usage Guidelines Use this command to configure the 3GPP N2 service specification version number.

profile compliance service namf-comm

Configures the 3GPP namf-comm specification version number.

Command Modes Exec > Global Configuration (config) > Compliance Profile Configuration (config-compliance-*profile_name*)

Syntax Description **service namf-comm version { full** *full_version* **| spec** *3gpp_spec_version* **| uri** *version_uri* **} | version-list version** *version_name* **{ full** *full_version* **| mode { active | offline } | spec** *3gpp_spec_version* **| uri** *version_uri* **}**

version

Specify the 3GPP compliance version to configure. It allows only one compliance version to be configured at a time.

full *full_version*

Specify the full version in the format *major-version*.*minor-version*.*patch-version*.[alpha-*draft-number*].

Must be a string in the pattern '\d+.\d+.\d+^?(.alpha-\d+)?'.

spec *3gpp_spec_version*

Specify the 3GPP namf-comm specification version number.

Must be one of the following:

- **15.0.0**
- **15.2.0**
- **15.4.0**

Default Value: 15.0.0.

uri *version_uri*

Specify the version URI.

Must be a string in the pattern 'v\d'.

version-list version *version_name*

Specify the 3GPP compliance versions to configure. It allows a maximum of two compliance versions to be configured at a time.

mode { active | offline }

Specify the status of configured 3GPP compliance versions. **mode** is an optional configuration. The default value is **active**. If **version-list version** is configured with two versions, then at least one version should be **active**.

Usage Guidelines Use this command to configure the 3GPP namf-comm specification version number.

profile compliance service nchf-convergedcharging

Configures the 3GPP nchf-convergedcharging service specification version number.

Command Modes Exec > Global Configuration (config) > Compliance Profile Configuration (config-compliance-*profile_name*)

Syntax Description **service nchf-convergedcharging version { full** *full_version* **| spec** *3gpp_spec_version* **| uri** *version_uri* **} | version-list version** *version_name* **{ full** *full_version* **| mode { active | offline } | spec** *3gpp_spec_version* **| uri** *version_uri* **}**

version

Specify the 3GPP compliance version to configure. It allows only one compliance version to be configured at a time.

full *full_version*

Specify the full version in the format *major-version.minor-version.patch-version*.[alpha-*draft-number*].

Must be a string in the pattern '\d+.\d+.\d+^?(.alpha-\d+)?'.

spec *3gpp_spec_version*

Specify the 3GPP nchf-convergedcharging service specification version number.

Must be one of the following:

- **15.0.0**
- **15.1.0**
- **15.2.1**
- **15.3.0.std**
- **15.3.0 custom**
- **15.3.0**
- **15.4.0**
- **16.8.1**
- **17.0.0**

Default Value: 15.0.0.

uri *version_uri*

Specify the version URI.

Must be a string in the pattern 'v\d'.

version-list version *version_name*

Specify the 3GPP compliance versions to configure. It allows a maximum of two compliance versions to be configured at a time.

mode { active | offline }

Specify the status of configured 3GPP compliance versions. **mode** is an optional configuration. The default value is **active**. If **version-list version** is configured with two versions, then at least one version should be **active**.

Usage Guidelines Use this command to configure the 3GPP nchf-convergedcharging service specification version number.

profile compliance service nnrf-disc

Configures the 3GPP nnrf-disc service specification version number.

Command Modes Exec > Global Configuration (config) > Compliance Profile Configuration (config-compliance-*profile_name*)

Syntax Description

```
service nnrf-disc version { full full_version | spec 3gpp_spec_version | uri
version_uri } | version-list version version_name { full full_version | mode {
active | offline } | spec 3gpp_spec_version | uri version_uri }
```

version

Specify the 3GPP compliance version to configure. It allows only one compliance version to be configured at a time.

full *full_version*

Specify the full version in the format *major-version*.*minor-version*.*patch-version*.[alpha-*draft-number*].

Must be a string in the pattern '\d+.\d+.\d+^?(.alpha-\d+)?'.

spec *3gpp_spec_version*

Specify the 3GPP nnrf-disc service specification version number.

Must be one of the following:

- **15.0.0**
- **15.2.0**
- **15.4.0**

Default Value: 15.2.0.

uri *version_uri*

Specify the version URI.

Must be a string in the pattern 'v\d'.

version-list version *version_name*

Specify the 3GPP compliance versions to configure. It allows a maximum of two compliance versions to be configured at a time.

mode { active | offline }

Specify the status of configured 3GPP compliance versions. **mode** is an optional configuration. The default value is **active**. If **version-list version** is configured with two versions, then at least one version should be **active**.

Usage Guidelines Use this command to configure the 3GPP nnrf-disc service specification version number.

profile compliance service nnrf-nfm

Configures the 3GPP nnrf-nfm service specification version number.

Command Modes Exec > Global Configuration (config) > Compliance Profile Configuration (config-compliance-*profile_name*)

Syntax Description **service nnrf-nfm version { full** *full_version* **| spec** *3gpp_spec_version* **| uri** *version_uri* **} | version-list version** *version_name* **{ full** *full_version* **| mode { active | offline } | spec** *3gpp_spec_version* **| uri** *version_uri* **}**

version

Specify the 3GPP compliance version to configure. It allows only one compliance version to be configured at a time.

full *full_version*

Specify the full version in the format *major-version*.*minor-version*.*patch-version*.[alpha-*draft-number*].

Must be a string in the pattern '\d+.\d+.\d+^?(.alpha-\d+)?'.

spec *3gpp_spec_version*

Specify the 3GPP nnrf-nfm service specification version number.

Must be one of the following:

- **15.0.0**
- **15.2.0**
- **15.4.0**

Default Value: 15.2.0.

uri *version_uri*

Specify the version URI.

Must be a string in the pattern 'v\d'.

version-list version *version_name*

Specify the 3GPP compliance versions to configure. It allows a maximum of two compliance versions to be configured at a time.

mode { active | offline }

Specify the status of configured 3GPP compliance versions. **mode** is an optional configuration. The default value is **active**. If **version-list version** is configured with two versions, then at least one version should be **active**.

Usage Guidelines Use this command to configure the 3GPP nnrf-nfm service specification version number.

profile compliance service npcf-smpolicycontrol

Configures the 3GPP npcf-smpolicycontrol service specification version number.

Command Modes Exec > Global Configuration (config) > Compliance Profile Configuration (config-compliance-*profile_name*)

Syntax Description

```
service npcf-smpolicycontrol version { full full_version | spec 3gpp_spec_version
 | uri version_uri } | version-list version version_name { full full_version |
mode { active | offline } | spec 3gpp_spec_version | uri version_uri }
```

version

Specify the 3GPP compliance version to configure. It allows only one compliance version to be configured at a time.

full *full_version*

Specify the full version in the format *major-version*.*minor-version*.*patch-version*.[alpha-*draft-number*].

Must be a string in the pattern '\d+.\d+.\d+^?(.alpha-\d+)?'.

spec *3gpp_spec_version*

Specify the 3GPP npcf-smpolicycontrol service specification version number.

Must be one of the following:

- **15.0.0**
- **15.2.0**
- **15.4.0**
- **16.10.0**
- **17.3.0**

Default Value: 15.2.0.

uri *version_uri*

Specify the version URI.

Must be a string in the pattern 'v\d'.

version-list version *version_name*

Specify the 3GPP compliance versions to configure. It allows a maximum of two compliance versions to be configured at a time.

mode { active | offline }

Specify the status of configured 3GPP compliance versions. **mode** is an optional configuration. The default value is **active**. If **version-list version** is configured with two versions, then at least one version should be **active**.

Usage Guidelines Use this command to configure the 3GPP npcf-smpolicycontrol service specification version number.

profile compliance service nsmf-pdusession

Configures the 3GPP nsmf-pdusession specification version number.

Command Modes Exec > Global Configuration (config) > Compliance Profile Configuration (config-compliance-*profile_name*)

Syntax Description

```
service nsmf-pdusession version { full full_version | spec 3gpp_spec_version |
uri version_uri } | version-list version version_name { full full_version | mode
{ active | offline } | spec 3gpp_spec_version | uri version_uri }
```

version

Specify the 3GPP compliance version to configure. It allows only one compliance version to be configured at a time.

full *full_version*

Specify the full version in the format *major-version.minor-version.patch-version*.[alpha-*draft-number*].

Must be a string in the pattern '\d+.\d+.\d+^?(.alpha-\d+)?'.

spec *3gpp_spec_version*

Specify the 3GPP nsmf-pdusession specification version number.

Must be one of the following:

- **15.0.0**
- **15.2.0**
- **15.4.0**

Default Value: 15.0.0.

uri *version_uri*

Specify the version URI.

Must be a string in the pattern 'v\d'.

version-list version *version_name*

Specify the 3GPP compliance versions to configure. It allows a maximum of two compliance versions to be configured at a time.

mode { active | offline }

Specify the status of configured 3GPP compliance versions. **mode** is an optional configuration. The default value is **active**. If **version-list version** is configured with two versions, then at least one version should be **active**.

Usage Guidelines Use this command to configure the 3GPP nsmf-pdusession specification version number.

profile compliance service nudm-sdm

Configures the 3GPP nudm-sdm service specification version number.

Command Modes Exec > Global Configuration (config) > Compliance Profile Configuration (config-compliance-*profile_name*)

Syntax Description

```
service nudm-sdm version { full full_version | spec 3gpp_spec_version | uri
version_uri } | version-list version version_name { full full_version | mode {
active | offline } | spec 3gpp_spec_version | uri version_uri }
```

version

Specify the 3GPP compliance version to configure. It allows only one compliance version to be configured at a time.

full *full_version*

Specify the full version in the format *major-version*.*minor-version*.*patch-version*.[alpha-*draft-number*].

Must be a string in the pattern '\d+.\d+.\d+^?(.alpha-\d+)?'.

spec *3gpp_spec_version*

Specify the 3GPP nudm-sdm service specification version number.

Must be one of the following:

- **15.1.0**
- **15.2.1**
- **15.4.0**

Default Value: 15.2.1.

uri *version_uri*

Specify the version URI.

Must be a string in the pattern 'v\d'.

version-list version *version_name*

Specify the 3GPP compliance versions to configure. It allows a maximum of two compliance versions to be configured at a time.

mode { active | offline }

Specify the status of configured 3GPP compliance versions. **mode** is an optional configuration. The default value is **active**. If **version-list version** is configured with two versions, then at least one version should be **active**.

Usage Guidelines Use this command to configure the 3GPP nudm-sdm service specification version number.

profile compliance service nudm-uecm

Configures the 3GPP nudm-uecm service specification version number.

Command Modes Exec > Global Configuration (config) > Compliance Profile Configuration (config-compliance-*profile_name*)

Syntax Description

```
service nudm-uecm version { full full_version | spec 3gpp_spec_version | uri
version_uri } | version-list version version_name { full full_version | mode {
active | offline } | spec 3gpp_spec_version | uri version_uri }
```

version

Specify the 3GPP compliance version to configure. It allows only one compliance version to be configured at a time.

full *full_version*

Specify the full version in the format *major-version.minor-version.patch-version*.[alpha-*draft-number*].

Must be a string in the pattern '\d+.\d+.\d+^?(.alpha-\d+)?'.

spec *3gpp_spec_version*

Specify the 3GPP nudm-uecm service specification version number.

Must be one of the following:

- **15.1.0**
- **15.2.1**
- **15.4.0**

Default Value: 15.2.1.

uri *version_uri*

Specify the version URI.

Must be a string in the pattern 'v\d'.

version-list version *version_name*

Specify the 3GPP compliance versions to configure. It allows a maximum of two compliance versions to be configured at a time.

mode { active | offline }

Specify the status of configured 3GPP compliance versions. **mode** is an optional configuration. The default value is **active**. If **version-list version** is configured with two versions, then at least one version should be **active**.

Usage Guidelines Use this command to configure the 3GPP nudm-uecm service specification version number.

profile compliance service threegpp23502

Configures the 3GPP 23.502 Stage-2 5GS specification version number.

Command Modes Exec > Global Configuration (config) > Compliance Profile Configuration (config-compliance-*profile_name*)

Syntax Description **service threegpp23502 version { full** *full_version* **| spec** *3gpp_spec_version* **| uri** *version_uri* **}**

version

Specify the 3GPP compliance version to configure. It allows only one compliance version to be configured at a time.

full *full_version*

Specify the full version in the format *major-version*.*minor-version*.*patch-version*.[alpha-*draft-number*].

Must be a string in the pattern '\d+.\d+.\d+^?(.alpha-\d+)?'.

spec *3gpp_spec_version*

Specify the 3GPP 23.502 Stage-2 5GS specification version number.

Must be one of the following:

- **15.4.0**
- **15.6.0**

Default Value: 15.4.0.

uri *version_uri*

Specify the version URI.

Must be a string in the pattern 'v\d'.

Usage Guidelines Use this command to configure the 3GPP 23.502 Stage-2 5GS specification version number.

profile content-filtering category database

Configures the Content Filtering database parameter.

Command Modes Exec > Global Configuration (config)

Syntax Description **content-filtering category database max-versions** *max_versions*

max-versions *max_versions*

Specify the maximum number of Content-Filtering database versions.

Must be an integer in the range of 1-3.

Usage Guidelines Use this command to configure the Content Filtering database parameter.

profile content-filtering category database directory

Configures the Content Filtering database directory parameter.

Command Modes Exec > Global Configuration (config)

Syntax Description **content-filtering category database directory path** *cf_directory_path*

path *cf_directory_path*

Specify the Content-Filtering directory path.

Must be a string of 1-255 characters.

Usage Guidelines Use this command to configure the Content Filtering database directory parameter.

profile converged-core activated-features

Enables the specific feature in converged core.

Command Modes Exec > Global Configuration (config) > Converged Core (config-converged-core *cc_profile_name*)

Syntax Description **profile converged-core** *cc_profile_name* **activated-features 2g3g | upf-blocklisting [use-alert** *custom_rule_name* **]**

activated-features 2g3g

Specify the 2g3g feature.

activated-features upf-blocklisting

Specify the UPF blocklisting feature.

[use-alert *custom_rule_name*]

Specify the custom rule name for the alerts.

The default value of the Command **[use-alert** *custom_rule_name* **]**, is “upf_inactive”. If the custom rule name is not configured, the system takes “upf_inactive” for blocklisting the UPF.

Note

- Changing the custom rule name during run-time requires the previous rule name to be removed. Configuring the new custom rule name before removing the previous rule name, results in activating both the both the rule names.
- The new alert configuration parameters should be configured with the new rule name in CEE alert configuration (CEE ops-center).

Usage Guidelines Use this CLI to enable the UPF blocking feature on SMF.

profile converged-core session-hold duration

Configures the session hold timer duration to enable the IP reuse feature.

Command Modes Exec > Global Configuration (config) > Converged Core Configuration (config-converged-core-*ccg_profile_name*)

Syntax Description **`session-hold duration`** *`hold_timer`*

session-hold duration *hold_timer*

Specify the session hold duration in seconds. By default this feature is disabled.

hold_timer must be an integer in the range of 30 to 300.

Note SMF does not support dynamic change in configuration of session hold timer for ongoing sessions. Any change in the timer value will be applicable only for new sessions.

SMF allows you to configure the session hold timer both at the converged core profile level and DNN level. When the timer is configured at both levels, the timer value configured in DNN overrides the value in converged core profile.

Use **no session-hold duration** command to disable the IP reuse feature.

Usage Guidelines Use this command to configure the session hold timer. If the user reattaches within the configured session hold timer after session release, SMF allocates the same IP address and session ID to the user session.

profile converged-core supported-features

Enables the supported features for a rolling upgrade and Enhanced PFCP Association Release.

Command Modes Exec > Global Configuration (config) > Converged Core (config-converged-core *cc_profile_name*)

Syntax Description

```
profile converged-core cc_profile_name supported-features [ app-rx-retx-cache
 | app-tx-retx | epfar | rolling-upgrade-all |
rolling-upgrade-enhancement-infra ]
```

supported-features [app-rx-retx-cache | app-tx-retx | rolling-upgrade-all | rolling-upgrade-enhancement-infra]

Specify one of following options to enable the supported features for the rolling upgrade.

- **app-rx-retx-cache**: Enable retransmission cache for inbound messages at application.
- **app-tx-retx**: Enable retransmission for outbound messages at application.
- **rolling-upgrade-all**: Enable the **rolling-upgrade-enhancement-infra**, **app-rx-retx-cache** , and **app-tx-retxrolling** upgrade features.
- **rolling-upgrade-enhancement-infra**: Enable infra level features.

Note By default, the rolling upgrade features are disabled.

supported-features epfar

Specify the **epfar** option to enable the support for Enhanced PFCP Association Release.

Note By default, the epfar feature is disabled.

Usage Guidelines Use this command to enable the supported features for a rolling upgrade and Enhanced PFCP Association Release.

profile diameter-client

Configures Diameter client.

Command Modes Exec > Global Configuration (config)

Syntax Description

```
profile diameter-client diameter_client_name [ dictionary-name { dcca-custom8
 | default | r8-gx-standard } | endpoint | failure-handling-profile |
host-selection | request-timeout ]
```

diameter-client *diameter_client_name*

Specify a Diameter client profile name.

dictionary-name { dcca-custom8 | default | r8-gx-standard }

Specify one of the following dictionaries to be used.

- **dcca-custom8** : This is the standard Gy dictionary.
- **default** : This is the default dictionary.
- **r8-gx-standard** : This is the standard Gx dictionary.

endpoint

Specify the associated diameter endpoint profile.

failure-handling-profile

Specify the associated diameter failure handling profile.

host-selection

Specify the Diameter host selection profile.

request-timeout

Indicate the time out of the request.

profile diameter-endpoint

Specify a Diameter endpoint on the Gx or Gy interface.

Command Modes

Exec > Global Configuration (config)

Syntax Description

profile diameter-endpoint *interface_name* **instance instance-id** *instance_id_value* **internal-vip** *ip_address* **[destination-host-avp** *message_type* **| vsa-support** *vendorId-source* **| max-outstanding** *number_of_messages* **| response-timeout** *response_timeout_value* **| connection-timeout** *connection-timeout_value* **| basemsg retransmission-timeout** *retransmission_timeout_value* **| basemsg retransmissions** *max_retry_value* **| basemsg watchdog-interval** *interval_value* **| dscp [** *dscp_value* **| af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef] | origin realm** *realm_name* **| origin host** *host_name* **address ipv4** *ip_address* **| origin peer** *origin_peer_name* **| realm** *realm_name* **| address ipv4** *ip_address* **| port** *peer_port* **| destination-host-name** *destination_host_name* **| load-balancing-algorithm highest-weight| route-entry host [host-name | *] realm [realm-name | *] peer** *peer_name* **weight** *weight_value* **| route-failure deadtime** *deadtime_value* **result-code** *result_code_value* **threshold** *number* **| route-failure result-code** *result_codes_value* **| route-failure threshold** *threshold_number* **| route-failure recovery-threshold percent** *recovery_threshold_percentage* **| dynamic-route**

expiry-timeout *expiry_timeout_value* **| dynamic-route expiry-timeout | dynamic-origin-state-id** *boolean_value* **| disconnect peer request| busy time** *time_duration*| **do not talk time** *time_interval*| **drain time** *time_interval*| **reboot time** *time_duration*]

profile diameter-endpoint *interface_name*

Specify a Diameter profile for the Gx or Gy interface.

instance instance-id *instance_id_value*

Specify the value of the instance ID.

internal-vip

Internal VIP IP address. This parameter is mandatory

destination-host-avp *message_type*

Specify the type of message in which the destination host AVP is to be encoded.

Note SMF supports *always* and *session-binding* values for the *message_type*.

vsa-support *vendorId-source*

Specify the source of vendor IDs DIABASE to be used for negotiation of Diameter peer capabilities.

Note SMF supports only the *all-from-dictionary* value for the *vendorId-source*.

max-outstanding *number_of_messages*

Specify the maximum number of Diameter messages to be sent to any peer in the profile, while awaiting the responses. The default value is 256. *number_of_messages* must be in the range of 1–4096.

response-timeout *response_timeout_value*

Specify the maximum allowed response time for request messages that the Diameter applications send to the Diameter server. The default value is 60. *response_timeout_value* must be in the range of 1–300.

connection-timeout *connection-timeout_value*

Specify the maximum allowed time for establishing the transport layer connectivity, such as the TCP connection, toward the Diameter server. The default value is 30. *connection-timeout_value* must be in the range of 1–300.

basemsg retransmission-timeout *retransmission_timeout_value*

Specify the timeout value between retransmissions of the base messages, such as Device Watchdog Request (DWR) and Capability Exchange Request (CER), toward the Diameter server. The default value is 30.

retransmission_timeout_value must be in the range of 1–120.

basemsg retransmissions *max_retry_value*

Specify the maximum number of times the base messages must be retransmitted. The default value is 1. *max-retries* must be in the range of 1–10.

basemsg watchdog-interval *interval_value*

Specify the time interval between the two DWR messages that are sent toward the Diameter server. The default value is 30. *interval_value* must be in the range of 6–30.

dscp [*dscp_value*| af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef]

Specify the Differential Services Code Point (DSCP) value in the IP header of the Diameter messages that are sent toward the Diameter server. The default value is **be**. *dscp_value* must be in the range of 0–63. Choose in the following other DSCP values, as required:

- **af**xx: Specify this value for the use of an assured forwarding xx per hop behavior (PHB).
- **be**: Specify this value for the use of best effort forwarding PHB. **be** is the default value.
- **cs**x: Specify this value for the use of class selector x per PHB.
- **ef**: Specify this value for the use of expedited forwarding PHB.

origin realm *realm_name*

Specify the name of the realm for the Diameter endpoint. This parameter is mandatory.

origin host *host_name* address ipv4 *ip_address*

Specify the host name, which is the FQDN of the Diameter endpoint. Specify the IPv4 address, which is the Diameter endpoint Bind IP address for the Diameter client connections.

origin peer *origin_peer_name*

Specify the identifier for a Diameter peer. This parameter is mandatory.

realm *realm_name*

Specify the name of the realm for a peer with the name of the peer. This parameter is mandatory.

address ipv4 *ip_address*

Specify the IP address of the Diameter peer.

port *peer_port*

Specify the port of the Diameter peer. This parameter is mandatory.

destination-host-name *destination_host_name*

Specify the custom destination host name to be used in destination host AVP. This parameter is optional.

load-balancing-algorithm highest-weight

Choose an idle server with the highest weight in failure scenarios. If multiple servers have the same high weight, then the load balancing happens among those servers.

route-entry host [host-name | *] realm [realm-name | *] peer *peer_name* weight *weight_value*

Use this command to configure two static entries, such as a peer in the route table. If you configure an entry with the existing same flag, host, realm, then only the weight is updated with higher of two of them. The **host** and **realm** parameters allow wildcard character values. The **weight** is an optional parameter with the default value as 10. The **peer** is a mandatory parameter.

Note You can configure multiple route entries with the same host and realm but a different peer without being overridden.

route-failure deadtime *deadtime_value* result-code *result_code_value* threshold *number*

Specify the duration in seconds for which the system keeps the route in the **FAILED** status. After the configured duration expires, the system changes the status to **AVAILABLE**. *deadtime_value* must be an integer in the range of 1–86400. The default value is 60.

route-failure result-code *result_codes_value*

Specify the answer messages that are to be considered as failures, in addition to the requests that time out.

Note You can specify up to 16 result codes.

route-failure threshold *threshold_number*

Specify the number of errors that cause the **FAILED** status. The default value is 16.

Note The error counter begins at zero. In a case of a good response, the error counter decrements or increments. This counter does not decrement below zero or increment above the configured threshold number.

route-failure recovery-threshold percent *recovery_threshold_percentage*

Specify the percentage value at which the failure counter is reset when provisionally changing the status from **FAILED** to **AVAILABLE**. For example, a failure counter of 16 caused the **AVAILABLE** status to change to **FAILED** status. After the configured deadtime expires, the status changes to **AVAILABLE**. If *recovery_threshold_percentage* is configured with 75 percent, the failure counter resets to 12, which is 75 percent of 16. The default value is 90.

dynamic-route expiry-timeout *expiry_timeout_value*

Specify the expiration time for dynamic routes that you created after reaching the Diameter destination host. The default value is 86400 secs, which equals one day.

dynamic-origin-state-id *boolean_value*

Specify whether you want to enable or disable the dynamic origin state ID. The default value is true.

disconnect peer request

The Disconnect-Peer-Request (DPR) is sent to a peer to inform its intentions to disconnect the connection from the peer nodes.

busy time *time_duration*

Specify the time duration after which the connection is reattempted to peer. The time duration value must be an integer in the range of 1–300 seconds. The default value is 3 seconds.

do not talk time *time_interval*

Specify the time interval between receiving of DPR by diameter endpoint and sending of DPA response. The time interval value must be the integer in the range of 1–300 seconds. The default value is 3 seconds.

drain time *time_interval*

Specify the time interval between receiving of DPR by diameter endpoint and sending of DPA response. The time interval value must be an integer in the range of 1 to 10 seconds. The default value is 3 seconds.

reboot time *time_duration*

Specify the time duration after which the connection is reattempted to peer. The time duration value must be an integer in the range of 1–300 seconds. The default value is 3 seconds.

profile diameter-host-selection

Configures the data of an individual profile name with algorithm and list of primary and secondary host details.

Command Modes

Exec > Global Configuration (config)

Syntax Description

profile diameter-host-selection *host_selection_name* **algorithm hosts** *hosts_precedence* **[primary host** *host_ip_address* **primary realm** *realm_name* **| secondary host** *host_ip_address* **secondary realm** *realm_name* **]**

profile diameter-host-selection*host_selection_name*

Specify the Diameter host selection profile name.

algorithm

Choose the algorithm to select the host.

Must be one of the following:

- **ipaddr-modulus**
- **msisdn-modulus**
- **round-robin**

hosts *hosts_precedence*

Specify the precedence of the host in the form of index from 1-64

Must be in the range of 1 to 64.

primary host *host_ip_address*

Specify the primary host name.

primary realm *realm_name*

Specify the primary host realm.

secondary host *host_ip_address*

Specify the secondary host name.

secondary realm *realm_name*

Specify the secondary host realm.

profile dnn

Configures DNN profile.

Command Modes

Exec > Global Configuration (config)

Syntax Description

profile dnn *dnn_profile_name* **intershat** *dnn_intershat***[always-on { false | true } | charging-profile** *profile_name* **| dcnr { false | true } | dnn-selection-mode** *dnn_selection_mode* **| dnn** *profile_name* **| emergency { false | true } | mode** *dnn_mode* **| only-nr-capable-ue { false | true } | pcc-ue-rule-precedence-mapping { false | true } | pcf-interaction { false | true } | pcscf-profile** *profile_name* **| ppd-profile** *profile_name* **| presence-reporting { false | true } | qci-qos-profile** *qci_qos_profile* **| qos-profile** *profile_name* **| eventmgmt-policy** *eventmgmt_policy_name* **| suppress-uli-reporting-on-s5 { disable | enable } | upf-selection-policy** *upf_selection_policy* **| userplane-inactivity-timer** *timeout_period* **| virtual-mac** *mac_address* **| wps-profile** *profile_name* **]**
supported-features [inter-plmn-ho nat-binding-update]

always-on { false | true }

Specify to enable or disable Always On PDU session.

Must be one of the following:

- **false**
- **true**

Default Value: false.

charging-characteristics-id *cc_id*

Specify the charging characteristics ID.

Must be an integer in the range of 1-16.

charging-profile *profile_name*

Specify name of the charging profile.

Must be a string.

charging-qbc-profile *profile_name*

Specify name of the charging QBC profile.

Must be a string.

dcnr { false | true }

Specify to enable or disable support for dual connectivity with new radio.

Must be one of the following:

- **false**
- **true**

Default Value: false.

dnn-selection-mode *dnn_selection_mode*

Specify the selection mode for subscription. The default mode is "verified".

Must be one of the following:

- **network-provided**
- **ue-provided**
- **verified**

dnn *dnn_profile_name*

Specify name of the DNN profile.

Must be a string.

emergency { false | true }

Specify whether the DNN is emergency DNN or not.

Must be one of the following:

- **false**
- **true**

Default Value: false.

hsmf-uri *hsmf_uri*

Specify the override hsmfURI.

Must be a string.

mode *dnn_mode*

Specify the DNN mode of operation.

Must be one of the following:

- **offline**: Offline. DNN in offline mode, new sessions are rejected.

only-nr-capable-ue { false | true }

Specify whether to allow only 5G capable UE, and reject calls from non-5G capable UE.

Must be one of the following:

- **false**
- **true**

Default Value: false.

override *profiles*

Specify the list of profiles for local preference.

Must be one of the following:

- **charging-characteristics-id**
- **charging-profile**
- **charging-qbc-profile**

pcc-ue-rule-precedence-mapping { false | true }

Specify whether to map PCC rule precedence to SMF-assigned TFT and auth rule precedence values. If disabled, values sent by PCF are used.

Must be one of the following:

- **false**
- **true**

Default Value: true.

pcf-interaction { false | true }

Specify to enable or disable PCF interaction.

Must be one of the following:

- **false**

- **true**

Default Value: true.

pcscf-profile *profile_name*

Specify the P-CSCF profile association.

Must be a string.

ppd-profile *profile_name*

Specify the Paging-Policy differentition.

Must be a string.

presence-reporting { false | true }

Specify whether to enable or disable presence reporting for this DNN.

Must be one of the following:

- **false**
- **true**

Default Value: false.

qci-qos-profile *qci_qos_profile*

Specify the QCI QoS Profile configuration related to QCI to QoS mapping.

Must be a string.

qos-profile *qos_profile*

Specify the QoS Profile configuration.

Must be a string.

| eventmgmt-policy *eventmgmt_policy_name*

allows configuring priority-based event handling associated to a DNN.

suppress-uli-reporting-on-s5 { disable | enable }

Specify whether to suppress ULI only MBR towards the S5 interface.

Must be one of the following:

- **disable**
- **enable**

upf-selection-policy *upf_selection_policy*

Specify the UPF selection policy specific configuration.

Must be a string.

userplane-inactivity-timer *timeout_period*

Specify the user plane inactivity timer in seconds.

Must be an integer in the range of 0-86400.

Default Value: 0.

virtual-mac *mac_address*

Specify the remote virtual MAC address used to generate interface ID for UE.

Must be a string in the mac-address pattern. For information on the mac-address pattern, see the *Input Pattern Types* chapter.

wps-profile *profile_name*

Specify name of the Wireless Priority Service (WPS) profile.

Must be a string.

supported-features [inter-plmn-ho nat-binding-update]

Configure NAT binding update procedure in SMF.

Usage Guidelines Use this command to configure the DNN profile. The CLI prompt changes to the DNN Profile Configuration mode (config-dnn-<profile_name>).

profile dnn ipam dhcp

Configures DHCP as the IPAM under DNN profile.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description

`profile dnn` *`dnn_profile_name`* `ipam dhcp`

ipam dhcp

Specify the DHCP as IPAM.



Note It is mandatory to have one IP pool to UPF mapping for DHCP based IPAM.

Usage Guidelines Use this command to indicate IPAM as DHCP.

profile dnn accounting

Configures accounting parameters.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **accounting server-group** *radius_server_group_name*

server-group *radius_server_group_name*

Specify name of the RADIUS server group.

Usage Guidelines Use this command to configure the accounting parameters.

profile dnn authentication algorithm

Configures the authentication algorithm.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **authentication algorithm { chap** *chap_preference* **| convert-to-mschap | mschap** *mschap_preference* **| pap** *pap_preference* **| password-use-pco }**

chap *chap_preference*

Specify the Challenge Handshake Authentication Protocol (CHAP) and preference. Lower value means higher preference. To disable, set it to 0.

Must be an integer in the range of 0-3.

Default Value: 0.

convert-to-mschap

Specify conversion of CHAP to MSCHAP when CHAP response length is 49 bytes.

mschap *mschap_preference*

Specify the Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) and preference. Lower value means higher preference. To disable, set it to 0.

Must be an integer in the range of 0-3.

Default Value: 0.

pap *pap_preference*

Specify the Password Authentication Protocol (PAP) and preference. Lower value means higher preference. To disable, set it to 0.

Must be an integer in the range of 0-3.

Default Value: 0.

password-use-pco

Specify to override password with PCO password.

Usage Guidelines Use this command to configure the authentication algorithm.

profile dnn authentication secondary

Configures the secondary authentication method.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **`authentication secondary radius group`** *`radius_server_group_name`*

group *radius_server_group_name*

Specify name of the RADIUS server group.

radius

Specify to use RADIUS as secondary authentication method.

Usage Guidelines Use this command to configure the secondary authentication method.

profile dnn authorization

Configures the authorization method.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **`authorization local rat-type`** *`rat_types`*

local

Specify to use local policy configuration.

rat-type *rat_types*

Specify the RAT types.

Must be one of the following:

- **eutra**
- **nr**
- **wlan**

Usage Guidelines Use this command to configure the authorization method.

profile dnn dnn

Configures a Virtual DNN profile under a DNN profile and NF user list.

Command Modes Exec > Global Configuration (config)

Syntax Description **dnn** *profile_name*

Usage Guidelines Use this command to configure a DNN profile that is used to map a UE-requested DNN to a Virtual DNN. The SMF sends "Mapped" DNNs for configured network functions and "UE-requested" DNNs for other network functions. The UE-requested DNN is always sent on the N1 interface.

profile dnn dnn nw-fu-conf

Configures network function parameters.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **dnn** *dnn_name* **network-function-list** *nf_list*

dnn *dnn_name*

Specify name of the DNN.

Must be a string.

network-function-list *nf_list*

Specify the list of network functions that the selected DNN profile will be sent. The list of network functions supported are CHF, OCS, PCF, PCRF, RADIUS and UPF.

Must be a string.

Usage Guidelines Configures a Virtual DNN profile under a DNN profile and NF user list. Use this command to configure the network function parameters.

profile dnn dnn rmgr-conf

Configures the RMGR parameters.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **dnn rmgr** *rmgr_nf*

rmgr *rmgr_nf*

Specify the RMGR Network Function.

Must be a string.

Usage Guidelines Use this command to configure the RMGR parameters.

profile dnn dns primary

Configures the primary DNS server details.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **dns primary { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **}**

ipv4 ***ipv4_address***

Specify the primary DNS server's IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 ***ipv6_address***

Specify the primary DNS server's IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure the primary DNS server details.

profile dnn dns secondary

Configures the secondary DNS server details.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **dns secondary { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **}**

ipv4 ***ipv4_address***

Specify the secondary DNS server's IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 ***ipv6_address***

Specify the secondary DNS server's IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure the secondary DNS server details.

profile dnn ims mark

Configures marking QCI value as IMS media.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **ims mark qci** *qos_class_id*

qci *qos_class_id*

Specify the standard QoS Class Identifiers.

Must be an integer from the following: 1-9, 65, 66, 69, 70, 80, 82, 83, 128-254.

You can configure a maximum of four elements with this keyword.

Usage Guidelines Use this command to configure marking QCI value as IMS media.

profile dnn ipv6-prefix-delegation

Configures the prefix delegation feature for the DNN.

Command Modes Exec > Global Configuration (config)> DNN Profile Configuration (config-dnn-profile_name)

Syntax Description **ipv6-prefix-delegation prefix length** *prefix_length* **dnn prefix-delegation** *vdnn*

prefix length *prefix_length*

Specify the length of the IPv6 prefix being delegated. The supported range of prefix length is from 48 to 62.

When UPF sends Session Report for DIPR without requested PD-Prefix-Length, SMF will use this value as the prefix length.

dnn prefix-delegation *vdnn*

Configure the Prefix Delegation (PD) for a virtual Dual-Stack Network Node (vDNN).

This configuration is mandatory because separate IP address pools are required for the delegated prefixes.

Usage Guidelines Use this command to configure the prefix delegation feature for the DNN.

profile dnn max-upf-sessions

Configures maximum UPF sessions at DNN level.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **profile dnn** *dnn_profile_name***max-upf-sessions** *max_upf_sessions_count*

profile dnn *dnn_profile_name*

Configures DNN profile.

max-upf-sessions *max_upf_sessions_count*

Configures maximum supported session per vDnn per UPF on SMF.

Usage Guidelines Use this command to configure maximum UPF sessions on a DNN level.

profile dnn network-element-profiles

Configures network element profiles.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **`network-element-profiles { amf | chf | pcf | pcrf | ocs | sepp | udm }`***`profile_name`*

amf *profile_name*

Specify name of the AMF network element profile. Changing the current profile name may impact existing calls. Requires DNN in offline mode.

Must be a string.

chf *profile_name*

Specify name of the CHF network element profile. Changing the current profile name may impact existing calls. Requires DNN in offline mode.

Must be a string.

pcf *profile_name*

Specify name of the PCF network element profile. Changing the current profile name may impact existing calls. Requires DNN in offline mode.

Must be a string.

pcrf *profile_name*

Specify name of the PCRF network element profile to enable Gx interface.

Must be a string.

ocs *profile_name*

Specify name of the OCS network element profile to enable Gy interface.

Must be a string.

sepp *profile_name*

Specify name of the SEPP network element profile.

Must be a string.

udm *profile_name*

Specify name of the UDM network element profile. Changing the current profile name may impact existing calls. Requires DNN in offline mode.

Must be a string.

Usage Guidelines Use this command to configure network element profiles. Changing the current profile name may impact existing calls. Requires DNN in offline mode.

profile dnn nexthop-forwarding-address

Configures the Redirect Service/NextHop IP address.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **`nexthop-forwarding-address { ipv4`** *`ipv4_address`* **`| ipv6`** *`ipv6_address`* **`}`**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure the Redirect Service/NextHop IP address.

profile dnn nssai

Configures the default NSSAI configuration.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **`nssai { [ sd`** *`slice_differentiator`* **`] [ sst`** *`slice_service_type`* **`] }`**

sd *slice_differentiator*

Specify the S-NSSAI Slice Differentiator (SD).

Must be a string in the hex-string6 pattern. For information on the hex-string6 pattern, see the *Input Pattern Types* chapter.

sst *slice_service_type*

Specify the S-NSSAI Slice/Service Type (SST).

Must be an integer in the range of 0-255.

Usage Guidelines Use this command to configure the default NSSAI configuration.

profile dnn outbound

Configures DNN host password for PPP session authentication.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **outbound password** *dnn_host_password*

password *dnn_host_password*

Specify the DNN host password.

Must be a string.

Usage Guidelines Use this command to configure designating the DNN host password for PPP session authentication.

profile dnn primary-plmn

Configures the primary PLMN configuration.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **primary-plmn { [mcc** *mobile_country_code* **] [mnc** *mobile_network_code* **] }**

mcc *mobile_country_code*

Specify the 3-digit Mobile Country Code.

mnc *mobile_network_code*

Specify the 2- or 3-digit Mobile Country Network.

Usage Guidelines Use this command to configure the primary PLMN configuration.

profile dnn session-hold duration

Configures the session hold timer duration to enable the IP reuse feature.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*dnn_profile_name*)

Syntax Description **session-hold duration** *hold_timer*

session-hold duration *hold_timer*

Specify the session hold duration in seconds. By default this feature is disabled.

hold_timer must be an integer in the range of 30 to 300.

Note SMF does not support dynamic change in configuration of session hold timer for ongoing sessions. Any change in the timer value will be applicable only for new sessions.

SMF allows you to configure the session hold timer both at the DNN profile level and converged core level. When the timer is configured at both levels, the timer value configured in DNN overrides the value in converged core profile.

Use **no session-hold duration** command to disable the IP reuse feature.

Usage Guidelines Use this command to configure the session hold timer. If the user reattaches within the configured session hold timer after session release, SMF allocates the same IP address and session ID to the user session.

profile dnn session type

Configures the PDU session type.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **`session type`** *`default_session_type`* **`[ allowed`** *`allowed_session_type`* **`]`**

allowed *allowed_session_type*

Specify the SMF allowed session types. Up to two allowed session types can be configured in addition to the default session type. The same session type cannot be configured both as allowed and default.

Must be one of the following:

- **IPV4**
- **IPV4V6**
- **IPV6**

You can configure a maximum of two elements with this keyword.

type *default_session_type*

Specify the default session type.

Must be one of the following:

- **IPV4**
- **IPV4V6**
- **IPV6**

Usage Guidelines Use this command to configure the PDU session type.

profile dnn skip-n10-registration

Ignores the UE registration messages towards UDM during the PDU setup and Wi-Fi attach procedures.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **`profile dnn`** *`dnn_profile_name`* **`{ skip-n10-registration rat-type [ NR | WIFI | ALL ] }`**

skip-n10-registration rat-type [NR | WIFI | ALL]

Specify one of the following RAT types to ignore the UDM registration.

- **NR**
- **WIFI**
- **ALL**



Note When you configure this CLI command, the SMF ignores the UDM registration during session creation in the 5G and Wi-Fi network. The handover between 5G and Wi-Fi fails because ePDG doesn't find the target SMF that was handling the session. If the UE registration fails during 5G or Wi-Fi attach and if the UDM failure handling template (FHT) is configured as continue or ignore, then SMF reattempts the registration during Wi-Fi-to 5G and 5G to Wi-Fi handovers.

Usage Guidelines Use this command to ignore the UDM registration messages during the PDU setup and Wi-Fi attach procedures.

profile dnn subscription

Allows you to choose and change a subscription method. This CLI command allows you to delete a configured subscription method.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **`subscription [ local | notify-immediate ] rat-type [ nr | eutra | wlan ]`**

subscription [local | notify-immediate]

Specify one of the following subscription options.

- **local**—Uses Local Policy for Subscription.
- **notify-immediate**—Skips Subscription Fetch and Continue with Subscribe to Notify with ImmediateReport.

rat-type [nr | eutra | wlan]

Specify one of the following RAT types.

- **nr**
- **eutra**
- **wlan**

Usage Guidelines Use this command to choose and change a subscription method, and delete a configured subscription method.

profile dnn ssc-mode

Configures Session and Service Continuity (SSC) Mode parameters.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **ssc-mode** *default_ssc_mode* **[allowed** *allowed_ssc_mode* **]**

allowed *allowed_ssc_mode*

Specify the allowed SSC Modes. Up to two allowed modes can be configured in addition to the default SSC mode. The same SSC mode cannot be configured both as allowed and default.

Must be one of the following:

- **1**
- **2**
- **3**

You can configure a maximum of two elements with this keyword.

ssc-mode *default_ssc_mode*

Specify the default SSC mode.

Must be one of the following:

- **1**
- **2**
- **3**

Usage Guidelines Use this command to configure SSC mode parameters.

profile dnn timeout

Configures session time-to-live (TTL) configuration.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **timeout { [absolute** *max_duration* **] [backoff** *backoff_timer_duration* **] [cp-idle** *cp_idle_duration* **] [default-flow-only** *default_flow_only_duration* **] [jitter** *jitter_duration* **] [setup** *setup_duration* **] [up-idle** *up_idle_duration* **] }**

absolute *max_session_duration*

Specify the maximum duration of the session in seconds, before the system automatically terminates the session. Value 0 indicates the function is disabled.

Must be an integer in the range of 0-2147483647.

Default Value: 0.

backoff *backoff_timer_duration*

Specify the maximum duration in seconds for backoff timer during IP Exhaustion and N4 Path Failure cases.

Must be an integer in the range of 0-576000.

Default Value: 0.

cp-idle *cp_idle_duration*

Specify the maximum duration after a 5G session has moved to idle (controlplane) state, before the system automatically terminates it. Value 0 indicates the function is disabled.

Must be an integer in the range of 0-2147483647.

Default Value: 0.

default-flow-only *default_flow_only_duration*

Specify the maximum allowed duration for a PDU/PDN session to be in idle state, after which the system automatically terminates it. Value 0 indicates the function is disabled.

Must be an integer in the range of 0-604800000.

Default Value: 0.

jitter *jitter_value*

Specify the jitter value in seconds.

Must be an integer in the range of 0-1000.

Default Value: 0.

setup *max_setup_duration*

Specify the maximum setup time duration in milliseconds, after which the system automatically aborts the request.

Must be an integer in the range of 5000-60000.

Default Value: 10000.

up-idle *up_idle_duration*

Specify the maximum duration after a 5G session has moved to idle (userplane) state, before the system automatically terminates it. Value 0 indicates the function is disabled.

Must be an integer in the range of 0-2147483647.

Default Value: 0.

Usage Guidelines Use this command to configure session time-to-live (TTL) configuration.

profile dnn timeout bearer-inactivity

Checks for low activity for a bearer.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **`bearer-inactivity [ exclude-default-bearer { false | true } ]`**

exclude-default-bearer { false | true }

Specify whether to exclude default bearer from the Bearer Inactivity feature.

Must be one of the following:

- **false**
- **true**

Usage Guidelines Use this command to configure checking for low activity for a bearer.

profile dnn timeout bearer-inactivity gbr

Checks for low activity for a GBR bearer.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **`gbr duration`** *`bearer_inactivity_timer`*

duration *bearer_inactivity_timer*

Specify the bearer inactivity timeout period in seconds.

Must be an integer in the range of 300-2592000.

Usage Guidelines Use this command to configure checking for low activity for a GBR bearer.

profile dnn timeout bearer-inactivity gbr volume

Configures data traffic threshold values for a bearer.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **volume { [downlink** *downlink_data_traffic* **] [total** *total_data_traffic* **] [uplink** *uplink_data_traffic* **] }**

downlink *downlink_data_traffic*

Specify the downlink data traffic for a bearer in bytes.

Must be an integer in the range of 1-4294967295.

total *total_data_traffic*

Specify the total uplink and downlink data traffic for a bearer in bytes.

Must be an integer in the range of 1-4294967295.

uplink *uplink_data_traffic*

Specify the uplink data traffic for a bearer in bytes.

Must be an integer in the range of 1-4294967295.

Usage Guidelines Use this command to configure the data traffic threshold values for a bearer.

profile dnn timeout bearer-inactivity non-gbr

Checks for low activity for a non-GBR bearer.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **gbr duration** *bearer_inactivity_timer*

duration *bearer_inactivity_timer*

Specify the bearer inactivity timeout period in seconds.

Must be an integer in the range of 300-2592000.

Usage Guidelines Use this command to configure checking for low activity for a non-GBR bearer.

profile dnn timeout bearer-inactivity non-gbr volume

Configures data traffic threshold values for a bearer.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **volume { [downlink** *downlink_data_traffic* **] [total** *total_data_traffic* **] [uplink** *uplink_data_traffic* **] }**

downlink *downlink_data_traffic*

Specify the downlink data traffic for a bearer in bytes.

Must be an integer in the range of 1-4294967295.

total *total_data_traffic*

Specify the total uplink and downlink data traffic for a bearer in bytes.

Must be an integer in the range of 1-4294967295.

uplink *uplink_data_traffic*

Specify the uplink data traffic for a bearer in bytes.

Must be an integer in the range of 1-4294967295.

Usage Guidelines Use this command to configure the data traffic threshold values for a bearer.

profile dnn upf

Configures the UPF APN profile.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **`upf apn`** *`apn_name`*

apn *apn_name*

Specify name of the APN.

Must be a string of 1-63 characters.

Usage Guidelines Use this command to configure the UPF APN profile.

profile dnn upcp status

Configures the User Plane Confidentiality Protection support on SMF and its parameters.

Command Modes Exec > Global Configuration (config) > DNN Profile Configuration (config-dnn-*profile_name*)

Syntax Description **`[ no ] upcp status { required | preferred | not-needed }`**

upcp status { required | preferred | not-needed }

Configures the UPCP status. There are three options in this command:

- Required
- Preferred
- Not needed

[no]

This is an optional command. It removes the local configuration for UPCP status.

Usage Guidelines Use this command to configure the UPCP locally on SMF.

profile dns-proxy

Configures DNS proxy profile parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile dns-proxy [cache-ttl** *ttl* **| query-type** *query_type* **| randomize-answers | round-robin-answers | timeout** *dns_timeout* **]**

cache-ttl *ttl*

Specify the TTL value of DNS responses in cache, in seconds.

Must be an integer in the range of 60-86400.

query-type *query_type*

Specify the DNS query type.

Must be one of the following:

- **ipv4-ipv6**
- **ipv4**
- **ipv6**

Default Value: ipv4.

randomize-answers

Specify to enable randomizing address fetch.

round-robin-answers

Specify to enable round-robin address fetch.

timeout *dns_timeout*

Specify the DNS timeout.

Must be an integer in the range of 200-10000.

Default Value: 500.

Usage Guidelines Use this command to enable and configure DNS proxy parameters.

profile dns-proxy servers

Configures DNS server parameters.

Command Modes

Exec > Global Configuration (config) > DNS Proxy Configuration (config-dns-proxy)

Syntax Description

servers *dns_server_name* **[ip** *dns_server_ip_address* **| port** *dns_server_port_number* **| priority** *dns_server_priority* **| protocol** *dns_server_protocol* **]**

ip *dns_server_ip_address*

Specify the IP address of the DNS server.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *dns_server_port_number*

Specify the port number of the DNS server.

Must be an integer in the range of 1-65535.

priority *dns_server_priority*

Specify the priority for the DNS server.

Must be an integer in the range of 1-100.

protocol *dns_server_protocol*

Specify the protocol type for the DNS server.

Must be one of the following:

- **tcp**
- **udp**

Default Value: tcp.

servers *dns_server_name*

Specify the name of the DNS server.

Must be a string.

Usage Guidelines

Use this command to configure the DNS server parameters.

profile ecgi-group

Configures ECGI group profile parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile ecgi-group** *group_name*

ecgi-group *group_name*

Specify name of the ECGI group.

Must be a string.

Usage Guidelines Use this command to configure ECGI group profile parameters.

profile ecgi-group ecgis

Configures the list of MCC, MNC, TAC, and ECGI groups.

Command Modes Exec > Global Configuration (config) > ECGI Group Configuration (config-ecgi-group-*profile_name*)

Syntax Description **mcc** *mobile_country_code* **mnc** *mobile_network_code*

mcc *mobile_country_code*

Specify the Mobile Country Code (MCC).

Must be a string in the three-digit pattern. For information on the three-digit pattern, see the *Input Pattern Types* chapter.

mnc *mobile_network_code*

Specify the Mobile Network Code (MNC).

Must be a string in the two-or-three-digit pattern. For information on the two-or-three-digit pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure the list of MCC, MNC, TAC, and ECGI groups.

You can configure a maximum of 16 elements with this command.

profile ecgi-group ecgis ecgi

Configures ECGI group parameters.

Command Modes Exec > Global Configuration (config) > ECGI Group Configuration (config-ecgi-group-*profile_name*) > ECGI Group MCC/MNC Configuration (config-ecgi-group-*mcc_mnc*)

Syntax Description **ecgi list** *ecgi_values*

list *ecgi_values*

Specify the list of ECGI values - 7 digit hex string Eutra Cell ID. For example, A12345f.

Must be a string in the hex-stringecgi pattern. For information on the hex-stringecgi pattern, see the *Input Pattern Types* chapter.

You can configure a maximum of 64 elements with this keyword.

Usage Guidelines Use this command to configure ECGI group parameters.

profile ecgi-group ecgis ecgi range

Configures ECGI range.

Command Modes Exec > Global Configuration (config) > ECGI Group Configuration (config-ecgi-group-*profile_name*) > ECGI Group MCC/MNC Configuration (config-ecgi-group-*mcc_mnc*)

Syntax Description **ecgi range start** *ecgi_range_start* **end** *ecgi_range_end*

end *ecgi_range_end*

Specify the ECGI range end value.

Must be a string in the hex-stringecgi pattern. For information on the hex-stringecgi pattern, see the *Input Pattern Types* chapter.

start *ecgi_range_start*

Specify the ECGI range start value.

Must be a string in the hex-stringecgi pattern. For information on the hex-stringecgi pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure an ECGI range.

You can configure a maximum of 64 elements with this command.

profile emergency-profile

Configures emergency profile.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile emergency-profile** *emergency_profile_name* **[udm-profile** *udm_profile_name* **]**

emergency-profile *emergency_profile_name*

Specify name of the emergency profile.

Must be a string.

udm-profile *udm_profile_name*

Specify name of the UDM profile.

Must be a string.

Usage Guidelines Use this command to configure emergency profiles.

profile failure-handling

Configures the Failure Handling profile.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile failure-handling** *profile_name*

failure-handling *profile_name*

Specify name of the Failure Handling profile.

Must be a string.

Usage Guidelines Use this command to configure the Failure Handling profile.

profile failure-handling interface diameter

Configures a failure handling profile.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile failure-handling** *failure_handling_profile_name* **interface diameter message** *message_type* **failure-type [any | local-error | result-code {** *result-code-value | result-code-range-start-value | result-code-range-end-value | comma-separated-result-code-value-or-range* **]retry** *count* **action [continue** *action_options* **| terminate** *terminate_options* **]**

profile failure-handling *failure_handling_profile_name*

Specify a name for the failure handling profile

Default Value: false.

interface diameter

Specify the failure handling profile for the Diameter interface.

message *message_type*

Specify name of the charging profile.

Must be one of the following:

- **any**
- **credit-control-initial**
- **credit-control-terminate**
- **credit-control-update**

failure-type [any | local-error | result-code { *result-code-value | result-code-range-start-value | result-code-range-end-value | comma-separated-result-code-value-or-range*]

Specify a Diameter failure type for which an action needs to be taken. Choose a failure type value from the available options. This

Must be one of the following:

- **any**
- **local-error**
- **result-code**

retry *count*

Specify the number of alternate peers to retry on receiving a failure response.

Default Value: zero.

action continue *continue_option*

Choose an action value as continue. Choose sub-actions of the selected action from the available options, as required

Must be one of the following:

- **discard-traffic**
- **local-fallback**
- **retry-server-on-event**
- **send-ccrt-on-call-termination**

action terminate *terminate_option*

Choose an action value as terminate. Choose sub-actions of the selected action from the available options, as required

Must be one of the following:

- **with-term-request**
- **without-term-request**

profile failure-handling interface gtpc message

Configures GTPC failure-handling template message types.

Command Modes Exec > Global Configuration (config) > Failure Handling Profile Configuration (config-failure-handling-*profile_name*)

Syntax Description **`interface gtpc message`** *`gtpc_message_type`*

message *gtpc_message_type*

Specify the GTPC message type.

Must be one of the following:

- **S5S8CreateBearerReq**
- **S5S8DeleteBearerReq**
- **S5S8UpdateBearerReq**

Usage Guidelines Use this command to configure GTPC failure-handling template message types.

profile failure-handling interface gtpc message cause-code-type cause-code

Configures GTPC interface cause code types.

Command Modes Exec > Global Configuration (config) > Failure Handling Profile Configuration (config-failure-handling-*profile_name*) > GTPC Message Configuration (config-message-*gtpc_message_type*)

Syntax Description **`cause-code`** *`gtpc_cause_code_type`*

cause-code *gtpc_cause_code_type*

Specify the GTPC cause code type.

Must be one of the following:

- **temp-fail**

Usage Guidelines Use this command to configure GTPC interface cause code types.

profile failure-handling interface gtpc message cause-code-type cause-code action

Configures the action type for the cause.

Command Modes Exec > Global Configuration (config) > Failure Handling Profile Configuration (config-failure-handling-*profile_name*) > GTPC Message Configuration (config-message-*gtpc_message_type*) > Cause Code Configuration (config-cause-code-*cause_code*)

Syntax Description **action** *action_type* **[timeout** *retry_interval* **| max-retry** *max_retry* **]**

action *action_type*

Specify the action type for the cause.

Must be one of the following:

- **clear**
- **retry**
- **terminate**

max-retry *max_retry*

Specify the maximum retry count.

Must be an integer in the range of 0-5.

Default Value: 1.

timeout *retry_interval*

Specify the retry interval in milliseconds.

Must be an integer in the range of 1000-5000.

Default Value: 1000.

Usage Guidelines Use this command to configure the action type for the cause.

profile failure-handling interface n11

Configures the N11 interface - SMF/PGW-C timer for reattempting bearer creation/updation.

Command Modes Exec > Global Configuration (config) > Failure Handling Profile Configuration (config-failure-handling-*profile_name*)

Syntax Description **interface n11**

Usage Guidelines Use this command to configure the N11 interface - SMF/PGW-C timer for reattempting bearer creation/updation.

profile failure-handling interface n11 message

Configures N11 message types.

Command Modes Exec > Global Configuration (config) > Failure Handling Profile Configuration (config-failure-handling-*profile_name*) > N11 Interface Configuration (config-n11)

Syntax Description **message** *message_type*

message *message_type*

Specify the N11 message type.

Must be one of the following:

- **n1n2transfer**

Usage Guidelines Use this command to configure n11 message types.

profile failure-handling interface n11 message cause-code-value cause-code

Configures the N11 interface cause code types.

Command Modes Exec > Global Configuration (config) > Failure Handling Profile Configuration (config-failure-handling-*profile_name*) > N11 Interface Configuration (config-n11) > n1n2transfer Message Configuration (config-message-n1n2transfer)

Syntax Description **cause-code** *n11_cause_code_type*

cause-code *n11_cause_code_type*

Specify the N11 interface cause code type.

Must be one of the following:

- **temp-reject-handover**
- **temp-reject-register**

Usage Guidelines Use this command to configure the N11 interface cause code types.

profile failure-handling interface n11 message cause-code-value cause-code action

Configures the action type for the cause.

Command Modes Exec > Global Configuration (config) > Failure Handling Profile Configuration (config-failure-handling-*profile_name*) > N11 Interface Configuration (config-n11) > n1n2transfer Message Configuration (config-message-n1n2transfer) > Cause Code Configuration (config-cause-code-temp-*cause_code*)

Syntax Description **action** *action_type* **[timeout** *retry_interval* **| max-retry** *max_retry* **]**

action *action_type*

Specify the action type for the cause.

Must be one of the following:

- **clear**
- **retry**
- **terminate**

max-retry *max_retry*

Specify the maximum retry count.

Must be an integer in the range of 1-5.

Default Value: 1.

timeout *retry_interval*

Specify the retry interval in milliseconds.

Must be an integer in the range of 100-5000.

Default Value: 300.

Usage Guidelines Use this command to configure the action type for the cause.

profile failure-handling interface pfcp

Configures PFCP Failure Handling template.

Command Modes Exec > Global Configuration (config) > Failure Handling Profile Configuration (config-failure-handling-*profile_name*)

Syntax Description **interface pfcp**

Usage Guidelines Use this command to configure PFCP Failure Handling template.

profile failure-handling interface pfcp message

Configures PFCP message types.

Command Modes Exec > Global Configuration (config) > Failure Handling Profile Configuration (config-failure-handling-*profile_name*) > PFCP Interface Configuration (config-pfcp)

Syntax Description **message** *pfcp_message_type*

message *pfcp_message_type*

Specify the PFCP message type.

Must be one of the following:

- **N4SessionEstablishmentReq**
- **N4SessionModificationReq**
- **N4SessionReportReq**

Usage Guidelines Use this command to configure PFCP message types.

profile failure-handling interface pfcp message cause-code-type-est cause-code

Configures PFCP interface cause code types.

Command Modes Exec > Global Configuration (config) > Failure Handling Profile Configuration (config-failure-handling-*profile_name*) > PFCP Interface Configuration (config-pfcp) > PFCP Message Configuration (config-message-*message_type*)

Syntax Description **cause-code** *cause_code_type*

cause-code *cause_code_type*

Specify the cause code type.

Must be a string.

-Or-

Must be one of the following:

- **no-resource-available**
- **no-response-received**
- **pfcp-entity-in-congestion**
- **reject**
- **service-not-supported**
- **system-failure**
- **peer-overload-reduction**

Usage Guidelines Use this command to configure PFCP interface cause code types.

profile failure-handling interface pfcp message cause-code-type-est cause-code action

Configures the action type for the cause.

Command Modes

Exec > Global Configuration

Syntax Description

action *action_type* **[timeout** *retry_interval* **| max-retry** *max_retry_count* **]**

action *action_type*

Specify the action type for the cause.

Must be one of the following:

- **retry-terminate**
- **terminate**

max-retry *max_retry_count*

Specify the maximum retry count for the retry-terminate action.

Must be an integer in the range of 0-5.

Default Value: 1.

Usage Guidelines

Use this command to configure the action type for the cause.

profile failure-handling interface pfcp message cause-code-type-mod cause-code

Configures PFCP interface cause code types.

Command Modes

Exec > Global Configuration (config) > Failure Handling Profile Configuration (config-failure-handling-*profile_name*) > PFCP Interface Configuration (config-pfcp) > PFCP Message Configuration (config-message-*message_type*)

Syntax Description

cause-code-type-mod cause-code *pfcp_cause_code_type*

cause-code *pfcp_cause_code_type*

Specify the PFCP cause code type.

Must be a string.

-Or-

Must be one of the following:

- **mandatory-ie-incorrect**

- **no-resource-available**
- **no-response-received**
- **pfcp-entity-in-congestion**
- **reject**
- **session-ctx-not-found**
- **peer-overload-reduction**

Usage Guidelines Use this command to configure the PFCP cause code type.

profile failure-handling interface pfcp message cause-code-type-mod cause-code action

Configures the action type for the cause.

Command Modes Exec > Global Configuration

Syntax Description **action** *action_type* **condition** *condition*

action *action_type*

Specify the action type for the cause.

Must be one of the following:

- **terminate**

condition *condition*

Specify the condition.

Must be one of the following:

- **handover-cancel**
- **handover-execution**
- **handover-preparation**
- **idft**
- **modify**

Usage Guidelines Use this command to configure the action type for the cause.

profile failure-handling interface pfcp message cause-code-type-sessreport cause-code

Configures the PFCP interface cause code types.

Command Modes Exec > Global Configuration

Syntax Description **cause-code-type-sessreport cause-code** *cause_id*

cause-code *cause_id*

Specify the cause ID or a range of cause IDs separated by either hyphhen (-) or comma (,) or both.

Must be a string.

Usage Guidelines Use this command to configure the PFCP interface cause-code types.

profile failure-handling interface pfcp message cause-code-type-sessreport cause-code action

Configures the action type for the cause.

Command Modes Exec > Global Configuration

Syntax Description **action** *action_type*

action *action_type*

Specify the action type for the cause.

Must be one of the following:

- **ignore**
- **terminate**

Usage Guidelines Use this command to configure the action type for the cause.

profile failure-handling interface sxa message

Configures Sxa message types.

Command Modes Exec > Global Configuration

Syntax Description **sxa message** *sxa_message_type*

message *sxa_message_type*

Specify the Sxa message type.

Must be one of the following:

- **SessionEstablishmentReq**

Usage Guidelines Use this command to configure Sxa message types.

profile failure-handling interface sxa message cause-code-type-est cause-code

Configures Sxa interface cause code types.

Command Modes Exec > Global Configuration

Syntax Description **cause-code** *sxa_cause_code_type*

cause-code *sxa_cause_code_type*

Specify the Sxa interface cause code type, or range of cause codes separated by either hyphen (-) or comma (,) or both.

Must be a string.

-Or-

Must be one of the following:

- **no-resource-available**
- **no-response-received**
- **pfcp-entity-in-congestion**
- **reject**
- **service-not-supported**
- **system-failure**

Usage Guidelines Use this command to configure Sxa interface cause code types.

profile failure-handling interface sxa message cause-code-type-est cause-code action

Configures the action type for the cause.

Command Modes Exec > Global Configuration

Syntax Description **action** *action_type* **[timeout** *retry_interval* **| max-retry** *max_retry_count* **]**

action *action_type*

Specify the action type for the cause.

Must be one of the following:

- **retry-terminate**
- **terminate**

max-retry *max_retry_count*

Specify the maximum retry count for the retry-terminate action.

Must be an integer in the range of 0-5.

Default Value: 1.

Usage Guidelines Use this command to configure the action type for the cause.

profile gtpp-profile gtpp

Configures a GTPP profile.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile gtpp-profile** *profile_name* **gtpp [dictionary| ignore** *ignore_value* **instance-id [charging-agent address** *IPv4_adress* **port** *UDP_port***server{ cgf address** *IPv4_adress* **max-cdrs** *max_cdrs* **{ node-alive** *Enable | Disable* **} }port** *UDP_port* **priority** *priority* **deadtime** *time_interval* **echo-interval** *echo_interval* **timeout** *timeout_val* **max-retry** *max_retry* **max-pdu-size** *max_pdu_size* **wait-time** *time_interval* **}| local-storage | mode[localstreaming-parallel]| cgf-server-redundancy-support]**

profile gtpp-profile *profile_name* gtpp

Specify a profile name for GTPP.

dictionary

Specify a dictionary for ASN.1 based encoding of a CDR.

ignore *ignore_value*

Specify the configuration to ignore the echo-rc-change. This CLI control option provides a flexibility to detect a CGF path failure due to a change in the echo response RC.

instance-id [charging-agent address *IPv4_adress* port *UDP_port*server{ cgf address *IPv4_adress* max-cdrs *max_cdrs*{ node-alive *Enable | Disable* }}port *UDP_port* priority *priority* deadtime *time_interval* echo-interval

echo_interval **timeout** ***timeout_val*** **max-retry** ***max_retry*** **max-pdu-size** ***max_pdu_size*** **wait-time** ***time_interval*** **}]**

Specify the instance ID of a GR instance.

- **charging-agent**: Configures the charging agent.
  - **address***IPv4_address*: Specify the IP address of the interface configured within the endpoint that is used to transmit CDR records to the CGF.
  - **port**: Specify the UDP port.



Note The Charging agent IP address and port configured in GTPP profiles should also be configured in the endpoint gtpprime under the Gz interface. The Runtime configuration update of the Charging agent IP address and port is not recommended. Ensure to add new profile with new Charging agent IP address and port.

- **server**: Configure server details.
  - **cgf**: Configure the CGF server with the following parameters.
    - **address** *IPv4_address*: Enter the IPv4 address of CGF server, using dotted-decimal notation range.
    - **max**: Configures maximum number of unacknowledged CDRs for a CGF. Must be an integer ranging from 1 to 2000.



Note The runtime configuration change of **max** is not recommended. Follow the Method of procedure:

1. Delete the **cgf** having old **max** and then commit the change.
2. Add the **cgf** again with a new **max** value.

    - **node-alive Enable | Disable** : Enables or disables sending Node Alive Request to a GTPP Server (such as CGF).
    - **port**: Specify which port that the CGF is using.
    - **priority**: Specify the relative priority of this server when system is selecting which CGF server to use.

  - **deadtime**: Configure the deadtime in seconds. Must be an integer ranging from 1 to 65535. Default value is 120.
  - **max-cdrs**: Designate the maximum number of CDRs in a GTPP message. Must be an integer ranging from 1 to 255.
  - **max-pdu-size**: Designate the maximum size of the PDU, in bytes. Must be an ranging from 1024 to 1460.

- **timeout**: Specify the number of times the system attempts to communicate with a CGF that is not responding.
- **wait-time**: Specify the time to wait before sending the GTPP request.

local-storage

Specify local storage details.

mode [localstreaming-parallel]

Specify a storage mode to be used.

- **local**: Specify the use of HDD to store CDRs
- **streaming-parallel**: Specify the use of HDD to store CDRs, if CGF fails. When CGF comes up, stream the CDRs to the CGF. Streaming is in a parallel and newly generated CDRs are sent to CGF along with CDRs streamed from HDD.

cgf-server-redundancy-support

Enable or disable the CGF server redundancy support per GTPP profile. By default this configuration is disabled.

profile icmpv6

Configures ICMPv6 profile parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **`profile icmpv6`** *`profile_name`*

icmpv6 *profile_name*

Specify name of the ICMPv6 profile.

Must be a string.

Usage Guidelines Use this command to configure the ICMPv6 profile parameters.

profile icmpv6 options

Configures ICMPv6 configuration parameters.

Command Modes Exec > Global Configuration (config) > ICMPv6 Profile Configuration (config-icmpv6-*profile_name*)

Syntax Description **`options { [ hop-limit`** *`hop_limit`* **`] [ mtu`** *`mtu_size`* **`] [ reachable-time`** *`reachable_period`* **`] [ retrans-timer`** *`retransmission_period`* **`] [ router-lifetime`** *`lifetime_period`* **`] [ virtual-mac`** *`mac_address`* **`] }`**

hop-limit *hop_limit*

Specify the hop limit.

Must be an integer in the range of 0-255.

Default Value: 255.

mtu *mtu_size*

Specify the Maximum Transmission Unit (MTU) size.

Must be an integer in the range of 1280-1500.

Default Value: 1500.

reachable-time *reachable_period*

Specify the reachable time in milliseconds.

Must be an integer in the range of 0-3600.

Default Value: 0.

retrans-timer *retransmission_period*

Specify the retransmission time in milliseconds.

Must be an integer in the range of 0-4294968.

Default Value: 0.

router-lifetime *lifetime_period*

Specify the router lifetime in seconds.

Must be an integer in the range of 0-65535.

Default Value: 65535.

virtual-mac *mac_address*

Specify the local virtual MAC address.

Must be a string in the mac-address pattern. For information on the mac-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure the ICMPv6 configuration parameters.

profile icmpv6 ra trigger

Configures trigger to send router advertisements.

Command Modes Exec > Global Configuration (config) > ICMPv6 Profile Configuration (config-icmpv6-*profile_name*)

Syntax Description

```
ra trigger handover { false | true }
```

handover { false | true }

Specify whether to disable or enable handovers of Wi-Fi.

Must be one of the following:

- **false**
- **true**

Default Value: false.

Usage Guidelines Use this command to configure trigger to send router advertisements.

profile interface-mapping default interface

This confiuration maps the Gm and Mw interfaces for P-CSCF restoration process.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile interface-mapping default interface [GM] [ipv4** *ipv4_address* **| ipv6** *ipv6_address* **] interface [MW] [ipv4** *ipv4_address* **| ipv6** *ipv6_address* **]**

profile interface-mapping default

Enables mapping Gm and Mw interfaces.

interface

Specifies the interfaces to be mapped. It has two possible values **GM** and **MW**.

[ipv4 ***ipv4_address*** **]**

Specifies the IPv4 address of the Gm or Mw interface to be mapped.

ipv6 ***ipv6_address***

Specifies the IPv6 address of the Gm or Mw interface to be mapped.

Usage Guidelines Use this command to map Gm and Mw interfaces to send the active P-CSCF addesses after a P-CSCF failure event.

profile load

Configures the load profile for load calculation and publishing.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile load** *load_profile_name* **[load-calc-frequency** *load_calc_frequency* **] [load-fetch-frequency** *load_fetch_frequency* **]**

load-calc-frequency *load_calc_frequency*

Specify the system load calculation interval in seconds.

Must be an integer in the range of 5-3600.

Default Value: 10.

load-fetch-frequency *load_fetch_frequency*

Specify the time interval at which Service pod fetches load from Cache pod in seconds.

Must be an integer in the range of 5-3600.

Default Value: 10.

load *load_profile_name*

Specify name of the load profile.

Must be a string.

Usage Guidelines Use this command to configure the load profile for load calculation and publishing.

You can configure a maximum of one element with this command.

profile load advertise

Configures the advertising action.

Command Modes Exec > Global Configuration (config) > Load Profile Configuration (config-load-*profile_name*)

Syntax Description **`advertise [ change-factor`** *`change_factor`* **`] [ interval`** *`interval`* **`]`**

change-factor *change_factor*

Specify the minimum change between current LCI and last indicated LCI, after which only advertising should happen.

Must be an integer in the range of 1-20.

Default Value: 5.

interval *interval*

Specify the periodicity of sending LCI to the peers in seconds.

Must be an integer in the range of 0-3600.

Default Value: 300.

Usage Guidelines Use this command to configure the advertising action.

profile load interface

Configures the list of interfaces.

Command Modes Exec > Global Configuration (config) > Load Profile Configuration (config-load-*profile_name*)

Syntax Description **interface** *interface_type* **[action** *action_on_interface* **]**

action *action_on_interface*

Specify the action on the interface.

Must be one of the following:

- **advertise**

interface *interface_type*

Specify the interface type.

Must be one of the following:

- **gtpc**

Usage Guidelines Use this command to configure the list of interfaces.

profile location-area-group

Configures the Location Area Group profile parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile location-area-group** *profile_name* **[ecgi-group** *ecgi_group_name* **] [ncgi-group** *ncgi_group_name* **] [tai-group** *tai_group_name* **]**

ecgi-group *ecgi_group_name*

Specify name of the ECGI group.

Must be a string.

location-area-group *profile_name*

Specify name of the Location Area Group profile.

Must be a string.

ncgi-group *ncgi_group_name*

Specify name of the NCGI group.

Must be a string.

tai-group *tai_group_name*

Specify name of the TAI group.

Must be a string.

Usage Guidelines Use this command to configure the Location Area Group profile parameters.

profile message-handling nf type udm mh-profile

Configures the UDM message handling profile.

Command Modes Exec > Global Configuration (config)

Syntax Description **`profile message-handling nf type udmmh-profile`** *`profile_name`*

profile message-handling nf type udm mh-profile *profile_name*

Configure the UDM message handling profile.

Usage Guidelines Use this command to configure UDM message handling profile at local configuration.

profile n3-tunnel

Configures N3 tunnelling information profile configuration.

Command Modes Exec > Global Configuration (config)

Syntax Description **`profile n3-tunnel`** *`profile_name`* **`[ notify ]`**

n3-tunnel *profile_name*

Specify name of the N3 tunnelling profile.

Must be a string.

notify

Specify to enable downlink data notification.

Usage Guidelines Use this command to configure N3 tunnelling information profile configuration.

profile n3-tunnel buffer

Configures the buffering for downlink direction.

Command Modes Exec > Global Configuration (config) > N3 Tunnel Profile Configuration (config-n3-tunnel-*profile_name*)

Syntax Description **`buffer`** *`node`*

buffer *node*

Specify to enable buffering.

Must be one of the following:

- **upf**: Enables buffering in UPF.

Usage Guidelines Use this command to configure buffering for downlink direction.

profile ncgi-group

Configures NCGI Group profile parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile ncgi-group** *profile_name*

ncgi-group *profile_name*

Specify name of the NCGI Group profile.

Must be a string.

Usage Guidelines Use this command to configure NCGI Group profile parameters.

profile ncgi-group ncgis

Configures the list of MCC, MNC, TAC, and NCGI groups.

Command Modes Exec > Global Configuration (config) > NCGI Group Profile Configuration (config-ncgi-group-*profile_name*)

Syntax Description **mcc** *mobile_country_code* **mnc** *mobile_network_code*

mcc *mobile_country_code*

Specify the Mobile Country Code (MCC). For example, 01, 001.

Must be a string in the three-digit pattern. For information on the three-digit pattern, see the *Input Pattern Types* chapter.

mnc *mobile_network_code*

Specify the Mobile Network Code (MNC). For example, 23, 456.

Must be a string in the two-or-three-digit pattern. For information on the two-or-three-digit pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure the list of MCC, MNC, TAC, and NCGI groups.

You can configure a maximum of 16 elements with this command.

profile ncgi-group ncgis ncgi

Configures NCGI Group parameters.

Command Modes Exec > Global Configuration (config) > NCGI Group Profile Configuration (config-ncgi-group-*profile_name*) > NCGI Group Profile MCC MNC Configuration (config-ncgi-group-*mcc*/*mnc*)

Syntax Description **ncgi list** *ncgi_values*

list *ncgi_values*

Specify the list of NCGI values - 9 digit hex string NR Cell ID.

Must be a string in the hex-stringncgi pattern. For information on the hex-stringncgi pattern, see the *Input Pattern Types* chapter.

You can configure a maximum of 64 elements with this keyword.

Usage Guidelines Use this command to configure NCGI Group parameters.

profile ncgi-group ncgis ncgi range

Configures an NCGI range.

Command Modes Exec > Global Configuration (config) > NCGI Group Profile Configuration (config-ncgi-group-*profile_name*) > NCGI Group Profile MCC MNC Configuration (config-ncgi-group-*mcc*/*mnc*)

Syntax Description **ncgi range start** *ncgi_range_start* **end** *ncgi_range_end*

end *ncgi_range_end*

Specify the NCGI range end value.

Must be a string in the hex-stringncgi pattern. For information on the hex-stringncgi pattern, see the *Input Pattern Types* chapter.

start *ncgi_range_start*

Specify the NCGI range start value.

Must be a string in the hex-stringncgi pattern. For information on the hex-stringncgi pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure an NCGI range.

You can configure a maximum of 64 elements with this command.

profile network-element amf

Configures the AMF profile.

Command Modes Exec > Global Configuration (config)

Syntax Description **`profile network-element amf`** *`amf_profile_name`* **`[ [ failure-handling-profile`** *`profile_name`* **`] [ nf-client-profile`** *`profile_name`* **`] [ query-target-plmn`** *`query_target_plmn`* **`] ]`**

amf *amf_profile_name*

Specify name of the AMF profile.

Must be a string.

failure-handling-profile *profile_name*

Specify name of the Failure Handling profile.

Must be a string.

nf-client-profile *profile_name*

Specify name of the NF Client profile.

Must be a string.

query-target-plmn *query_target_plmn*

Specify the query parameter target-plmn to be used.

Must be one of the following:

- **primary**
- **serving**
- **ue**

Usage Guidelines Use this command to configure the AMF profile. The CLI prompt changes to the AMF Profile Configuration mode (config-amf-<profile_name>).

profile network-element amf discovery

Configures the discovery method.

Command Modes Exec > Global Configuration (config) > AMF Profile Configuration (config-amf-*profile_name*)

Command Modes Exec > Global Configuration (config) > CHF Profile Configuration (config-chf-*profile_name*)

Command Modes Exec > Global Configuration (config) > PCF Profile Configuration (config-pcf-*profile_name*)

Command Modes Exec > Global Configuration (config) > UDM Profile Configuration (config-udm-*profile_name*)

Syntax Description **`discovery local`**

local

Specify to use local configuration for NF discovery. NF discovery through NRF will be skipped.

Usage Guidelines Use this command to configure the discovery method.

profile network-element amf query-params

Configures query parameter for NF discovery.

Command Modes Exec > Global Configuration (config) > AMF Profile Configuration (config-amf-*profile_name*)

Command Modes Exec > Global Configuration (config) > CHF Profile Configuration (config-chf-*profile_name*)

Command Modes Exec > Global Configuration (config) > PCF Profile Configuration (config-pcf-*profile_name*)

Command Modes Exec > Global Configuration (config) > UDM Profile Configuration (config-udm-*profile_name*)

Syntax Description **query-params** *query_parameters*

query-params *query_parameters*

Specify the query parameters.

Must be one of the following:

- **chf-supported-plmn**
- **dnn**
- **region-set**
- **requester-snssais**
- **tai**
- **target-nf-instance-id**
- **target-plmn**

Usage Guidelines Use this command to configure the query parameter for NF discovery.

profile network-element chf

Configures the CHF profile.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile network-element chf** *chf_profile_name* **[[failure-handling-profile** *profile_name* **] [failure-handling-profile-offline** *profile_name* **] [nf-client-profile** *profile_name* **] [nf-client-profile-offline** *profile_name* **] [nf-client-profile** *profile_name* **]]**

chf *chf_profile_name*

Specify name of the CHF profile.

Must be a string.

failure-handling-profile-offline *profile_name*

Specify the Failure Handling profile name for offline server.

Must be a string.

failure-handling-profile *profile_name*

Specify name of the Failure Handling profile.

Must be a string.

nf-client-profile-offline *profile_name*

Specify the NF Client profile name for offline server.

Must be a string.

nf-client-profile *profile_name*

Specify name of the NF Client profile.

Must be a string.

query-chf-supported-plmn *plmn_type*

Specify the PLMN type to be used for query parameter chf-supported-plmn.

Must be one of the following:

- **primary**
- **serving**
- **ue**

query-target-plmn *query_target_plmn*

Specify the query parameter target-plmn to be used.

Must be one of the following:

- **primary**
- **serving**
- **ue**

Usage Guidelines

Use this command to configure the CHF profile. The CLI prompt changes to the CHF Profile Configuration mode (config-chf-<profile_name>).

profile network-element chf discovery

Configures the discovery method.

Command Modes Exec > Global Configuration (config) > AMF Profile Configuration (config-amf-*profile_name*)

Command Modes Exec > Global Configuration (config) > CHF Profile Configuration (config-chf-*profile_name*)

Command Modes Exec > Global Configuration (config) > PCF Profile Configuration (config-pcf-*profile_name*)

Command Modes Exec > Global Configuration (config) > UDM Profile Configuration (config-udm-*profile_name*)

Syntax Description **`discovery local`**

local

Specify to use local configuration for NF discovery. NF discovery through NRF will be skipped.

Usage Guidelines Use this command to configure the discovery method.

profile network-element chf query-params

Configures query parameter for NF discovery.

Command Modes Exec > Global Configuration (config) > AMF Profile Configuration (config-amf-*profile_name*)

Command Modes Exec > Global Configuration (config) > CHF Profile Configuration (config-chf-*profile_name*)

Command Modes Exec > Global Configuration (config) > PCF Profile Configuration (config-pcf-*profile_name*)

Command Modes Exec > Global Configuration (config) > UDM Profile Configuration (config-udm-*profile_name*)

Syntax Description **`query-params`** *`query_parameters`*

query-params *query_parameters*

Specify the query parameters.

Must be one of the following:

- **chf-supported-plmn**
- **dnn**
- **requester-snssais**
- **tai**
- **target-nf-instance-id**
- **target-plmn**

Usage Guidelines Use this command to configure the query parameter for NF discovery.

profile network-element nrf

Configures NRF profile.

Command Modes Exec > Global Configuration (config)

Syntax Description

```
profile network-element nrf  nrf_profile_name nf-type nrf
message-handling-profileprofile_name nf-type nrf mh-profile
mh_profile_nameservice name type { nnrf-at | nnrf-bs | nnrf-nfd | nnrf-nfm
} message type { nf-deregister | nf-list-retrieval | nf-profile-retrieval
 | nf-register | nf-status-notify | nf-status-subscribe |
nf-status-unsubscribe | nf-updatenf-register }skip optional-ies locality
 ie smfinfolist tac-based
```

message-handling-profile *profile_name*

Specify name of the Message Handling profile.

nf-type nrf

Specify the NF type as NRF.

mh-profile *mh_profile_name*

Specify the NRF message handling profile configuration.

service name type { nnrf-at | nnrf-bs | nnrf-nfd | nnrf-nfm }

Specify the NRF service name type as nnrf-at, nnrf-bs, nnrf-nfd, and nnrf-nfm.

message type { nf-deregister | nf-list-retrieval | nf-profile-retrieval | nf-register | nf-status-notify | nf-status-subscribe | nf-status-unsubscribe | nf-updatenf-register }

Specify the message type as as NF Deregister, NF list retrieval, NF profile retrieval, NF register, NF status notify, NF status subscribe, NF status unsubscribe, NF update, and NF regsiter.

skip optional-ies locality

Specify the locality parameter to skip for the selected NRF message.

Important The **skip optional-ies locality** CLI configuration is currently ineffective and will require backend changes in the future releases. This CLI must be enabled to facilitate seamless rolling upgrade to future releases when this CLI backend support is fully available.

ie smfinfolist

Specify the **smfInfoList** Information Element name to be grouped.

tac-based

Groups the **smfInfo** attributes based on TAC Group.



Note You are recommended to use this configuration only when you want to add new slice or TAC Group information.

Usage Guidelines Use this command to configure the NRF profile.

profile network-element pcf

Configures the PCF profile.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile network-element pcf** *pcf_profile_name* **[[cause-map-class-profile** *profile_name* **] [failure-handling-profile** *profile_name* **] [nf-client-profile** *profile_name* **] [predefined-rule-prefix** *prefix_name* **] [query-target-plmn** *query_target_plmn* **] [response-timeout** *response_timeout_duration* **] [rulebase-prefix** *rulebase_prefix* **] [update-notify** *update_notify* **] [use-amf-provided-pcf [false | true]]**

cause-map-class-profile *profile_name*

Specify name of the Cause Map Class profile.

Must be a string.

failure-handling-profile *profile_name*

Specify name of the Failure Handling profile.

Must be a string.

nf-client-profile *profile_name*

Specify name of the NF Client profile.

Must be a string.

pcf *pcf_profile_name*

Specify name of the PCF profile.

Must be a string.

predefined-rule-prefix *prefix_name*

Specify the predefined rule prefix string.

Must be a string.

query-target-plmn *query_target_plmn*

Specify the query parameter target-plmn to be used.

Must be one of the following:

- **primary**
- **serving**
- **ue**

response-timeout *response_timeout_duration*

Specify the response timeout duration, in milliseconds.

Must be an integer in the range of 1000-30000.

Default Value: 4000.

rulebase-prefix *rulebase_prefix*

Specify the rulebase prefix string.

Must be a string.

update-notify *update_notify*

Specify the SMF Immediate UpdateNotify Response behavior.

Must be one of the following:

- **expidite-response**

use-amf-provided-pcf { false | true }

Specify to enable or disable PCF discovery using PCF ID provided by the AMF.

Must be one of the following:

- **false**
- **true**

Default Value: true.

Usage Guidelines Use this command to configure the PCF profile. The CLI prompt changes to the PCF Profile Configuration mode ().

profile network-element pcf bitrates

Configures bitrates round-up parameter.

Command Modes Exec > Global Configuration (config) > PCF Profile Configuration (config-pcf-*profile_name*)

Syntax Description `bitrates rounded-up`

rounded-up

Specify to round up.

Usage Guidelines Use this command to configure bitrates round-up parameter.

profile network-element pcf discovery

Configures the discovery method.

Command Modes Exec > Global Configuration (config) > AMF Profile Configuration (config-amf-*profile_name*)

Command Modes Exec > Global Configuration (config) > CHF Profile Configuration (config-chf-*profile_name*)

Command Modes Exec > Global Configuration (config) > PCF Profile Configuration (config-pcf-*profile_name*)

Command Modes Exec > Global Configuration (config) > UDM Profile Configuration (config-udm-*profile_name*)

Syntax Description **`discovery local`**

local

Specify to use local configuration for NF discovery. NF discovery through NRF will be skipped.

Usage Guidelines Use this command to configure the discovery method.

profile network-element pcf query-params

Configures query parameter for NF discovery.

Command Modes Exec > Global Configuration (config) > AMF Profile Configuration (config-amf-*profile_name*)

Command Modes Exec > Global Configuration (config) > CHF Profile Configuration (config-chf-*profile_name*)

Command Modes Exec > Global Configuration (config) > PCF Profile Configuration (config-pcf-*profile_name*)

Command Modes Exec > Global Configuration (config) > UDM Profile Configuration (config-udm-*profile_name*)

Syntax Description **`query-params`** *`query_parameters`*

query-params *query_parameters*

Specify the query parameters.

Must be one of the following:

- **chf-supported-plmn**
- **dnn**
- **requester-snssais**

- **tai**
- **target-nf-instance-id**
- **target-plmn**

Usage Guidelines Use this command to configure the query parameter for NF discovery.

profile network-element scp

Configures the SCP profile.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile network-element scp** *scp_profile_name* **[nf-client-profile** *scp_client_profile_name* **[discovery-params [service-names]] | failure-handling-profile***failure_handling_scp_profile_name* **]] [query-target-plmn** *query_target_plmn* **]**

profile network-element scp*scp_profile_name*

Specify the SCP as the network element profile.

scp_profile_name must an alphanumeric string representing the corresponding network element profile name.

nf-client-profile *scp_client_profile_name*

Specify the SCP client profile.

scp_client_profile_name must an alphanumeric string representing the corresponding NF client profile name.

discovery-params [service-names]

Specify this option to include 3gpp-Sbi-Discovery-service-names IE in the SCP header.

Important If you are downgrading SMF, make sure you first disable this command. If this CLI command is configured after the upgrade, you will observe that only the new sessions will include the discovery service names as one of the headers in SCP.

failure-handling-profile*failure_handling_scp_profile_name*

Specify the SCP failure handling network profile for the configured SCP.

failure_handling_scp_profile_name must an alphanumeric string representing the corresponding SCP failure handling network profile name.

Usage Guidelines Use this command to configure the SCP profile.

profile network-element sepp

Configures the SEPP profile.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile network-element sepp** *sepp_profile_name* **[[failure-handling-profile** *profile_name* **] [nf-client-profile** *profile_name* **] [query-target-plmn** *query_target_plmn* **]]**

failure-handling-profile *profile_name*

Specify name of the Failure Handling profile.

Must be a string.

nf-client-profile *profile_name*

Specify name of the NF Client profile.

Must be a string.

query-target-plmn *query_target_plmn*

Specify the query parameter target-plmn to be used.

Must be one of the following:

- **primary**
- **serving**
- **ue**

sepp *sepp_profile_name*

Specify name of the SEPP profile.

Must be a string.

Usage Guidelines Use this command to configure the SEPP profile. The CLI prompt changes to the SEPP Profile Configuration mode (config-sepp-<profile_name>).

profile network-element sepp discovery

Configures the discovery method.

Command Modes Exec > Global Configuration (config) > AMF Profile Configuration (config-amf-*profile_name*)

Command Modes Exec > Global Configuration (config) > CHF Profile Configuration (config-chf-*profile_name*)

Command Modes Exec > Global Configuration (config) > PCF Profile Configuration (config-pcf-*profile_name*)

Command Modes Exec > Global Configuration (config) > UDM Profile Configuration (config-udm-*profile_name*)

Syntax Description **`discovery local`**

local

Specify to use local configuration for NF discovery. NF discovery through NRF will be skipped.

Usage Guidelines Use this command to configure the discovery method.

profile network-element sepp query-params

Configures query parameter for NF discovery.

Command Modes Exec > Global Configuration (config) > AMF Profile Configuration (config-amf-*profile_name*)

Command Modes Exec > Global Configuration (config) > CHF Profile Configuration (config-chf-*profile_name*)

Command Modes Exec > Global Configuration (config) > PCF Profile Configuration (config-pcf-*profile_name*)

Command Modes Exec > Global Configuration (config) > UDM Profile Configuration (config-udm-*profile_name*)

Syntax Description **`query-params`** *`query_parameters`*

query-params *query_parameters*

Specify the query parameters.

Must be one of the following:

- **chf-supported-plmn**
- **dnn**
- **requester-snssais**
- **tai**
- **target-nf-instance-id**
- **target-plmn**

Usage Guidelines Use this command to configure the query parameter for NF discovery.

profile network-element udm

Configures UDM profile.

Command Modes Exec > Global Configuration (config)

Syntax Description

profile network-element udm *udm_profile_name* **[[cause-map-class-profile** *profile_name* **] [failure-handling-profile** *profile_name* **] [message-handling-profile** *profile_name* **] [nf-client-profile** *profile_name* **]]**

cause-map-class-profile *profile_name*

Specify name of the Cause Map Class profile.

Must be a string.

failure-handling-profile *profile_name*

Specify name of the Failure Handling profile.

Must be a string.

message-handling-profile *profile_name*

Specify name of the Message Handling profile.

nf-client-profile *profile_name*

Specify name of the NF Client profile.

Must be a string.

query-target-plmn *query_target_plmn*

Specify the query parameter target-plmn to be used.

Must be one of the following:

- **primary**
- **serving**
- **ue**

response-timeout *response_timeout_duration*

Specify the response timeout duration in milliseconds.

Must be an integer in the range of 1000-30000.

Default Value: 4000.

udm *udm_profile_name*

Specify name of the UDM profile.

Must be a string.

Usage Guidelines

Use this command to configure the UDM profile. The CLI prompt changes to the UDM Profile Configuration mode (config-udm-<profile_name>)

profile network-element udm discovery

Configures the discovery method.

Command Modes Exec > Global Configuration (config) > AMF Profile Configuration (config-amf-*profile_name*)

Command Modes Exec > Global Configuration (config) > CHF Profile Configuration (config-chf-*profile_name*)

Command Modes Exec > Global Configuration (config) > PCF Profile Configuration (config-pcf-*profile_name*)

Command Modes Exec > Global Configuration (config) > UDM Profile Configuration (config-udm-*profile_name*)

Syntax Description **`discovery local`**

local

Specify to use local configuration for NF discovery. NF discovery through NRF will be skipped.

Usage Guidelines Use this command to configure the discovery method.

profile network-element udm failure-handling-profile-rat

Configures Failure Handling profile specific to RAT type.

Command Modes Exec > Global Configuration > Profile Configuration

Syntax Description **`failure-handling-profile-rat rat-type`** *`rat_type`* **`failure-handling-profile`** *`failure_handling_profile_name`*

failure-handling-profile *failure_handling_profile_name*

Specify name of Failure Handling profile.

Must be a string.

rat-type *rat_type*

Specify the RAT type.

Must be one of the following:

- **eutra**
- **nr**
- **wlan**

Usage Guidelines Use this command to configure Failure Handling profile specific to RAT type.

profile network-element udm query-params

Configures query parameter for NF discovery.

Command Modes Exec > Global Configuration (config) > AMF Profile Configuration (config-amf-*profile_name*)

Command Modes Exec > Global Configuration (config) > CHF Profile Configuration (config-chf-*profile_name*)

Command Modes Exec > Global Configuration (config) > PCF Profile Configuration (config-pcf-*profile_name*)

Command Modes Exec > Global Configuration (config) > UDM Profile Configuration (config-udm-*profile_name*)

Syntax Description **query-params** *query_parameters*

query-params *query_parameters*

Specify the query parameters.

Must be one of the following:

- **chf-supported-plmn**
- **dnn**
- **requester-snssais**
- **tai**
- **target-nf-instance-id**
- **target-plmn**

Usage Guidelines Use this command to configure the query parameter for NF discovery.

profile network-element upf

Configures the UPF profile.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile network-element upf** *upf_profile_name* **{ max-upf-sessions** *max_upf_sessions_count* **[[capacity** *lb_capacity* **] [dnn-list** *dnn_list* **] [downlink-data-buffer { false | true }] [downlink-data-report { false | true }] [dual-stack-transport { false | true }] [mode** *mode_of_operation* **] [n4-peer-port** *port_number* **] [node-id** *node_id* **] [priority** *lb_priority* **] [upf-group-profile** *profile_name* **]] }**

max-upf-sessions *max_upf_sessions_count*

Configures maximum UPF sessions on SMF.

capacity *lb_capacity*

Specify the static capacity relative to other UPFs used for load balancing.

Must be an integer in the range of 0-65535.

Default Value: 10.

dnn-list *dnn_list*

Specify the list of DNNs supported by the UPF node.

Must be a string.

downlink-data-buffer { false | true }

Specify to enable or disable buffering in UPF for downlink data.

Must be one of the following:

- **false**
- **true**

Default Value: true.

downlink-data-report { false | true }

Specify to enable or disable notification from UPF for downlink data.

Must be one of the following:

- **false**
- **true**

Default Value: true.

dual-stack-transport { false | true }

Specify to enable or disable the dual stack transport for the N3 interface.

When the **dual-stack-transport true** command is configured, SMF sends the Outer Header Removal (OHR) IE with the value 6 for the IPv6 address on the supported interfaces.

Must be one of the following:

- **false**
- **true**

Default Value: false.



Note This CLI configuration is applicable for SMF with the legacy interfaces as well.

mode *mode_of_operation*

Specify the UPF mode of operation.

Must be one of the following:

- **offline**

n4-peer-port *port_number*

Specify the UPF N4 peer port number.

Must be an integer in the range of 0-65535.

Default Value: 8805.

node-id *node_id*

Specify the node ID for the UPF peer node.

Must be a string.

priority *lb_priority*

Specify the static priority relative to other UPFs used for load balancing.

Must be an integer in the range of 0-65535.

Default Value: 1.

upf-group-profile *profile_name*

Specify the name of the UPF Group profile.

Must be a string.

upf *upf_profile_name*

Specify the name of the UPF peer.

Must be a string.

Usage Guidelines Use this command to configure the UPF profile. When the active profile is removed, clears if any existing sessions and UPF will be detached. The CLI prompt changes to the UPF Profile Configuration mode (config-upf-<profile_name>).

profile network-element upf n4-peer-address

Configures the N4 peer address.

Command Modes Exec > Global Configuration (config) > UPF Profile Configuration (config-upf-*profile_name*)

Syntax Description **`n4-peer-address { [ ipv4-address`** *`ipv4_address`* **`] [ ipv6-address`** *`ipv6_address`* **`] }`**

ipv4-address *ipv4_address*

Specify the N4 peer IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6-address *ipv6_address*

Specify the N4 peer IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to confgure the N4 peer address.

profile nf-client nf-type amf amf-profile

Configures AMF profile parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **`profile nf-client nf-type amf amf-profile`** *`profile_name`*

amf-profile *profile_name*

Specify the AMF profile name

Must be a string.

Usage Guidelines Use this command to configure AMF profile parameters.

profile nf-client nf-type amf amf-profile locality

Configures the AMF profile locality parameter.

Command Modes Exec > Global Configuration (config) > AMF Profile Configuration (config-amf-profile-*profile_name*)

Syntax Description **`locality`** *`locality_name`* **`[ priority`** *`locality_priority`* **`]`**

locality *locality_name*

Specify name of the locality.

Must be a string.

priority *locality_priority*

Specify priority of the locality configuration.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the AMF profile locality parameter.

profile nf-client nf-type amf amf-profile locality service name type

Configures the AMF service name type parameter.

Command Modes Exec > Global Configuration (config) > AMF Configuration (config-amf) > Failure Handling *profile_name* Configuration mode (config-failure-handling-*profile_name*)

Syntax Description **type** *amf_service_name_type*

responsetimeout *response_timeout*

Specify the response timeout interval in milliseconds.

Must be an integer.

Default Value: 2000.

type *amf_service_name_type*

Specify the service name type.

Must be one of the following:

- **namf-comm**
- **namf-evts**
- **namf-loc**
- **namf-mt**

Usage Guidelines Use this command to configure the AMF service name type parameter.

profile nf-client nf-type amf amf-profile locality service name type endpoint-profile

Configures endpoint profile parameters.

Command Modes Exec > Global Configuration

Syntax Description **endpoint-profile** *endpoint_profile_name* **{ capacity** *capacity_value* **| priority** *profile_priority* **| api-uri-prefix** *api_uri_prefix* **| api-root** *api_root* **| uri-scheme** *uri_scheme* **}**

api-root *api_root*

Specify the API root.

Must be a string.

api-uri-prefix *api_uri_prefix*

Specify the API URI prefix.

Must be a string.

capacity *capacity_value*

Specify the profile capacity.

Must be an integer in the range of 0-65535.

Default Value: 10.

endpoint-profile *endpoint_profile_name*

Specify name of the endpoint profile.

Must be a string.

priority *profile_priority*

Specify the priority of the profile.

Must be an integer in the range of 0-65535.

Default Value: 1.

uri-scheme *uri_scheme*

Specify the URI scheme.

Must be one of the following:

- **http**: HTTP.
- **https**: HTTPS.

Usage Guidelines Use this command to configure endpoint profile parameters.

profile nf-client nf-type amf amf-profile locality service name type endpoint-profile endpoint-name

Configures the endpoint name parameter.

Command Modes Exec > Global Configuration

Syntax Description **endpoint-name** *endpoint_name* **[priority** *node_priority* **| capacity** *node_capacity* **]**

capacity *node_capacity*

Specify the node capacity for the endpoint.

Must be an integer in the range of 0-65535.

endpoint-name *endpoint_name*

Specify name of the endpoint. You can configure the primary, secondary, and tertiary host (IP: Port) within each endpoint for NF server failover handling. The server failover configuration accepts both IPv4 and IPv6 addresses. However, the SMF gives preference to the IPv4 address.

Must be a string.

priority *node_priority*

Specify the node priority for the endpoint.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this configuration to configure the endpoint name parameter.

profile nf-client nf-type amf amf-profile locality service name type endpoint-profile endpoint-name primary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **`ip-address { { ipv4`** *`ipv4_address`* **`| ipv6`** *`ipv6_address`* **`} | port`** *`port_number`* **`}`**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type amf amf-profile locality service name type endpoint-profile endpoint-name secondary ip-address

Configures the endpoint IP address and port number.

Command Modes

Exec > Global Configuration

Syntax Description

ip-address { { ipv4 *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 ***ipv4_address***

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 ***ipv6_address***

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port ***port_number***

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines

Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type amf amf-profile locality service name type endpoint-profile endpoint-name tertiary ip-address

Configures the endpoint IP address and port number.

Command Modes

Exec > Global Configuration

Syntax Description

ip-address { { ipv4 *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 ***ipv4_address***

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type amf amf-profile locality service name type endpoint-profile version uri-version

Configures the URI version.

Command Modes Exec > Global Configuration > UDM NF-Client Profile Configuration > UDM Profile Configuration > Locality Configuration > UDM Service Name Type Configuration > Endpoint Profile Configuration > Version Configuration > URL Version Configuration

Syntax Description **`version uri-version {`** *`uri_version`* **`|`** **`full-version`** *`full_version`* **`}`**

full-version *full_version*

Specify the full version in the format *major-version.minor-version.patch-version*.[alpha-*draft-number*]

Must be a string.

uri-version *uri_version*

Specify the URI version.

Must be a string in the pattern v\d.

Usage Guidelines Use this command to configure the URI version information.

profile nf-client nf-type ausf ausf-profile

Configures AUSF profile parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **`profile nf-client nf-type ausf ausf-profile`** *`profile_name`*

ausf-profile *profile_name*

Specify name of the AUSF profile.

Must be a string.

Usage Guidelines Use this command to configure AUSF profile parameters.

profile nf-client nf-type ausf ausf-profile locality

Configures the AUSF profile locality parameter.

Command Modes Exec > Global Configuration (config) > AUSF Profile Configuration (config-ausf-profile-*profile_name*)

Syntax Description **`locality`** *`locality_name`* **`[ priority`** *`locality_priority`* **`]`**

locality *locality_name*

Specify name of the locality.

Must be a string.

priority *locality_priority*

Specify priority of the locality configuration.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the AUSF profile locality parameter.

profile nf-client nf-type ausf ausf-profile locality service name type

Configures the AUSF service name type parameter.

Command Modes Exec > Global Configuration (config) > AUSF Configuration (config-ausf) > Failure Handling *profile_name* Configuration mode (config-failure-handling-*profile_name*)

Syntax Description **`type`** *`ausf_service_name_type`*

responsetimeout *response_timeout*

Specify the response timeout interval in milliseconds.

Must be an integer.

Default Value: 2000.

type *ausf_service_name_type*

Specify the AUSF service name type.

Must be one of the following:

- **nausf-auth**

Usage Guidelines Use this command to configure the AUSF service name type parameter.

profile nf-client nf-type ausf ausf-profile locality service name type endpoint-profile

Configures endpoint profile parameters.

Command Modes Exec > Global Configuration

Syntax Description **endpoint-profile** *endpoint_profile_name* **{ capacity** *capacity_value* **| priority** *profile_priority* **| api-uri-prefix** *api_uri_prefix* **| api-root** *api_root* **| uri-scheme** *uri_scheme* **}**

api-root *api_root*

Specify the API root.

Must be a string.

api-uri-prefix *api_uri_prefix*

Specify the API URI prefix.

Must be a string.

capacity *capacity_value*

Specify the profile capacity.

Must be an integer in the range of 0-65535.

Default Value: 10.

endpoint-profile *endpoint_profile_name*

Specify name of the endpoint profile.

Must be a string.

priority *profile_priority*

Specify the priority of the profile.

Must be an integer in the range of 0-65535.

Default Value: 1.

uri-scheme *uri_scheme*

Specify the URI scheme.

Must be one of the following:

- **http**: HTTP.

- **https**: HTTPS.

Usage Guidelines Use this command to configure endpoint profile parameters.

profile nf-client nf-type ausf ausf-profile locality service name type endpoint-profile endpoint-name

Configures the endpoint name parameter.

Command Modes Exec > Global Configuration

Syntax Description **endpoint-name** *endpoint_name* **[priority** *node_priority* **| capacity** *node_capacity* **]**

capacity *node_capacity*

Specify the node capacity for the endpoint.

Must be an integer in the range of 0-65535.

endpoint-name *endpoint_name*

Specify name of the endpoint. You can configure the primary, secondary, and tertiary host (IP: Port) within each endpoint for NF server failover handling. The server failover configuration accepts both IPv4 and IPv6 addresses. However, the SMF gives preference to the IPv4 address.

Must be a string.

priority *node_priority*

Specify the node priority for the endpoint.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this configuration to configure the endpoint name parameter.

profile nf-client nf-type ausf ausf-profile locality service name type endpoint-profile endpoint-name primary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **ip-address { { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type ausf ausf-profile locality service name type endpoint-profile endpoint-name secondary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **ip-address { { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type ausf ausf-profile locality service name type endpoint-profile endpoint-name tertiary ip-address

Configures the endpoint IP address and port number.

Command Modes

Exec > Global Configuration

Syntax Description

ip-address { { ipv4 *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines

Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type ausf ausf-profile locality service name type endpoint-profile version uri-version

Configures the URI version.

Command Modes

Exec > Global Configuration > UDM NF-Client Profile Configuration > UDM Profile Configuration > Locality Configuration > UDM Service Name Type Configuration > Endpoint Profile Configuration > Version Configuration > URL Version Configuration

Syntax Description

version uri-version { *uri_version* **| full-version** *full_version* **}**

full-version *full_version*

Specify the full version in the format *major-version*.*minor-version*.*patch-version*.[alpha-*draft-number*]

Must be a string.

uri-version *uri_version*

Specify the URI version.

Must be a string in the pattern v\d.

Usage Guidelines Use this command to configure the URI version information.

profile nf-client nf-type chf chf-profile

Configures the CHF profile parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile nf-client nf-type chf chf-profile** *profile_name*

chf-profile *profile_name*

Specify name of the CHF profile.

Must be a string.

Usage Guidelines Use this command to configure the CHF profile parameters.

profile nf-client nf-type chf chf-profile locality

Configures the CHF profile locality parameter.

Command Modes Exec > Global Configuration (config) > CHF Profile Configuration (config-chf-profile-*profile_name*)

Syntax Description **locality** *locality_name* **[priority** *locality_priority* **]**

locality *locality_name*

Specify name of the locality.

Must be a string.

priority *locality_priority*

Specify priority of the locality configuration.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the CHF profile locality parameter.

profile nf-client nf-type chf chf-profile locality service name type

Configures the CHF service name type parameter.

Command Modes Exec > Global Configuration (config) > CHF Configuration (config-chf) > Failure Handling *profile_name* Configuration mode (config-failure-handling-*profile_name*)

Syntax Description **type** *service_name_type*

responsetimeout *response_timeout*

Specify the response timeout interval in milliseconds.

Must be an integer.

Default Value: 2000.

type *service_name_type*

Specify the CHF service name type.

Must be one of the following:

- **nchf-convergedcharging**
- **nchf-spendinglimitcontrol**

Usage Guidelines Use this command to configure the CHF service name type parameter.

profile nf-client nf-type chf chf-profile locality service name type endpoint-profile

Configures endpoint profile parameters.

Command Modes Exec > Global Configuration

Syntax Description **endpoint-profile** *endpoint_profile_name* **{ capacity** *capacity_value* **| priority** *profile_priority* **| api-uri-prefix** *api_uri_prefix* **| api-root** *api_root* **| uri-scheme** *uri_scheme* **}**

api-root *api_root*

Specify the API root.

Must be a string.

api-uri-prefix *api_uri_prefix*

Specify the API URI prefix.

Must be a string.

capacity *capacity_value*

Specify the profile capacity.

Must be an integer in the range of 0-65535.

Default Value: 10.

endpoint-profile *endpoint_profile_name*

Specify name of the endpoint profile.

Must be a string.

priority *profile_priority*

Specify the priority of the profile.

Must be an integer in the range of 0-65535.

Default Value: 1.

uri-scheme *uri_scheme*

Specify the URI scheme.

Must be one of the following:

- **http**: HTTP.
- **https**: HTTPS.

Usage Guidelines Use this command to configure endpoint profile parameters.

profile nf-client nf-type chf chf-profile locality service name type endpoint-profile endpoint-name

Configures the endpoint name parameter.

Command Modes Exec > Global Configuration

Syntax Description **endpoint-name** *endpoint_name* **[priority** *node_priority* **| capacity** *node_capacity* **]**

capacity *node_capacity*

Specify the node capacity for the endpoint.

Must be an integer in the range of 0-65535.

endpoint-name *endpoint_name*

Specify name of the endpoint. You can configure the primary, secondary, and tertiary host (IP: Port) within each endpoint for NF server failover handling. The server failover configuration accepts both IPv4 and IPv6 addresses. However, the SMF gives preference to the IPv4 address.

Must be a string.

priority *node_priority*

Specify the node priority for the endpoint.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this configuration to configure the endpoint name parameter.

profile nf-client nf-type chf chf-profile locality service name type endpoint-profile endpoint-name primary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **`ip-address { { ipv4` *`ipv4_address`* **`| ipv6`** *`ipv6_address`* **`} | port`** *`port_number`* **`}`**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type chf chf-profile locality service name type endpoint-profile endpoint-name secondary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **ip-address { { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type chf chf-profile locality service name type endpoint-profile endpoint-name tertiary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **ip-address { { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type chf chf-profile locality service name type endpoint-profile version uri-version

Configures the URI version.

Command Modes Exec > Global Configuration > UDM NF-Client Profile Configuration > UDM Profile Configuration > Locality Configuration > UDM Service Name Type Configuration > Endpoint Profile Configuration > Version Configuration > URL Version Configuration

Syntax Description **`version uri-version {`** *`uri_version`* **`|`** **`full-version`** *`full_version`* **`}`**

full-version *full_version*

Specify the full version in the format *major-version*.*minor-version*.*patch-version*.[alpha-*draft-number*]

Must be a string.

uri-version *uri_version*

Specify the URI version.

Must be a string in the pattern v\d.

Usage Guidelines Use this command to configure the URI version information.

profile nf-client nf-type eir eir-profile

Configures EIR profile parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **`profile nf-client nf-type eir eir-profile`** *`eir_profile_name`*

eir-profile *eir_profile_name*

Specify name of the EIR profile.

Must be a string.

Usage Guidelines Use this command to configure the EIR profile parameters.

profile nf-client nf-type eir eir-profile locality

Configures the EIR profile locality parameter.

Command Modes Exec > Global Configuration (config) > EIR Profile Configuration (config-eir-profile-*profile_name*)

Syntax Description **`locality`** *`locality_name`* **`[ priority`** *`priority`* **`]`**

locality *locality_name*

Specify name of the locality.

Must be a string.

priority *priority*

Specify the priority of the locality configuration.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the EIR profile locality parameter.

profile nf-client nf-type eir eir-profile locality service name type

Configures the EIR service name type parameter.

Command Modes Exec > Global Configuration (config) > EIR Configuration (config-eir) > Failure Handling *profile_name* Configuration mode (config-failure-handling-*profile_name*)

Syntax Description **`type`** *`service_name_type`*

responsetimeout *response_timeout_interval*

Specify the response timeout interval in milliseconds.

Must be an integer.

Default Value: 2000.

type *service_name_type*

Specify the EIR service name type.

Must be one of the following:

- **n5g-eir-eic**

Usage Guidelines Use this command to configure the EIR service name type parameter.

profile nf-client nf-type eir eir-profile locality service name type endpoint-profile

Configures endpoint profile parameters.

Command Modes Exec > Global Configuration

Syntax Description **endpoint-profile** *endpoint_profile_name* **{ capacity** *capacity_value* **| priority** *profile_priority* **| api-uri-prefix** *api_uri_prefix* **| api-root** *api_root* **| uri-scheme** *uri_scheme* **}**

api-root *api_root*

Specify the API root.

Must be a string.

api-uri-prefix *api_uri_prefix*

Specify the API URI prefix.

Must be a string.

capacity *capacity_value*

Specify the profile capacity.

Must be an integer in the range of 0-65535.

Default Value: 10.

endpoint-profile *endpoint_profile_name*

Specify name of the endpoint profile.

Must be a string.

priority *profile_priority*

Specify the priority of the profile.

Must be an integer in the range of 0-65535.

Default Value: 1.

uri-scheme *uri_scheme*

Specify the URI scheme.

Must be one of the following:

- **http**: HTTP.

- **https**: HTTPS.

Usage Guidelines Use this command to configure endpoint profile parameters.

profile nf-client nf-type eir eir-profile locality service name type endpoint-profile endpoint-name

Configures the endpoint name parameter.

Command Modes Exec > Global Configuration

Syntax Description **endpoint-name** *endpoint_name* **[priority** *node_priority* **| capacity** *node_capacity* **]**

capacity *node_capacity*

Specify the node capacity for the endpoint.

Must be an integer in the range of 0-65535.

endpoint-name *endpoint_name*

Specify name of the endpoint. You can configure the primary, secondary, and tertiary host (IP: Port) within each endpoint for NF server failover handling. The server failover configuration accepts both IPv4 and IPv6 addresses. However, the SMF gives preference to the IPv4 address.

Must be a string.

priority *node_priority*

Specify the node priority for the endpoint.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this configuration to configure the endpoint name parameter.

profile nf-client nf-type eir eir-profile locality service name type endpoint-profile endpoint-name primary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **ip-address { { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type eir eir-profile locality service name type endpoint-profile endpoint-name secondary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **`ip-address { { ipv4`** *`ipv4_address`* **`| ipv6`** *`ipv6_address`* **`} | port`** *`port_number`* **`}`**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type eir eir-profile locality service name type endpoint-profile endpoint-name tertiary ip-address

Configures the endpoint IP address and port number.

Command Modes

Exec > Global Configuration

Syntax Description

ip-address { { ipv4 *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 ***ipv4_address***

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 ***ipv6_address***

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port ***port_number***

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines

Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type eir eir-profile locality service name type endpoint-profile version uri-version

Configures the URI version.

Command Modes

Exec > Global Configuration > UDM NF-Client Profile Configuration > UDM Profile Configuration > Locality Configuration > UDM Service Name Type Configuration > Endpoint Profile Configuration > Version Configuration > URL Version Configuration

Syntax Description

version uri-version { *uri_version* **| full-version** *full_version* **}**

full-version ***full_version***

Specify the full version in the format *major-version*.*minor-version*.*patch-version*.[alpha-*draft-number*]

Must be a string.

uri-version *uri_version*

Specify the URI version.

Must be a string in the pattern v\d.

Usage Guidelines Use this command to configure the URI version information.

profile nf-client nf-type endpoint-name fqdn name fqdn port

Configures the fqdn name and port for NF client profile.

Command Modes Exec > Global Configuration (config) > NF Client Configuration (config-profile nf-client nf-type-*client_nf_type*)

Syntax Description **nf-client profile** *nf_client_profile_name* **[locality** *locality_name* **[priority** *priority_value* **{ service name type** *service_name_type* **{ endpoint-profile** *endpoint_profile_name* **[capacity** *capacity_value* **| priority** *priority_value* **| uri-scheme** *uri_scheme_name* **| endpoint-name** *endpoint_name* **{ fqdn** *fqdn_value* **| fqdn-port** *fqdn_port* **}] } }]]**

nf-client profile *nf_client_profile_name* [locality *locality_name* [priority *priority_value* { service name type *service_name_type* { endpoint-profile *endpoint_profile_name* [capacity *capacity_value* | priority *priority_value* | uri-scheme *uri_scheme_name* | endpoint-name *endpoint_name* { fqdn *fqdn_name* | fqdn-port *fqdn_port* }] }}]]

- **locality** *locality_name* —Specify the locality of the profile.
- **priority** *priority_value* —Specify the priority value.
- **service name type** *service_name_type* —Specify the service name type.
- **uri-scheme** *uri_scheme_name* —Specify the uri-scheme as http or https.
- **fqdn name** *fqdn_address* —Specify the fqdn name.
- **fqdn-port** *fqdn_port* —Specify the fqdn port number. If port is not configured, SMF uses the standard port for FQDN, that is 80 for URI scheme http and 443 for URI scheme https.

Usage Guidelines Use this command to configure Configures the fqdn name and port for NF client profile.

profile nf-client nf-type pcf pcf-profile

Configures PCF profile parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile nf-client nf-type pcf pcf-profile** *profile_name*

pcf-profile *profile_name*

Specify name of the PCF profile.

Must be a string.

Usage Guidelines Use this command to configure the PCF profile.

profile nf-client nf-type pcf pcf-profile locality

Configures the PCF profile locality parameter.

Command Modes Exec > Global Configuration (config) > PCF Profile Configuration (config-psf-profile-*profile_name*)

Syntax Description **`locality`** *`locality_name`* **`[ priority`** *`locality_priority`* **`]`**

locality *locality_name*

Specify name of the locality.

Must be a string.

priority *locality_priority*

Specify priority of the locality configuration.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the PCF profile locality parameter.

profile nf-client nf-type pcf pcf-profile locality service name type

Configures the PCF service name type parameter.

Command Modes Exec > Global Configuration (config) > PCF Configuration (config-pcf) > Failure Handling *profile_name* Configuration mode (config-failure-handling-*profile_name*)

Syntax Description **`type`** *`service_name_type`*

responsetimeout *response_timeout*

Specify the response timeout interval in milliseconds.

Must be an integer.

Default Value: 2000.

type *service_name_type*

Specify the PCF service name parameters.

Must be one of the following:

- **npcf-am-policy-control**

- **npcf-bdtpolicycontrol**
- **npcf-eventexposure**
- **npcf-policyauthorization**
- **npcf-smpolicycontrol**
- **npcf-ue-policy-control**

Usage Guidelines Use this command to configure the PCF service name type parameter.

profile nf-client nf-type pcf pcf-profile locality service name type endpoint-profile

Configures endpoint profile parameters.

Command Modes Exec > Global Configuration

Syntax Description **endpoint-profile** *endpoint_profile_name* **{ capacity** *capacity_value* **| priority** *profile_priority* **| api-uri-prefix** *api_uri_prefix* **| api-root** *api_root* **| uri-scheme** *uri_scheme* **}**

api-root *api_root*

Specify the API root.

Must be a string.

api-uri-prefix *api_uri_prefix*

Specify the API URI prefix.

Must be a string.

capacity *capacity_value*

Specify the profile capacity.

Must be an integer in the range of 0-65535.

Default Value: 10.

endpoint-profile *endpoint_profile_name*

Specify name of the endpoint profile.

Must be a string.

priority *profile_priority*

Specify the priority of the profile.

Must be an integer in the range of 0-65535.

Default Value: 1.

uri-scheme *uri_scheme*

Specify the URI scheme.

Must be one of the following:

- **http**: HTTP.
- **https**: HTTPS.

Usage Guidelines Use this command to configure endpoint profile parameters.

profile nf-client nf-type pcf pcf-profile locality service name type endpoint-profile endpoint-name

Configures the endpoint name parameter.

Command Modes Exec > Global Configuration

Syntax Description **endpoint-name** *endpoint_name* **[priority** *node_priority* **| capacity** *node_capacity* **]**

capacity *node_capacity*

Specify the node capacity for the endpoint.

Must be an integer in the range of 0-65535.

endpoint-name *endpoint_name*

Specify name of the endpoint. You can configure the primary, secondary, and tertiary host (IP: Port) within each endpoint for NF server failover handling. The server failover configuration accepts both IPv4 and IPv6 addresses. However, the SMF gives preference to the IPv4 address.

Must be a string.

priority *node_priority*

Specify the node priority for the endpoint.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this configuration to configure the endpoint name parameter.

profile nf-client nf-type pcf pcf-profile locality service name type endpoint-profile endpoint-name primary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **ip-address { { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type pcf pcf-profile locality service name type endpoint-profile endpoint-name secondary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **ip-address { { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type pcf pcf-profile locality service name type endpoint-profile endpoint-name tertiary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **ip-address { { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type pcf pcf-profile locality service name type endpoint-profile version uri-version

Configures the URI version.

Command Modes Exec > Global Configuration > UDM NF-Client Profile Configuration > UDM Profile Configuration > Locality Configuration > UDM Service Name Type Configuration > Endpoint Profile Configuration > Version Configuration > URL Version Configuration

Syntax Description **version uri-version {** *uri_version* **| full-version** *full_version* **}**

full-version *full_version*

Specify the full version in the format *major-version.minor-version.patch-version*.[alpha-*draft-number*]

Must be a string.

uri-version *uri_version*

Specify the URI version.

Must be a string in the pattern v\d.

Usage Guidelines Use this command to configure the URI version information.

profile nf-client nf-type scp scp-profile

Configures SCP profile parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description

```
profile nf-client nf-type scp scp-profile profile_name scp-profile
scp_profile_namescp-profile scp_profile_namelocality locality_name [
prioritypriority_value service name type service_name_type_value responsetimeout
 responsetimeout_value endpoint-profile endpoint-profile_name [ capacity capacity_value
 priority priority_value uri-scheme uri_scheme_value endpoint-name endpoint_name
[ priority priority_value capacity endpoint-profile_name primary ip-address ipv4
 ipv4_address primary ip-address port port_number] ] ]
```

scp-profile *scp_profile_name*

Specify the name of the SCP profile.

Must be a string.

locality *locality_name*

Specify the locality of SCP.

priority*priority_value*

Specify the priority value.

service name type *service_name_type_value*

Specify the service name type.

responsetimeout *responsetimeout_value*

Specify the response timeout value.

endpoint-profile *endpoint-profile_name*

Specify the SCP endpoint profile name.

primary ip-address ipv4 *ipv4_address*

Specify the IPv4 address of the primary endpoint.

primary ip-address port *primary_port_number*

Specify the port number of primary endpoint.

Usage Guidelines Use this command to configure the SCP profile parameters.

profile nf-client nf-type sepp sepp-profile

Configures SEPP profile parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile nf-client nf-type sepp sepp-profile** *profile_name*

sepp-profile *profile_name*

Specify name of the SEPP profile.

Must be a string.

Usage Guidelines Use this command to configure SEPP profile parameters.

profile nf-client nf-type sepp sepp-profile locality

Configures the SEPP profile locality parameter.

Command Modes Exec > Global Configuration (config) > SEPP Profile Configuration (config-sepp-profile-*profile_name*)

Syntax Description **locality** *locality_name* **[priority** *locality_priority* **]**

locality *locality_name*

Specify name of the locality.

Must be a string.

priority *locality_priority*

Specify priority of the locality configuration.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the SEPP profile locality parameter.

profile nf-client nf-type sepp sepp-profile locality service name type

Configures the SEPP service name type parameter.

Command Modes Exec > Global Configuration (config) > SEPP Configuration (config-sepp) > Failure Handling *profile_name* Configuration mode (config-failure-handling-*profile_name*)

Syntax Description **type** *service_name_type* **[responsetimeout** *response_timeout* **]**

responsetimeout *response_timeout*

Specify the response timeout interval in milliseconds.

Must be an integer.

Default Value: 2000.

type *service_name_type*

Specify the service name type.

Must be one of the following:

- **nsmf-pdusession**

Usage Guidelines Use this command to configure the SEPP service name type parameter.

profile nf-client nf-type sepp sepp-profile locality service name type endpoint-profile

Configures endpoint profile parameters.

Command Modes Exec > Global Configuration

Syntax Description **endpoint-profile** *endpoint_profile_name* **{ capacity** *capacity_value* **| priority** *profile_priority* **| api-uri-prefix** *api_uri_prefix* **| api-root** *api_root* **| uri-scheme** *uri_scheme* **}**

api-root *api_root*

Specify the API root.

Must be a string.

api-uri-prefix *api_uri_prefix*

Specify the API URI prefix.

Must be a string.

capacity *capacity_value*

Specify the profile capacity.

Must be an integer in the range of 0-65535.

Default Value: 10.

endpoint-profile *endpoint_profile_name*

Specify name of the endpoint profile.

Must be a string.

priority *profile_priority*

Specify the priority of the profile.

Must be an integer in the range of 0-65535.

Default Value: 1.

uri-scheme *uri_scheme*

Specify the URI scheme.

Must be one of the following:

- **http**: HTTP.
- **https**: HTTPS.

Usage Guidelines Use this command to configure endpoint profile parameters.

profile nf-client nf-type sepp sepp-profile locality service name type endpoint-profile endpoint-name

Configures the endpoint name parameter.

Command Modes Exec > Global Configuration

Syntax Description **endpoint-name** *endpoint_name* **[priority** *node_priority* **| capacity** *node_capacity* **]**

capacity *node_capacity*

Specify the node capacity for the endpoint.

Must be an integer in the range of 0-65535.

endpoint-name *endpoint_name*

Specify name of the endpoint. You can configure the primary, secondary, and tertiary host (IP: Port) within each endpoint for NF server failover handling. The server failover configuration accepts both IPv4 and IPv6 addresses. However, the SMF gives preference to the IPv4 address.

Must be a string.

priority *node_priority*

Specify the node priority for the endpoint.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this configuration to configure the endpoint name parameter.

profile nf-client nf-type sepp sepp-profile locality service name type endpoint-profile endpoint-name primary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **ip-address { { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type sepp sepp-profile locality service name type endpoint-profile endpoint-name secondary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **ip-address { { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type sepp sepp-profile locality service name type endpoint-profile endpoint-name tertiary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **ip-address { { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type sepp sepp-profile locality service name type endpoint-profile version uri-version

Configures the URI version.

Command Modes Exec > Global Configuration > UDM NF-Client Profile Configuration > UDM Profile Configuration > Locality Configuration > UDM Service Name Type Configuration > Endpoint Profile Configuration > Version Configuration > URL Version Configuration

Syntax Description **version uri-version {** *uri_version* **| full-version** *full_version* **}**

full-version *full_version*

Specify the full version in the format *major-version.minor-version.patch-version*.[alpha-*draft-number*]

Must be a string.

uri-version *uri_version*

Specify the URI version.

Must be a string in the pattern v\d.

Usage Guidelines Use this command to configure the URI version information.

profile nf-client nf-type smf smf-profile

Configures SMF profile parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile nf-client nf-type smf smf-profile** *smf_profile_name*

smf-profile *smf_profile_name*

Specify name of the SMF profile.

Must be a string.

Usage Guidelines Use this command to configure the SMF profile parameters.

profile nf-client nf-type smf smf-profile locality

Configures the SMF profile locality parameter.

Command Modes Exec > Global Configuration (config) > SMF Profile Configuration (config-smf-profile-*profile_name*)

Syntax Description **locality** *locality_name* **[priority** *priority* **]**

locality *locality_name*

Specify name of the locality.

Must be a string.

priority *priority*

Specify the priority of the locality configuration.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the SMF profile locality parameter.

profile nf-client nf-type smf smf-profile locality service name type

Configures the SMF service name type parameter.

Command Modes Exec > Global Configuration (config) > SMF Configuration (config-smf) > Failure Handling *profile_name* Configuration mode (config-failure-handling-*profile_name*)

Syntax Description **type** *smf_service_name_type*

responsetimeout *response_timeout*

Specify the response timeout interval in milliseconds.

Must be an integer.

Default Value: 2000.

type *smf_service_name_type*

Specify the service name type.

Must be one of the following:

- **nsmf-pdusession**

Usage Guidelines Use this command to configure the SMF service name type parameter.

profile nf-client nf-type smf smf-profile locality service name type endpoint-profile

Configures endpoint profile parameters.

Command Modes Exec > Global Configuration

Syntax Description **endpoint-profile** *endpoint_profile_name* **{ capacity** *capacity_value* **| priority** *profile_priority* **| api-uri-prefix** *api_uri_prefix* **| api-root** *api_root* **| uri-scheme** *uri_scheme* **}**

api-root *api_root*

Specify the API root.

Must be a string.

api-uri-prefix *api_uri_prefix*

Specify the API URI prefix.

Must be a string.

capacity *capacity_value*

Specify the profile capacity.

Must be an integer in the range of 0-65535.

Default Value: 10.

endpoint-profile *endpoint_profile_name*

Specify name of the endpoint profile.

Must be a string.

priority *profile_priority*

Specify the priority of the profile.

Must be an integer in the range of 0-65535.

Default Value: 1.

uri-scheme *uri_scheme*

Specify the URI scheme.

Must be one of the following:

- **http**: HTTP.
- **https**: HTTPS.

Usage Guidelines Use this command to configure endpoint profile parameters.

profile nf-client nf-type smf smf-profile locality service name type endpoint-profile endpoint-name

Configures the endpoint name parameter.

Command Modes Exec > Global Configuration

Syntax Description **endpoint-name** *endpoint_name* **[priority** *node_priority* **| capacity** *node_capacity* **]**

capacity *node_capacity*

Specify the node capacity for the endpoint.

Must be an integer in the range of 0-65535.

endpoint-name *endpoint_name*

Specify name of the endpoint. You can configure the primary, secondary, and tertiary host (IP: Port) within each endpoint for NF server failover handling. The server failover configuration accepts both IPv4 and IPv6 addresses. However, the SMF gives preference to the IPv4 address.

Must be a string.

priority *node_priority*

Specify the node priority for the endpoint.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this configuration to configure the endpoint name parameter.

profile nf-client nf-type smf smf-profile locality service name type endpoint-profile endpoint-name primary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **`ip-address { { ipv4` *`ipv4_address`* **| ipv6** *`ipv6_address`* **} | port** *`port_number`* **}**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type smf smf-profile locality service name type endpoint-profile endpoint-name secondary ip-address

Configures the endpoint IP address and port number.

Command Modes

Exec > Global Configuration

Syntax Description

ip-address { { ipv4 *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 ***ipv4_address***

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 ***ipv6_address***

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port ***port_number***

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines

Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type smf smf-profile locality service name type endpoint-profile endpoint-name tertiary ip-address

Configures the endpoint IP address and port number.

Command Modes

Exec > Global Configuration

Syntax Description

ip-address { { ipv4 *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 ***ipv4_address***

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type smf smf-profile locality service name type endpoint-profile version uri-version

Configures the URI version.

Command Modes Exec > Global Configuration > UDM NF-Client Profile Configuration > UDM Profile Configuration > Locality Configuration > UDM Service Name Type Configuration > Endpoint Profile Configuration > Version Configuration > URL Version Configuration

Syntax Description **`version uri-version {`** *`uri_version`* **`|`** **`full-version`** *`full_version`* **`}`**

full-version *full_version*

Specify the full version in the format *major-version.minor-version.patch-version*.[alpha-*draft-number*]

Must be a string.

uri-version *uri_version*

Specify the URI version.

Must be a string in the pattern v\d.

Usage Guidelines Use this command to configure the URI version information.

profile nf-client nf-type udm udm-profile

Configures UDM profile parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **`profile nf-client nf-type udm udm-profile`** *`udm_profile_name`*

udm-profile *udm_profile_name*

Specify name of the UDM profile.

Must be a string.

Usage Guidelines Use this command to configure the UDM profile for an NF client.

profile nf-client nf-type udm udm-profile locality

Configures the UDM profile locality parameters.

Command Modes Exec > Global Configuration (config) > UDM Profile Configuration (config-udm-profile-*profile_name*)

Syntax Description **`locality`** *`locality_name`* **`[ priority`** *`priority`* **`]`**

locality *locality_name*

Specify name of the locality.

Must be a string.

priority *priority*

This keyword sets the priority for the locality configuration.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the UDM profile locality parameter.

profile nf-client nf-type udm udm-profile locality service name type

Configures the UDM service name type parameter.

Command Modes Exec > Global Configuration (config) > UDM Configuration (config-udm) > Failure Handling *profile_name* Configuration mode (config-failure-handling-*profile_name*)

Syntax Description **`type`** *`service_name_type`*

responsetimeout *response_timeout*

Specify the response timeout interval in milliseconds.

Must be an integer.

Default Value: 2000.

type *service_name_type*

Specify the UDM service name type.

Must be one of the following:

- **nudm-ee**

- **nudm-pp**
- **nudm-sdm**
- **nudm-ueau**
- **nudm-uecm**

Usage Guidelines Use this command to configure the UDM service name type parameter.

profile nf-client nf-type udm udm-profile locality service name type endpoint-profile

Configures endpoint profile parameters.

Command Modes Exec > Global Configuration

Syntax Description **endpoint-profile** *endpoint_profile_name* **{ capacity** *capacity_value* **| priority** *profile_priority* **| api-uri-prefix** *api_uri_prefix* **| api-root** *api_root* **| uri-scheme** *uri_scheme* **}**

api-root *api_root*

Specify the API root.

Must be a string.

api-uri-prefix *api_uri_prefix*

Specify the API URI prefix.

Must be a string.

capacity *capacity_value*

Specify the profile capacity.

Must be an integer in the range of 0-65535.

Default Value: 10.

endpoint-profile *endpoint_profile_name*

Specify name of the endpoint profile.

Must be a string.

priority *profile_priority*

Specify the priority of the profile.

Must be an integer in the range of 0-65535.

Default Value: 1.

uri-scheme *uri_scheme*

Specify the URI scheme.

Must be one of the following:

- **http**: HTTP.
- **https**: HTTPS.

Usage Guidelines Use this command to configure endpoint profile parameters.

profile nf-client nf-type udm udm-profile locality service name type endpoint-profile endpoint-name

Configures the endpoint name parameter.

Command Modes Exec > Global Configuration

Syntax Description **endpoint-name** *endpoint_name* **[priority** *node_priority* **| capacity** *node_capacity* **]**

capacity *node_capacity*

Specify the node capacity for the endpoint.

Must be an integer in the range of 0-65535.

endpoint-name *endpoint_name*

Specify name of the endpoint. You can configure the primary, secondary, and tertiary host (IP: Port) within each endpoint for NF server failover handling. The server failover configuration accepts both IPv4 and IPv6 addresses. However, the SMF gives preference to the IPv4 address.

Must be a string.

priority *node_priority*

Specify the node priority for the endpoint.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this configuration to configure the endpoint name parameter.

profile nf-client nf-type udm udm-profile locality service name type endpoint-profile endpoint-name primary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **ip-address { { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type udm udm-profile locality service name type endpoint-profile endpoint-name secondary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **ip-address { { ipv4** *ipv4_address* **| ipv6** *ipv6_address* **} | port** *port_number* **}**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type udm udm-profile locality service name type endpoint-profile endpoint-name tertiary ip-address

Configures the endpoint IP address and port number.

Command Modes Exec > Global Configuration

Syntax Description **`ip-address { { ipv4`** *`ipv4_address`* **`| ipv6`** *`ipv6_address`* **`} | port`** *`port_number`* **`}`**

ipv4 *ipv4_address*

Specify the IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *port_number*

Specify the port number.

Must be an integer in the range of 0-65535.

Usage Guidelines Use this command to configure the endpoint IP address and port number.

profile nf-client nf-type udm udm-profile locality service name type endpoint-profile version uri-version

Configures the URI version.

Command Modes Exec > Global Configuration > UDM NF-Client Profile Configuration > UDM Profile Configuration > Locality Configuration > UDM Service Name Type Configuration > Endpoint Profile Configuration > Version Configuration > URL Version Configuration

Syntax Description **`version uri-version {`** *`uri_version`* **`| full-version`** *`full_version`* **`}`**

full-version *full_version*

Specify the full version in the format *major-version*.*minor-version*.*patch-version*.[alpha-*draft-number*]

Must be a string.

uri-version *uri_version*

Specify the URI version.

Must be a string in the pattern v\d.

Usage Guidelines Use this command to configure the URI version information.

profile nf-client-failure nf-type amf

Configures the AMF Profile Failure Handling parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **`profile nf-client-failure nf-type amf`**

Usage Guidelines Use this command to configure the AMF Profile Failure Handling parameters. The CLI prompt changes to the AMF Configuration mode (config-amf).

profile nf-client-failure nf-type amf profile failure-handling

Configures the AMF failure handling template parameter.

Command Modes Exec > Global Configuration (config) > AMF Configuration (config-amf)

Syntax Description **`profile failure-handling`** *`fh_template_name`*

failure-handling *fh_template_name*

Specify name of the AMF failure handling template.

Must be a string.

Usage Guidelines Use this command to configure the AMF failure handling template parameter. The CLI prompt changes to the Failure Handling <profile_name> Configuration mode (config-failure-handling-<profile_name>).

profile nf-client-failure nf-type amf profile failure-handling service name type

Configures the AMF service name type parameter.

Command Modes Exec > Global Configuration (config) > AMF Configuration (config-amf) > Failure Handling *profile_name* Configuration mode (config-failure-handling-*profile_name*)

Syntax Description **`service name type`** *`amf_service_name_type`*

responsetimeout *response_timeout*

Specify the response timeout interval in milliseconds.

Must be an integer.

Default Value: 2000.

type *amf_service_name_type*

Specify the AMF service name type.

Must be one of the following:

- **namf-comm**
- **namf-evts**
- **namf-loc**
- **namf-mt**

Usage Guidelines Use this command to configure AMF service name type parameter. The CLI prompt changes to the Failure Handling Service Name Type Configuration mode (config-type-<service_name_type>)

profile nf-client-failure nf-type amf profile failure-handling service name type message type

Configures the AMF message type parameters.

Command Modes Exec > Global Configuration (config) > AMF Configuration (config-amf) > Failure Handling *profile_name* Configuration mode (config-failure-handling-*profile_name*) > Failure Handling Service Name Type Configuration (config-type-*service_name_type*)

Syntax Description **`message type`** *`amf_message_type`*

type *amf_message_type*

Specify the AMF message type.

Must be one of the following:

- **AmfCommCreateUeContext**
- **AmfCommEBIAssignment**
- **AmfCommN1N2MessageTransfer**
- **AmfCommSMStatusChangeNotify**
- **AmfCommUeContextTransfer**
- **AmfCommUeContextTransferUpdate**

Usage Guidelines Use this command to configure the AMF message type parameters.

profile nf-client-failure nf-type amf profile failure-handling service name type message type status-code httpv2

Configures HTTPv2 status codes.

Command Modes Exec > Global Configuration

Syntax Description **`status-code httpv2`** *`range`* **`{ code`** *`code_value`* **`| retry`** *`retry_value`* **`| action`** *`action`* **`}`**

action *action*

Specify the action.

Must be one of the following:

- **continue**: Specify to continue the session without any retry. The retry count configuration is invalid with this action.
- **retry-and-continue**: Specify to retry as per the configured retry count and continue the session.
- **retry-and-ignore**
- **retry-and-terminate**: Specify to retry as per the configured retry count and terminate the session in case all retry fails.
- **terminate**: Specify to terminate the session without any retry. Retry count configuration is invalid with this action.

code *code_value*

Specify the code, or a range of status codes separated by either - (hyphen) or , (comma).

Must be an integer.

-Or-

Must be a string.

retransmit-interval *retransmit_interval*

Specify the retransmit interval in milliseconds.

Must be an integer.

retransmit *retransmit*

Specify the maximum number of retransmits.

Must be an integer in the range of 1-10.

retry *retry_value*

Specify the number of times the NF service must retry before proceeding with the action.

Must be an integer in the range of 1-10.

Usage Guidelines Use this command to configure HTTPv2 status codes.

profile nf-client-failure nf-type ausf

Configures AUSF profile failure handling parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **`profile nf-client-failure nf-type ausf`**

Usage Guidelines Use this command to configure AUSF failure handling parameters. The CLI prompt changes to the AUSF Configuration mode (config-ausf).

profile nf-client-failure nf-type ausf profile failure-handling

Configures the AUSF failure handling template parameters.

Command Modes Exec > Global Configuration (config) > AUSF Configuration (config-ausf)

Syntax Description **`profile failure-handling`** *`fh_template_name`*

failure-handling *fh_template_name*

Specify name of the AUSF failure handling template.

Must be a string.

Usage Guidelines Use this command to configure the AUSF failure handling template parameters. The CLI prompt changes to the Failure Handling Profile Configuration mode (config-failure-handling-<profile_name>).

profile nf-client-failure nf-type ausf profile failure-handling service name type

Configures the AUSF service name type.

Command Modes Exec > Global Configuration (config) > AUSF Configuration (config-ausf) > Failure Handling *profile_name* Configuration mode (config-failure-handling-*profile_name*)

Syntax Description **`service name type`** *`ausf_service_name_type`*

responsetimeout *response_timeout*

Specify the response timeout interval in milliseconds.

Must be an integer.

Default Value: 2000.

type *ausf_service_name_type*

Specify the AUSF service name type.

Must be one of the following:

- **nausf-auth**

Usage Guidelines Use this command to configure the AUSF service name type.

profile nf-client-failure nf-type ausf profile failure-handling service name type message type

Configures the AUSF message type parameters.

Command Modes Exec > Global Configuration (config) > AUSF Configuration (config-ausf) > Failure Handling *profile_name* Configuration mode (config-failure-handling-*profile_name*) > Failure Handling Service Name Type Configuration (config-type-*service_name_type*)

Syntax Description **message type** *ausf_message_type*

type *ausf_message_type*

Specify the AUSF message type.

Must be one of the following:

- **AusfAuthenticationCfm**
- **AusfAuthenticationReq**

Usage Guidelines Use this command to configure the AUSF message type parameters.

profile nf-client-failure nf-type ausf profile failure-handling service name type message type status-code httpv2

Configures HTTPv2 status codes.

Command Modes Exec > Global Configuration

Syntax Description **status-code httpv2** *range* **{ code** *code_value* **| retry** *retry_value* **| action** *action* **}**

action *action*

Specify the action.

Must be one of the following:

- **continue**: Specify to continue the session without any retry. The retry count configuration is invalid with this action.
- **retry-and-continue**: Specify to retry as per the configured retry count and continue the session.
- **retry-and-ignore**
- **retry-and-terminate**: Specify to retry as per the configured retry count and terminate the session in case all retry fails.
- **terminate**: Specify to terminate the session without any retry. Retry count configuration is invalid with this action.

code *code_value*

Specify the code, or a range of status codes separated by either - (hyphen) or , (comma).

Must be an integer.

-Or-

Must be a string.

retransmit-interval *retransmit_interval*

Specify the retransmit interval in milliseconds.

Must be an integer.

retransmit *retransmit*

Specify the maximum number of retransmits.

Must be an integer in the range of 1-10.

retry *retry_value*

Specify the number of times the NF service must retry before proceeding with the action.

Must be an integer in the range of 1-10.

Usage Guidelines Use this command to configure HTTPv2 status codes.

profile nf-client-failure nf-type chf

Configures CHF profile failure handling parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description

```
profile nf-client-failure nf-type chf
```

Usage Guidelines Use this command to configure CHF failure handling parameters. The CLI prompt changes to the CHF Configuration mode (config-chf).

profile nf-client-failure nf-type chf profile failure-handling

Configures the CHF failure handling template parameters.

Command Modes Exec > Global Configuration (config) > CHF Configuration (config-chf)

Syntax Description **`profile failure-handling`** *`fh_template_name`*

failure-handling *fh_template_name*

Specify name of the CHF failure handling template.

Must be a string.

Usage Guidelines Use this command to configure the CHF failure handling template for CHF profile.

profile nf-client-failure nf-type chf profile failure-handling service name type

Configures the CHF service name type parameters.

Command Modes Exec > Global Configuration

Syntax Description **`type`** *`chf_service_name_type`*

responsetimeout *response_timeout*

Specify the response timeout interval in milliseconds.

Must be an integer.

Default Value: 2000.

type *chf_service_name_type*

Specify the CHF service name type.

Must be one of the following:

- **nchf-convergedcharging**
- **nchf-spendinglimitcontrol**

Usage Guidelines Use this command to configure the CHF service name type parameters.

profile nf-client-failure nf-type chf profile failure-handling service name type message type

Configures the CHF message type parameters.

Command Modes Exec > Global Configuration (config) > CHF Configuration (config-chf) > Failure Handling *profile_name* Configuration mode (config-failure-handling-*profile_name*) > Failure Handling Service Name Type Configuration (config-type-*service_name_type*)

Syntax Description **message type** *chf_message_type*

type *chf_message_type*

Specify the CHF message type.

Must be one of the following:

- **ChfConvergedchargingCreate**
- **ChfConvergedchargingDelete**
- **ChfConvergedchargingUpdate**
- **ChfSpendingLimitContolSubscribe**
- **ChfSpendingLimitContolUnSubscribe**

Usage Guidelines Use this command to configure the CHF message type parameters.

profile nf-client-failure nf-type chf profile failure-handling service name type message type status-code httpv2

Configures HTTPv2 status codes.

Command Modes Exec > Global Configuration

Syntax Description **status-code httpv2** *range* **{ code** *code_value* **| retry** *retry_value* **| action** *action* **}**

action *action*

Specify the action.

Must be one of the following:

- **continue**: Specify to continue the session without any retry. The retry count configuration is invalid with this action.
- **retry-and-continue**: Specify to retry as per the configured retry count and continue the session.
- **retry-and-ignore**

- **retry-and-terminate**: Specify to retry as per the configured retry count and terminate the session in case all retry fails.
- **terminate**: Specify to terminate the session without any retry. Retry count configuration is invalid with this action.

code *code_value*

Specify the code, or a range of status codes separated by either - (hyphen) or , (comma).

Must be an integer.

-Or-

Must be a string.

retransmit-interval *retransmit_interval*

Specify the retransmit interval in milliseconds.

Must be an integer.

retransmit *retransmit*

Specify the maximum number of retransmits.

Must be an integer in the range of 1-10.

retry *retry_value*

Specify the number of times the NF service must retry before proceeding with the action.

Must be an integer in the range of 1-10.

Usage Guidelines Use this command to configure HTTPv2 status codes.

profile nf-client-failure nf-type eir

Configures EIR profile failure handling parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description `profile nf-client-failure nf-type eir`

Usage Guidelines Use this command to configure EIR failure handling parameters. The CLI prompt changes to the EIR Configuration mode (config-eir).

profile nf-client-failure nf-type eir profile failure-handling

Configures the EIR failure handling template parameters.

Command Modes Exec > Global Configuration (config) > EIR Configuration (config-eir)

Syntax Description **`profile failure-handling`** *`fh_template_name`*

failure-handling *fh_template_name*

Specify name of the EIR failure handling template.

Must be a string.

Usage Guidelines Use this command to configure the EIR failure handling template for EIR profile.

profile nf-client-failure nf-type eir profile failure-handling service name type

Configures the EIR service name type parameters.

Command Modes Exec > Global Configuration

Syntax Description **`type`** *`eir_service_name_type`*

responsetimeout *response_timeout*

Specify the response timeout interval in milliseconds.

Must be an integer.

Default Value: 2000.

type *eir_service_name_type*

Specify the EIR service name type.

Must be one of the following:

- **n5g-eir-eic**

Usage Guidelines Use this command to configure the EIR service name type parameters.

profile nf-client-failure nf-type eir profile failure-handling service name type message type

Specify the EIR message type parameters.

Command Modes Exec > Global Configuration (config) > EIR Configuration (config-eir) > Failure Handling *profile_name* Configuration mode (config-failure-handling-*profile_name*) > Failure Handling Service Name Type Configuration (config-type-*service_name_type*)

Syntax Description **`message type`** *`eir_message_type`*

type *eir_message_type*

Specify the EIR message type.

Must be one of the following:

- **EirCheckEquipmentIdentity**

Usage Guidelines Use this command to configure the EIR message type parameters.

profile nf-client-failure nf-type eir profile failure-handling service name type message type status-code httpv2

Configures HTTPv2 status codes.

Command Modes Exec > Global Configuration

Syntax Description **`status-code httpv2`** *`range`* **`{ code`** *`code_value`* **`| retry`** *`retry_value`* **`| action`** *`action`* **`}`**

action *action*

Specify the action.

Must be one of the following:

- **continue**: Specify to continue the session without any retry. The retry count configuration is invalid with this action.
- **retry-and-continue**: Specify to retry as per the configured retry count and continue the session.
- **retry-and-ignore**
- **retry-and-terminate**: Specify to retry as per the configured retry count and terminate the session in case all retry fails.
- **terminate**: Specify to terminate the session without any retry. Retry count configuration is invalid with this action.

code *code_value*

Specify the code, or a range of status codes separated by either - (hyphen) or , (comma).

Must be an integer.

-Or-

Must be a string.

retransmit-interval *retransmit_interval*

Specify the retransmit interval in milliseconds.

Must be an integer.

retransmit *retransmit*

Specify the maximum number of retransmits.

Must be an integer in the range of 1-10.

retry *retry_value*

Specify the number of times the NF service must retry before proceeding with the action.

Must be an integer in the range of 1-10.

Usage Guidelines Use this command to configure HTTPv2 status codes.

profile nf-client-failure nf-type nrf

Configures NRF profile failure handling parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **`profile nf-client-failure nf-type nrf`**

Usage Guidelines Use this command to configure NRF failure handling parameters. The CLI prompt changes to the NRF Configuration mode (config-nrf).

profile nf-client-failure nf-type nrf profile failure-handling

Configures the NRF failure handling template parameters.

Command Modes Exec > Global Configuration (config) > NRF Configuration (config-nrf)

Syntax Description **`profile failure-handling`** *`fh_template_name`*

failure-handling *fh_template_name*

Specify name of the NRF failure handling template.

Must be a string.

Usage Guidelines Use this command to configure the failure handling template parameters.

profile nf-client-failure nf-type nrf profile failure-handling service name type

Configures NRF service name type parameters.

Command Modes Exec > Global Configuration

Syntax Description **type** *nrf_service_name_type* **responsetimeout** *response_timeout*

responsetimeout *response_timeout*

Specify the timeout interval in milliseconds.

Must be an integer.

Default Value: 2000.

nrf_service_name_type

Specify the NRF service name type.

Must be one of the following:

- **nrf-nfm**

Usage Guidelines Use this command to configure the NRF service name type parameters.

profile nf-client-failure nf-type nrf profile failure-handling service name type message type

Configures NRF message type parameters.

Command Modes Exec > Global Configuration (config) > NRF Configuration (config-nrf) > Failure Handling *profile_name* Configuration mode (config-failure-handling-*profile_name*) > Failure Handling Service Name Type Configuration (config-type-*service_name_type*)

Syntax Description **type** *message_type* **failover-enabled { false | true } re-registration-enabled { false | true }**

failover-enabled { false | true }

Specify whether to enable or disable failover to next NRF.

Must be one of the following:

- **false**
- **true**

Default Value: true.

re-registration-enabled { false | true }

Specify whether to enable or disable re-registration.

Must be one of the following:

- **false**
- **true**

Default Value: true.

type *message_type*

Specify the message type.

Must be one of the following:

- **Heartbeat**
- **NFUpdate**
- **NRFRegistration**

Usage Guidelines Use this command to configure the NRF message type parameters.

profile nf-client-failure nf-type nrf profile failure-handling service name type message type status-code httpv2

Configures HTTPv2 status code.

Command Modes Exec > Global Configuration

Syntax Description `status-code httpv2 { code code_value | action action }`

action *action*

Specify the action.

Must be one of the following:

- **retry-next**
- **retry**

code *code_value*

Specify the code value. Ranges of status codes must be separated by either hyphen (-) or comma (,).

Must be an integer.

-Or-

Must be a string.

Usage Guidelines Use this command to configure HTTPv2 status codes.

profile nf-client-failure nf-type pcf

Configures PCF profile failure handling parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **`profile nf-client-failure nf-type pcf`**

Usage Guidelines Use this command to configure PCF failure handling parameters. The CLI prompt changes to the PCF Configuration mode (config-pcf).

profile nf-client-failure nf-type pcf profile failure-handling

Configures the PCF failure handling template parameters.

Command Modes Exec > Global Configuration (config) > PCF Configuration (config-pcf)

Syntax Description **`profile failure-handling`** *`fh_template_name`*

failure-handling *fh_template_name*

Specify name of the PCF failure handling template.

Must be a string.

Usage Guidelines Use this command to configure the failure handling template for PCF profile.

profile nf-client-failure nf-type pcf profile failure-handling service name type

Configures PCF service name type.

Command Modes Exec > Global Configuration

Syntax Description **`type`** *`pcf_service_name_type`*

responsetimeout *response_timeout*

Specify the response timeout interval in milliseconds.

Must be an integer.

Default Value: 2000.

pcf_service_name_type

Specify the PCF service name type.

Must be one of the following:

- **npcf-am-policy-control**
- **npcf-bdtpolicycontrol**
- **npcf-eventexposure**

- **npcf-policyauthorization**
- **npcf-smpolicycontrol**
- **npcf-ue-policy-control**

Usage Guidelines Use this command to configure the PCF service name type.

profile nf-client-failure nf-type pcf profile failure-handling service name type message type

Configures the PCF message type parameters.

Command Modes Exec > Global Configuration (config) > PCF Configuration (config-pcf) > Failure Handling *profile_name* Configuration mode (config-failure-handling-*profile_name*) > Failure Handling Service Name Type Configuration (config-type-*service_name_type*)

Syntax Description **message type** *pcf_message_type*

type *pcf_message_type*

Specify the PCF message type.

Must be one of the following:

- **PcfAmfPolicyControlCreate**
- **PcfAmfPolicyControlDelete**
- **PcfSmpolicycontrolCreate**
- **PcfSmpolicycontrolDelete**
- **PcfSmpolicycontrolUpdate**

Usage Guidelines Use this command to configure the PCF message type parameters.

profile nf-client-failure nf-type pcf profile failure-handling service name type message type status-code httpv2

Configures HTTPv2 status codes.

Command Modes Exec > Global Configuration

Syntax Description **status-code httpv2** *range* **{ code** *code_value* **| retry** *retry_value* **| action** *action* **}**

action *action*

Specify the action.

Must be one of the following:

- **continue**: Specify to continue the session without any retry. The retry count configuration is invalid with this action.
- **retry-and-continue**: Specify to retry as per the configured retry count and continue the session.
- **retry-and-ignore**
- **retry-and-terminate**: Specify to retry as per the configured retry count and terminate the session in case all retry fails.
- **terminate**: Specify to terminate the session without any retry. Retry count configuration is invalid with this action.

code *code_value*

Specify the code, or a range of status codes separated by either - (hyphen) or , (comma).

Must be an integer.

-Or-

Must be a string.

retransmit-interval *retransmit_interval*

Specify the retransmit interval in milliseconds.

Must be an integer.

retransmit *retransmit*

Specify the maximum number of retransmits.

Must be an integer in the range of 1-10.

retry *retry_value*

Specify the number of times the NF service must retry before proceeding with the action.

Must be an integer in the range of 1-10.

Usage Guidelines Use this command to configure HTTPv2 status codes.

profile nf-client-failure nf-type scp

Configures the failure handling for NF clients using specific service and error handling parameters.

Command Modes Exec > Global Configuration (config) > NF Client Failure Configuration (config-nf-client-failure-*nf_type*)

Syntax Description **profile nf-client-failure nf-type** *nf_type* **[profile failure-handling** *failure_handlr_profile_name* **[service-name-type** *service_name_type* **| message type** *message_type* **{ status-code** *status_code* **| retry** *retry_count* **| action { continue**

```
 | retry-and-continue | retry-and-fallback | retry-and-ignore |
retry-and-terminate | terminate } } } ] ] ]
```

profile nf-client-failure nf-type ***nf_type*** **[profile failure-handling** ***failure_handlr_profile_name*** **[service-name-type** ***service_name_type*** **| message type** ***message_type*** **{ status-code** ***status_code*** **| retry** ***retry_count*** **| action { continue | retry-and-continue | retry-and-fallback | retry-and-ignore | retry-and-terminate | terminate } } }]]]**

- **profile nf-client-failure nf-type** *nf_type* —Specify the NF client failure configuration.
- **profile failure-handling** *failure_handling_profile_name* —Specify the failure handling profile name.
- **service-name-type** *service_name_type* —Specify the the service name and type.
- **message type** *message_type* —Specify the the message type.
- **status-code** *status_code* —Specify the status code for http2 error or DNS failure.
- **retry** *retry_count* —Specify the retry count.
- **action { continue | retry-and-continue | retry-and-fallback | retry-and-ignore | retry-and-terminate | terminate }**—Specify any action from the preceding options for retry.

Usage Guidelines Use this command to configure failure handling and its related action.

profile nf-client-failure nf-type sepp

Configures SEPP profile failure handling parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **`profile nf-client-failure nf-type sepp`**

Usage Guidelines Use this command to configure SEPP failure handling parameters. The CLI prompt changes to the SEPP Configuration mode (config-epp).

profile nf-client-failure nf-type sepp profile failure-handling

Configures the SEPP failure handling template parameters.

Command Modes Exec > Global Configuration (config) > SEPP Configuration (config-sepp)

Syntax Description **`profile failure-handling`** *`fh_template_name`*

failure-handling *fh_template_name*

Specify name of the SEPP failure handling template.

Must be a string.

Usage Guidelines Use this command to configure the SEPP failure handling template for SEPP profile.

profile nf-client-failure nf-type sepp profile failure-handling service name type

Configures the SEPP service name type.

Command Modes

Exec > Global Configuration (config) > SEPP Configuration (config-sepp) > Failure Handling *profile_name* Configuration mode (config-failure-handling-*profile_name*)

Syntax Description

`service name type` *`sepp_service_name_type`* **`[ responsetimeout`** *`response_timeout`* **`]`**

responsetimeout *response_timeout*

Specify the response timeout interval in milliseconds.

Must be an integer.

Default Value: 2000.

type *sepp_service_name_type*

Specify the SEPP service name type.

Must be one of the following:

- **nsmf-pdusession**

Usage Guidelines

Use this command to configure the SEPP service name type.

profile nf-client-failure nf-type sepp profile failure-handling service name type message type

Configures the SEPP message type parameters.

Command Modes

Exec > Global Configuration (config) > SEPP Configuration (config-sepp) > Failure Handling *profile_name* Configuration mode (config-failure-handling-*profile_name*) > Failure Handling Service Name Type Configuration (config-type-*service_name_type*)

Syntax Description

`message type` *`sepp_message_type`*

type *sepp_message_type*

Specify the SEPP message type.

Must be one of the following:

- **HsmfPduSessionNotify**
- **HsmfPduSessionUpdate**
- **VsmfPduSessionCreate**

- **VsmfPduSessionRelease**
- **VsmfPduSessionUpdate**

Usage Guidelines Use this command to configure the SEPP message type parameters.

profile nf-client-failure nf-type sepp profile failure-handling service name type message type status-code httpv2

Configures HTTPv2 status codes.

Command Modes Exec > Global Configuration

Syntax Description **status-code httpv2** *range* **{ code** *code_value* **| retry** *retry_value* **| action** *action* **}**

action *action*

Specify the action.

Must be one of the following:

- **continue**: Specify to continue the session without any retry. The retry count configuration is invalid with this action.
- **retry-and-continue**: Specify to retry as per the configured retry count and continue the session.
- **retry-and-ignore**
- **retry-and-terminate**: Specify to retry as per the configured retry count and terminate the session in case all retry fails.
- **terminate**: Specify to terminate the session without any retry. Retry count configuration is invalid with this action.

code *code_value*

Specify the code, or a range of status codes separated by either - (hyphen) or , (comma).

Must be an integer.

-Or-

Must be a string.

retransmit-interval *retransmit_interval*

Specify the retransmit interval in milliseconds.

Must be an integer.

retransmit *retransmit*

Specify the maximum number of retransmits.

Must be an integer in the range of 1-10.

retry *retry_value*

Specify the number of times the NF service must retry before proceeding with the action.

Must be an integer in the range of 1-10.

Usage Guidelines Use this command to configure HTTPv2 status codes.

profile nf-client-failure nf-type smf

Configures SMF profile failure handling parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **`profile nf-client-failure nf-type smf`**

Usage Guidelines Use this command to configure SMF failure handling parameters. The CLI prompt changes to the SMF Configuration mode (config-smf).

profile nf-client-failure nf-type smf profile failure-handling

Configures the SMF failure handling template parameters.

Command Modes Exec > Global Configuration (config) > SMF Configuration (config-smf)

Syntax Description **`profile failure-handling`** *`fh_template_name`*

failure-handling *fh_template_name*

Specify name of the SMF failure handling template.

Must be a string.

Usage Guidelines Use this command to configure the SMF failure handling template for SMF profile.

profile nf-client-failure nf-type smf profile failure-handling service name type

Configures the SMF service name type.

Command Modes Exec > Global Configuration (config) > SMF Configuration (config-smf) > Failure Handling *profile_name* Configuration mode (config-failure-handling-*profile_name*)

Syntax Description **`service name type`** *`smf_service_name_type`*

responsetimeout *response_timeout*

Specify the response timeout interval in milliseconds.

Must be an integer.

Default Value: 2000.

type *smf_service_name_type*

Specify the SMF service name type.

Must be one of the following:

- **nsmf-pdusession**

Usage Guidelines Use this command to configure the SMF service name type.

profile nf-client-failure nf-type smf profile failure-handling service name type message type status-code httpv2

Configures HTTPv2 status codes.

Command Modes Exec > Global Configuration

Syntax Description **`status-code httpv2`** *`range`* **`{ code`** *`code_value`* **`| retry`** *`retry_value`* **`| action`** *`action`* **`}`**

action *action*

Specify the action.

Must be one of the following:

- **continue**: Specify to continue the session without any retry. The retry count configuration is invalid with this action.
- **retry-and-continue**: Specify to retry as per the configured retry count and continue the session.
- **retry-and-ignore**
- **retry-and-terminate**: Specify to retry as per the configured retry count and terminate the session in case all retry fails.
- **terminate**: Specify to terminate the session without any retry. Retry count configuration is invalid with this action.

code *code_value*

Specify the code, or a range of status codes separated by either - (hyphen) or , (comma).

Must be an integer.

-Or-

Must be a string.

retransmit-interval *retransmit_interval*

Specify the retransmit interval in milliseconds.

Must be an integer.

retransmit *retransmit*

Specify the maximum number of retransmits.

Must be an integer in the range of 1-10.

retry *retry_value*

Specify the number of times the NF service must retry before proceeding with the action.

Must be an integer in the range of 1-10.

Usage Guidelines Use this command to configure HTTPv2 status codes.

profile nf-client-failure nf-type udm

Configures UDM profile failure handling parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description `profile nf-client-failure nf-type udm`

Usage Guidelines Use this command to configure UDM failure handling parameters. The CLI prompt changes to the UDM Configuration mode (config-udm).

profile nf-client-failure nf-type udm profile failure-handling

Configures the UDM failure handling template parameters.

Command Modes Exec > Global Configuration (config) > UDM Configuration (config-udm)

Syntax Description `profile failure-handling` *fh_template_name*

failure-handling *fh_template_name*

Specify name of the UDM failure handling template.

Must be a string.

Usage Guidelines Use this command to configure the failure handling template for UDM profile.

profile nf-client-failure nf-type udm profile failure-handling service name type

Configures UDM service name type.

Command Modes Exec > Global Configuration (config) > UDM Configuration (config-udm) > Failure Handling *profile_name* Configuration mode (config-failure-handling-*profile_name*)

Syntax Description **type** *udm_service_name_type* **[responsetimeout** *response_timeout* **]**

responsetimeout *response_timeout*

Specify the response timeout interval in milliseconds.

Must be an integer.

Default Value: 2000.

udm_service_name_type

Specify the UDM service name type.

Must be one of the following:

- **nudm-ee**
- **nudm-pp**
- **nudm-sdm**
- **nudm-ueau**
- **nudm-uecm**

Usage Guidelines Use this command to configure the UDM service name type.

profile nf-client-failure nf-type udm profile failure-handling service name type message type

Configures the UDM message type parameters.

Command Modes Exec > Global Configuration (config) > UDM Configuration (config-udm) > Failure Handling *profile_name* Configuration mode (config-failure-handling-*profile_name*) > Failure Handling Service Name Type Configuration (config-type-*service_name_type*)

Syntax Description **message type** *udm_message_type*

type *udm_message_type*

Specify the UDM message type.

Must be one of the following:

- **UdmDeRegistrationReq**
- **UdmRegistrationReq**
- **UdmSdmGetUESMSubscriptionData**
- **UdmSdmSubscribeToNotification**
- **UdmSdmUnsubscribeToNotification**
- **UdmSubscriptionReq**
- **UdmUecmRegisterSMF**
- **UdmUecmUnregisterSMF**
- **UdmUnSubscriptionReq**

Usage Guidelines Use this command to configure the UDM message type parameters.

profile nf-client-failure nf-type udm profile failure-handling service name type message type status-code httpv2

Configures HTTPv2 status codes.

Command Modes Exec > Global Configuration

Syntax Description **status-code httpv2** *range* **{ code** *code_value* **| retry** *retry_value* **| action** *action* **}**

action *action*

Specify the action.

Must be one of the following:

- **continue**: Specify to continue the session without any retry. The retry count configuration is invalid with this action.
- **retry-and-continue**: Specify to retry as per the configured retry count and continue the session.
- **retry-and-ignore**
- **retry-and-terminate**: Specify to retry as per the configured retry count and terminate the session in case all retry fails.
- **terminate**: Specify to terminate the session without any retry. Retry count configuration is invalid with this action.

code *code_value*

Specify the code, or a range of status codes separated by either - (hyphen) or , (comma).

Must be an integer.

-Or-

Must be a string.

retransmit-interval *retransmit_interval*

Specify the retransmit interval in milliseconds.

Must be an integer.

retransmit *retransmit*

Specify the maximum number of retransmits.

Must be an integer in the range of 1-10.

retry *retry_value*

Specify the number of times the NF service must retry before proceeding with the action.

Must be an integer in the range of 1-10.

Usage Guidelines Use this command to configure HTTPv2 status codes.

profile nf-pair nf-type

Configures the NF client pair type parameter.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile nf-pair nf-type** *nf_type* **[[limit** *max_discovery_profiles* **] [max-payload-size** *max_payload_size* **] [nrf-discovery-group** *group_name* **]]**

limit *max_discovery_profiles*

Specify the maximum number of discovery profiles that NRF can send.

Must be an integer in the range of 1-1000.

Default Value: 10.

max-payload-size *max_payload_size*

Specify the maximum payload size of the discovery response.

Must be an integer in the range of 124-2000.

Default Value: 124.

nf-type *nf_type*

Specify the NF client pair type.

Must be one of the following:

- **5G_EIR**

- **AF**
- **AMF**
- **AUSF**
- **BSF**
- **CHF**
- **GMLC**
- **LMF**
- **N3IWF**
- **NEF**
- **NRF**
- **NSSF**
- **NWDAF**
- **PCF**
- **SEPP**
- **SMF**
- **SMSF**
- **UDM**
- **UDR**
- **UDSF**
- **UPF**

nrf-discovery-group *group_name*

Specify name of the NRF discovery group.

Must be a string.

Usage Guidelines Configures NF client pair parameters. Use this command to configure the NF client pair type parameter.

profile nf-pair nf-type cache invalidation true

Configures the invalidation cache for "true" case.

Command Modes Exec > Global Configuration (config) > NF Type Configuration (config-nf-type-*nf_type*)

Syntax Description **`cache invalidation { false | true [ timeout`** *`timeout_duration`* **`] }`**

timeout *timeout_duration*

Specify the invalidation cache timeout duration in milliseconds.

Must be an integer.

Default Value: 0.

true

True condition.

Usage Guidelines Use this command to configure the true case parameters for invaldation cache.

profile nf-pair nf-type locality

Configures client locality parameter.

Command Modes Exec > Global Configuration (config) > NF Type Configuration (config-nf-type-*nf_type*)

Syntax Description **locality { client** *locality_name* **| geo-server** *locality_name* **| preferred-server** *locality_name* **}**

client *locality_name*

Specify the Client Locality information.

Must be a string.

geo-server *locality_name*

Specify the Geo Service Locality information.

Must be a string.

preferred-server *locality_name*

Specify the preferred server locality information.

Must be a string.

Usage Guidelines Use this command to configure the client locality parameter.

profile overload

Configures overload protection profile.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile overload** *profile_name*

overload *profile_name*

Specify name of the overload protection profile.

Must be a string.

Usage Guidelines Use this command to configure overload protection profile. The CLI prompt changes to the Overload Profile Configuration mode (config-overload-<profile_name>)

You can configure a maximum of one element with this command.

profile overload node-level

Configures Overload profile's node-level parameters.

Command Modes Exec > Global Configuration (config) > Overload Profile Configuration (config-overload-*profile_name*)

Syntax Description **node-level**

Usage Guidelines Use this command to configure the overload profile's node-level parameters. The CLI prompt chnages to the Node-level Configuration mode (config-node-level).

profile overload node-level advertise

Configures the advertising action.

Command Modes Exec > Global Configuration (config) > Overload Profile Configuration (config-overload-*profile_name*) > Node Level Configuration (config-node-level)

Syntax Description **advertise { [interval** *advertising_interval* **] [change-factor** *change_factor* **] [validity-period** *validity_period* **] }**

change-factor *change_factor*

Specify the minimum change between current OCI and last indicated OCI, after which only advertising should happen.

Must be an integer in the range of 1-20.

Default Value: 5.

interval *advertising_interval*

Specify the advertising interval in seconds.

Must be an integer in the range of 0-3600.

Default Value: 300.

validity-period *validity_period*

Specify the validity period of the advertised OCI value in seconds.

Must be an integer in the range of 1-3600.

Default Value: 600.

Usage Guidelines Use this command to configure the advertising action.

profile overload node-level interface

Configures the list of interfaces.

Command Modes Exec > Global Configuration (config) > Overload Profile Configuration (config-overload-*profile_name*) > Node Level Configuration (config-node-level)

Syntax Description **`interface`** *`interface_type`* **`[ overloaded-action`** *`overloaded_action`* **`]`**

interface *interface_type*

Specify the type of the interface.

Must be one of the following:

- **gtpc**

overloaded-action *overloaded_action*

Specify the action on the interface in overloaded state.

Must be one of the following:

- **advertise**

Usage Guidelines Use this command to configure the list of interfaces.

profile overload node-level reduction-metric

Configures the percentage reduction metric configuration.

Command Modes Exec > Global Configuration (config) > Overload Profile Configuration (config-overload-*profile_name*) > Node Level Configuration (config-node-level)

Syntax Description **`reduction-metric { [ minimum`** *`minimum_reduction`* **`] [ maximum`** *`maximum_reduction`* **`] }`**

maximum *maximum_reduction*

Specify the percentage of reduction in tandem with tolerance maximum configuration. Maximum reduction must be greater than minimum reduction.

Must be an integer in the range of 1-100.

Default Value: 100.

minimum *minimum_reduction*

Specify the percentage of reduction in tandem with tolerance minimum configuration. Minimum reduction must be lesser than maximum reduction.

Must be an integer in the range of 1-100.

Default Value: 10.

Usage Guidelines Use this command to configure the Percentage Reduction Metric configuration.

profile overload node-level tolerance

Configures the percentage tolerance level configuration.

Command Modes Exec > Global Configuration (config) > Overload Profile Configuration (config-overload-*profile_name*) > Node-level Configuration (config-node-level)

Syntax Description **tolerance { [minimum** *minimum_tolerance* **] [maximum** *maximum_tolerance* **] }**

maximum *maximum_tolerance*

Specify the tolerance level above which the system is considered to be in self-protection state. Maximum tolerance must be greater than minimum tolerance.

Must be an integer in the range of 1-100.

Default Value: 95.

minimum *minimum_tolerance*

Specify the tolerance level below which the system is considered to be in normal state. Minimum tolerance must be lesser than maximum tolerance.

Must be an integer in the range of 1-100.

Default Value: 80.

Usage Guidelines Use this command to configure the percentage tolerance level configuration.

profile overload overload-exclude-profile

Configures excluding profiles for overload scenarios.

Command Modes Exec > Global Configuration (config) > Overload Profile Configuration (config-overload-*profile_name*)

Syntax Description **overload-exclude-profile self-protection** *exclude_profile_name* **peer-overload** *exclude_profile_name*

peer-overload *exclude_profile_name*

Specify to exclude profile for peer overload.

Must be a string.

self-protection *exclude_profile_name*

Specify to exclude profile for self protection.

Must be a string.

Usage Guidelines Use this command to configure excluding profiles for overload scenarios.

profile overload peer-level interface

Configures the list of interfaces.

Command Modes Exec > Global Configuration

Syntax Description **`interface type`** *`interface_type`*

type *interface_type*

Specify the interface type.

Must be one of the following:

- **gtpc**

Usage Guidelines Use this command to configure the list of interfaces.

profile overload peer-level interface action throttle

Configures the throttling action.

Command Modes Exec > Global Configuration

Syntax Description **`throttle duration`** *`throttling_duration`* **`threshold`** *`max_messages`*

duration *throttling_duration*

Specify the duration for which messages must be throttled.

Must be an integer.

threshold *max_messages*

Specify the maximum percentage of messages to be allowed during throttling.

Must be an integer in the range of 1-100.

Usage Guidelines Use this command to configure the throttling action.

profile overload peer-level message-prioritization

Configures peer-level message prioritization parameter.

Command Modes Exec > Global Configuration

Syntax Description **peer-level message-prioritization group1** *message_priority* **group2** *message_priority* **group3** *message_priority* **group4** *message_priority*

group1 *message_priority*

Specify the message prioritization for group 1.

Must be an integer in the range of 0-100.

Default Value: 50.

group2 *message_priority*

Specify the message prioritization for group 2.

Must be an integer in the range of 0-100.

Default Value: 50.

Usage Guidelines Use this command to configure the peer-level message prioritization parameters. The total of all weights must be 100. That is, "group1 + group2 + group3 + group4 = 100".

profile overload-exclude

Configures the list of exclude overloads.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile overload-exclude** *exclude_profile_name* **[[arp-list** *arp_list* **] [dnn-list** *dnn_list* **] [procedure-list** *procedures_list* **] [qi5-list** *qi5_list* **]]**

arp-list *arp_list*

Specify the Allocation and Retention Priorities to be excluded from throttling decisions.

You can configure a maximum of eight elements with this keyword.

Must be an integer in the range of 1-15.

dnn-list *dnn_list*

Specify the DNNs to be excluded from throttling decisions.

You can configure a maximum of three elements with this keyword.

Must be a string.

overload-exclude *exclude_profile_name*

Specify the name of the exclude profile.

Must be a string.

procedure-list *procedures_list*

Specify the procedures to be excluded from throttling decisions. Applicable only for Self-Protection.

Must be one of the following:

- **session-delete**

qi5-list *qi5_list*

Specify the 5G QoS Identifiers to be excluded from throttling decisions.

You can configure a maximum of eight elements with this keyword.

Must be an integer in the range of 1-15.

Usage Guidelines Use this command to configure the list of exclude overloads.

profile overload-exclude message-priority

Configures the message priorities to be excluded from throttling decisions.

Command Modes Exec > Global Configuration (config) > Overload Exclude Profile Configuration (config-overload-exclude-*profile_name*)

Syntax Description **`message-priority`** *`interface_type`* **`upto`** *`message_priority_upto`*

message-priority *interface_type*

Specify the interface type.

Must be one of the following:

- **n4**
- **n7**
- **n10**
- **n11**
- **n16**
- **n40**
- **s5**

upto *message_priority_upto*

Specify the message priority up to which must be excluded from throttling decisions.

Must be an integer in the range of 0–31 for SBA interface and 0–15 for GTPC and PFCP interfaces.

Usage Guidelines Use this command to configure the message priorities to be excluded from throttling decisions.

profile overload-exclude procedure-list

Configures the procedures to be performed on messages as part of the overload exclude process.

Command Modes Exec > Global Configuration (config) > Overload Exclude Profile Configuration (config-overload-exclude-*profile_name*)

Syntax Description **`procedure-list [ session-delete | new-call | xnho | modify | chf-reauth | inter-rat-ho | intra-rat-ho | imexit-nw | imexit-ue | usar ]`**

procedure-list

Specify the procedure type to be performed.

Must be one of the following:

- **session-delete**: Session delete procedure. This is the default procedure.
- **new-call**: New call procedure.
- **xnho**: XNHO procedure.
- **modify**: Modify procedure.
- **chf-reauth**: CHF Reauth procedure.
- **inter-rat-ho**: Inter-RAT HO procedure.
- **intra-rat-ho**: Intra RAT HO procedure.
- **imexit-nw**: IM Exit NW Initiated procedure.
- **imexit-ue**: IM Exit UE Initiated procedure.
- **usar**: USAR procedure.

Usage Guidelines Use this command to configure the procedures to be performed on the messages as part of the overload exclude process.

profile pcscf

Configures the P-CSCF profile.

Command Modes Exec > Global Configuration (config)

Syntax Description **`profile pcscf`** *`profile_name`*

pcscf *profile_name*

Specify name of the P-CSCF profile.

Must be a string.

Usage Guidelines Use this command to configure the P-CSCF profile. The CLI prompt changes to the P-CSCF Profile Configuration mode (config-pcscf-<profile_name>).

profile pcscf fqdn

Configures the P-CSCF server's Fully Qualified Domain Name (FQDN).

Command Modes Exec > Global Configuration (config) > P-CSCF Profile Configuration (config-pcscf-*profile_name*)

Syntax Description **fqdn** *fqdn*

fqdn *fqdn*

Specify the P-CSCF server's FQDN.

Must be a string.

Usage Guidelines Use this command to configure the P-CSCF server's FQDN.

profile pcscf pcscf-selection

Configures the P-CSCF server selection algorithm.

Command Modes Exec > Global Configuration (config) > P-CSCF Profile Configuration (config-pcscf-*profile_name*)

Syntax Description **pcscf-selection** *algorithm*

pcscf-selection *algorithm*

Specify the P-CSCF server selection algorithm.

Must be one of the following:

- **round-robin**

Default Value: round-robin.

Usage Guidelines Use this command to configure the P-CSCF server selection method.

profile pcscf pcscf-restoration trigger

Configures SMF to reselect active P-CSCF addresses for UE.

Command Modes Exec > Global Configuration (config) > P-CSCF Profile Configuration (config-pcscf-*profile_name*)

Syntax Description `pcscf-restoration trigger [ UDM ] [ action [ mark-down ] ]`

pcscf-restoration trigger [UDM]

Enables UDM triggered P-CSCF restoration and reselection. **trigger [UDM]** specifies that the restoration configuration is triggered by UDM.

[action [mark-down]]

It is optional and if configured, it can only have **[mark-down]** as the option.

Usage Guidelines Use this command to configure the P-CSCF to select active P-CSCF addresses post a P-CSCF address failure.

profile pcscf v4-list

Configures the P-CSCF IPv4 server details in the P-CSCF profile.

Command Modes Exec > Global Configuration (config) > P-CSCF Profile Configuration (config-pcscf-*profile_name*)

Syntax Description `v4-list`

Usage Guidelines Use this command to configure the P-CSCF IPv4 server details in the P-CSCF profile. The CLI prompt changes to the V4 List Configuration mode (config-v4-list).

profile pcscf v4-list list-entry

Configures the P-CSCF IPv4 server list entries.

Command Modes Exec > Global Configuration (config) > P-CSCF Profile Configuration (config-pcscf-*profile_name*) > V4 List Configuration (config-v4-list)

Syntax Description `precedence precedence_number`

precedence *precedence_number*

Specify the precedence number for P-CSCF IPv4 server configuration.

Must be an integer in the range of 1-64.

Usage Guidelines Configures the P-CSCF IPv4 server details in the P-CSCF profile. Use this command to configure the P-CSCF IPv4 server list entries.

profile pcscf v4-list list-entry primary

Configures the IPv4 address of the primary P-CSCF server.

Command Modes Exec > Global Configuration

Syntax Description **primary ipv4** *ipv4_address*

ipv4 *ipv4_address*

Specify the IPv4 address of the primary P-CSCF server in dotted-decimal notation.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure the IPv4 address of the primary P-CSCF server.

Example

The following command configures the primary P-CSCF server with IPv4 address 30.22.21.44:

```
primary ipv4 30.22.21.44
```

profile pcscf v4-list list-entry secondary

Configures the IPv4 address of the secondary P-CSCF server.

Command Modes Exec > Global Configuration

Syntax Description **secondary ipv4** *ipv4_address*

ipv4 *ipv4_address*

Specify the IPv4 address of the secondary P-CSCF server in dotted-decimal notation.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this to command configure the IPv4 address of the secondary P-CSCF server.

Example

The following command configures the secondary P-CSCF server with IPv4 address 30.22.21.44:

```
secondary ipv4 30.22.21.44
```

profile pcscf v4-list list-entry tertiary

Configures the IPv4 address of the tertiary P-CSCF server.

Command Modes Exec > Global Configuration

Syntax Description **tertiary ipv4** *ipv4_address*

ipv4 *ipv4_address*

Specify the IPv4 address of the tertiary P-CSCF server in dotted-decimal notation.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this to command configure the IPv4 address of the tertiary P-CSCF server.

Example

The following command configures the tertiary P-CSCF server with IPv4 address 30.22.21.44:

```
tertiary ipv4 30.22.21.44
```

profile pcscf v4v6-list

Configures the P-CSCF IPv4v6 server details.

Command Modes Exec > Global Configuration (config) > P-CSCF Profile Configuration (config-pcscf-*profile_name*)

Syntax Description **`v4v6-list`**

Usage Guidelines Use this command to configure the P-CSCF IPv4v6 server details in the P-CSCF profile. The CLI prompt changes to the v4v6 List Configuration Mode (config-v4v6-list).

profile pcscf v4v6-list list-entry

Configures the P-CSCF IPv4v6 server list entries.

Command Modes Exec > Global Configuration (config) > P-CSCF Profile Configuration (config-pcscf-*profile_name*) > v4v6 Configuration Mode (config-v4v6-list)

Syntax Description **`precedence`** *`precedence_number`*

precedence *precedence_number*

Specify the precedence of entries in the P-CSCF IPv4v6 server list.

Must be an integer in the range of 1-64.

Usage Guidelines Use this command to configure the P-CSCF IPv4v6 server list entries.

profile pcscf v4v6-list list-entry primary

Configures the IPv4v6 address of the primary P-CSCF server.

Command Modes Exec > Global Configuration

Syntax Description **primary ipv4** *ipv4_address* **ipv6** *ipv6_address*

ipv4 *ipv4_address*

Specify the IPv4 address of the primary P-CSCF server in dotted-decimal notation.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address of the primary P-CSCF server in colon-separated hexadecimal notation.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure the IPv4v6 address of the primary P-CSCF server.

Example

The following command configures the primary P-CSCF server with IPv4 address as 30.22.21.44 and IPv6 address as 123:345:456::6578:

```
primary ipv4 30.22.21.44 ipv6 123:345:456::6578
```

profile pcscf v4v6-list list-entry secondary

Configures the IPv4v6 address of the secondary P-CSCF server.

Command Modes Exec > Global Configuration

Syntax Description **secondary { [ipv4** *ipv4_address* **] [ipv6** *ipv6_address* **] }**

ipv4 *ipv4_address*

Specify the IPv4 address of the secondary P-CSCF server in dotted-decimal notation.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address of the secondary P-CSCF server in colon-separated hexadecimal notation.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure the IPv4v6 address of the secondary P-CSCF server.

Example

The following command configures the secondary P-CSCF server with IPv4 address as 30.22.21.44 and IPv6 address as 123:345:456::6578:

```
secondary ipv4 30.22.21.44 ipv6 123:345:456::6578
```

profile pcscf v4v6-list list-entry tertiary

Configures the IPv4v6 address of the tertiary P-CSCF server.

Command Modes Exec > Global Configuration

Syntax Description **`tertiary { [ ipv4`** *`ipv4_address`* **`] [ ipv6`** *`ipv6_address`* **`] }`**

ipv4 *ipv4_address*

Specify the IPv4 address of the tertiary P-CSCF server in dotted-decimal notation.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

ipv6 *ipv6_address*

Specify the IPv6 address of the tertiary P-CSCF server in colon-separated hexadecimal notation.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure the IPv4v6 address of the tertiary P-CSCF server.

Example

The following command configures the tertiary P-CSCF server with IPv4 address as 30.22.21.44 and IPv6 address as 123:345:456::6578:

```
tertiary ipv4 30.22.21.44 ipv6 123:345:456::6578
```

profile pcscf v6-list

Configures the P-CSCF IPv6 server details.

Command Modes Exec > Global Configuration (config) > P-CSCF Profile Configuration (config-pcscf-*profile_name*)

Syntax Description **`v6-list`**

Usage Guidelines Use this command to configure the P-CSCF IPv6 server details in the P-CSCF profile. The CLI prompt changes to the V6 List Configuration mode (config-v6-list).

profile pcscf v6-list list-entry

Configures the P-CSCF IPv6 server list entries.

Command Modes Exec > Global Configuration (config) > P-CSCF Profile Configuration (config-pcscf-*profile_name*) > V6 List Configuration (config-v6-list)

Syntax Description **precedence** *precedence_level*

precedence *precedence_level*

Specify the precedence of entries in the P-CSCF IPv6 server list.

Must be an integer in the range of 1-64.

Usage Guidelines Use this command to configure the P-CSCF IPv6 server list entries.

profile pcscf v6-list list-entry primary

Configures the IPv6 address of the primary P-CSCF server.

Command Modes Exec > Global Configuration (config) > P-CSCF Profile Configuration (config-pcscf-*profile_name*) > V6 List Configuration (config-v6-list)

Syntax Description **primary ipv6** *ipv6_address*

ipv6 *ipv6_address*

Specify the IPv6 address of the primary P-CSCF server in colon-separated hexadecimal notation.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure the IPv6 address of the primary P-CSCF server.

Example

The following command configures the primary P-CSCF server with IPv6 address 123:345:456::6578:

```
primary ipv6 123:345:456::6578
```

profile pcscf v6-list list-entry secondary

Configures the IPv6 address of the secondary P-CSCF server.

Command Modes Exec > Global Configuration

Syntax Description **secondary ipv6** *ipv6_address*

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure the IPv6 address of the secondary P-CSCF server.

Example

The following command configures the secondary P-CSCF server with IPv6 address 123:345:456::6578:

```
secondary ipv6 123:345:456::6578
```

profile pcscf v6-list list-entry tertiary

Configures the IPv6 address of the tertiary P-CSCF server.

Command Modes Exec > Global Configuration

Syntax Description **tertiary ipv6** *ipv6_address*

ipv6 *ipv6_address*

Specify the IPv6 address.

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure the IPv6 address of the tertiary P-CSCF server.

Example

The following command configures the tertiary P-CSCF server with the IPv6 address 123:345:456::6578:

```
tertiary ipv6 123:345:456::6578
```

profile ppd

Configures the Paging Policy Differentiation (PPD) profile configuration.

Command Modes Exec > Global Configuration (config)

Syntax Description **ppd** *ppd_profile_name* **[fqi** *5qi_priority_levels* **]**

fqi *5qi_priority_levels*

Specify the range of 5qi priority levels.

Must be an integer.

-Or-

Must be a string.

ppd *ppd_profile_name*

Specify name of the PPD profile.

Must be a string.

Usage Guidelines Use this command to configure the PPD profile configuration.

profile ppd dscp-list

Configures the Differentiated Services Code Point (DSCP) values.

Command Modes Exec > Global Configuration (config) > PPD Configuration (config-ppd-*profile_name*)

Syntax Description **dscp** *dscp_value* **[ppi** *ppi_value* **]**

dscp *dscp_value*

Specify the DSCP value.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ppi *ppi_value*

Specify the Paging Policy Indicator (PPI) value.

Must be an integer in the range of 0-7.

Usage Guidelines Use this command to configure the DSCP values.

profile qos

Configures the QoS profile configuration.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile qos** *qos_profile_name* **message-priority-profile** *profile_name* **[[priority** *qi_priority* **] [qi5** *qos_id* **]]arp-priority-level** *arp_value* **message-priority-profile** *profile_name*

priority *qi_priority*

Specify the 5QI priority level.

Must be an integer in the range of 1-127.

profile qos *qos_profile_name*

Specify name of the QoS profile.

Must be a string.

message-priority-profile *profile_name*

Associates message priority profile to QoS profile.

qi5 *qos_id*

Specify the ID for the authorized QoS parameters.

Must be an integer in the range of 0-255.

arp-priority-level *arp_value* **message-priority-profile** *profile_name* : Message priority profile associated to ARP. Specify the ARP value in the range between 1 to 255.

The Message priority profile associated to QCI or ARP or QoS profile, or message priority profile associated to WPS are negotiated to find the one which has the better priority.

vplmn-qos-negotiation { false | true }

Specify whether to enable or disable configured QoS to negotiate for defalut flow.

Must be one of the following:

- **false**
- **true**

Default Value: false.

Usage Guidelines Use this command to configure the QoS profile configuration.

profile qos ambr

Configures the Aggregate Maximum Bit Rate (AMBR).

Command Modes Exec > Global Configuration (config) > QoS Profile Configuration (config-qos-*profile_name*)

Syntax Description **`ambr { ul`** *`ambr_uplink_threshold`* **`| dl`** *`ambr_downlink_threshold`* **`}`**

dl *ambr_downlink_threshold*

Specify the AMBR downlink threshold in bps, Kbps, Mbps, Gbps, or Tbps.

Must be a string in the pattern '[0-9]+.[0-9]+ (bps|Kbps|Mbps|Gbps|Tbps)'.

ul *ambr_uplink_threshold*

Specify the AMBR uplink threshold in bps, Kbps, Mbps, Gbps, or Tbps.

Must be a string in the pattern '[0-9]+.[0-9]+ (bps|Kbps|Mbps|Gbps|Tbps)'.

Usage Guidelines Use this command to configure the AMBR.

profile qos arp

Configures the Allocation and Retention Priority (ARP) for the service data.

Command Modes Exec > Global Configuration (config) > QoS Profile Configuration (config-qos-*profile_name*)

Syntax Description **arp priority-level** *priority_level* **[preempt-cap** *preempttion_capability* **] [preempt-vuln** *preemption_vulnerability* **]**

preempt-cap *preempttion_capability*

Specify the preemption capability.

Must be one of the following:

- **MAY_PREEMPT**
- **NOT_PREEMPT**

Default Value: MAY_PREEMPT.

preempt-vuln *preemption_vulnerability*

Specify the preemption vulnerability.

Must be one of the following:

- **NOT_PREEMPTABLE**
- **PREEMPTABLE**

Default Value: NOT_PREEMPTABLE.

priority-level *priority_level*

Specify the priority level.

Must be an integer in the range of 1-15.

Usage Guidelines Use this command to configure the ARP for the service data.

profile qos dscp-map qi5

Configures the standard 5QI value.

Command Modes Exec > Global Configuration (config) > QoS Profile Configuration (config-qos-*profile_name*)

Syntax Description **dscp-map qi5** *standard_qci*

qi5 *standard_qci*

Specify the standard QCI value.

Must be an integer in the range of 1-255.

Usage Guidelines Configures the 5QI to DSCP-Marking mapping. Use this command to configure the standard 5QI value.

profile qos dscp-map qi5 arp-priority-level

Configures the ARP priority level.

Command Modes Exec > Global Configuration (config) > QoS Profile Configuration (config-qos-*profile_name*)

Syntax Description **arp priority-level** *arp_priority_level*

Command Modes Exec > Global Configuration (config) > SGW QoS Profile Configuration (config-sgw-qos-profile-*profile_name*)

Syntax Description **dscp-map operator-defined-qci** *operator_defined_qci* **[gbr arp-priority-level** *arp_priority_level* **]**

arp-priority-level *arp_priority_level*

Specify the ARP priority level.

Must be an integer in the range of 1-255.

Usage Guidelines Configures the type of the QCI to GBR. Use this command to configure the ARP priority level.

profile qos dscp-map qi5 arp-priority-level dscp-info

Configures the Differentiated Services Code Point (DSCP) type.

Command Modes Exec > Global Configuration

Syntax Description **dscp-info type** *dscp_type*

dl-encap-copy-inner

Specify to copy the inner DSCP to outer.

dl-encap-dscp-marking *dscp_marking*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encaps-header

Specify the DSCP value be applied to encaps header.

dl-ud-dscp *dscp_marking*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-ud-encap-copy-inner

Specify to copy the inner DSCP to outer.

dl-ud-encap-dscp *dscp_marking*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

encsp-header

Specify the DSCP value to be applied to encaps header.

type *dscp_type*

Specify the DCSP type.

Must be one of the following:

- **downlink**
- **uplink**

user-datagram1

Specify the DSCP value be applied to user datagram.

Usage Guidelines Configures the type of the QCI to GBR. Use this command to configure the DSCP type.

profile qos dscp-map qi5 arp-priority-level dscp-info user-datagram

Configures the Differentiated Services Code Point (DCSP) value to be applied to user datagram.

Command Modes Exec > Global Configuration

Syntax Description **`user-datagram ul-uD-dscp-marking`** *`dscp_marking`*

ul-uD-dscp-marking *dscp_marking*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure the DCSP value to be applied to user datagram.

profile qos dscp-map qi5 dscp-info

Configures the Differentiated Services Code Point (DSCP) type.

Command Modes Exec > Global Configuration

Syntax Description **`dscp-info type`** *`dscp_type`*

dl-encap-copy-inner

Specify to copy the inner DSCP to outer.

dl-encap-dscp-marking *dscp_marking*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encaps-header

Specify the DSCP value be applied to encaps header.

dl-ud-dscp *dscp_marking*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-ud-encap-copy-inner

Specify to copy the inner DSCP to outer.

dl-ud-encap-dscp *dscp_marking*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

encsp-header

Specify the DSCP value to be applied to encaps header.

type *dscp_type*

Specify the DCSP type.

Must be one of the following:

- **downlink**
- **uplink**

user-datagram1

Specify the DSCP value be applied to user datagram.

Usage Guidelines Configures the type of the QCI to GBR. Use this command to configure the DSCP type.

profile qos dscp-map qi5 dscp-info user-datagram

Configures the Differentiated Services Code Point (DCSP) value to be applied to user datagram.

Command Modes Exec > Global Configuration

Syntax Description **`user-datagram ul-uD-dscp-marking`** *`dscp_marking`*

ul-uD-dscp-marking *dscp_marking*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure the DCSP value to be applied to user datagram.

profile qos max

Configures the maximum data burst volume.

Command Modes Exec > Global Configuration (config) > QoS Profile Configuration (config-qos-*profile_name*)

Syntax Description **`max data-burst`** *`max_data_burst_volume`*

data-burst *max_data_burst_volume*

Specify the maximum data burst volume.

Must be an integer in the range of 1-4095.

Usage Guidelines Use this command to configure the maximum data burst volume.

profile qos qos-enforcement

Configures flow-level QoS enforcement configuration.

Command Modes Exec > Global Configuration (config) > QoS Profile Configuration (config-qos-*profile_name*)

Syntax Description **`qos-enforcement flow-level`**

flow-level

Specify flow-level QoS enforcement.

Usage Guidelines Use this command to configure flow-level QoS enforcement configuration.

profile qos qosflow qi5

Configures Qos flow parameters for 5QI/ARP values.

Command Modes Exec > Global Configuration (config)

Syntax Description

```
qosflow qi5  qci_value
      arp-priority-level arp_value
            message-priority-profile profile_name
     message-priority-profile profile_name
```

qosflow qi5 *qci_value*

Specify the QCI value.

Must be an integer in the range of 1-255.

Note If there is no message priority profile associated to a default bearer/flow qci/arp, then message priority value is considered from message priority profile that is associated to a QoS profile for the IMS and emergency calls. When a dedicated bearer/flow gets created, message priority is considered from message priority profile associated to the qci/arp depending on the configuration.

Usage Guidelines Use this command to configure the Qos flow parameters for 5QI/ARP values.

profile qos qosflow qi5 arp-priority-level

Configures the ARP priority level.

Command Modes Exec > Global Configuration (config)

Syntax Description **`arp-priority-level arp-value`** *`arp_value`*

arp-value *arp_value*

Specify the ARP value.

Must be an integer in the range of 1-255.

Usage Guidelines Use this command to configure the the ARP priority level.

profile qos qosflow qi5 arp-priority-level dscp-info downlink encaps-header

Configures the DSCP value to be applied to encaps header.

Command Modes Exec > Global Configuration (config)

Syntax Description **encaps-header** *dscp_for_encaps_header*

dscp-marking *dscp_for_packets*

Specify the DSCP value to be applied to packets. For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

encap-copy-inner

Specify to copy inner DSCP to outer.

encap-copy-outer

Specify to copy outer DSCP to inner.

encaps-header *dscp_for_encaps_header*

Specify the DSCP value to be applied to encaps header.

Usage Guidelines Configures downlink/uplink DSCP information. Use this command to configure the DSCP value to be applied to encaps header.

profile qos qosflow qi5 arp-priority-level dscp-info downlink user-datagram

Configures the DSCP value to be applied to user datagram.

Command Modes Exec > Global Configuration (config)

Syntax Description **user-datagram ud-dscp** *dscp_for_packets* **ud-encaps-header** *dscp_for_encaps_header*

dscp-marking *dscp_for_packets*

Specify the DSCP value to be applied to packets. For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

encap-copy-inner

Specify to copy inner DSCP to outer.

encap-copy-outer

Specify to copy outer DSCP to inner.

ud-dscp *dscp_for_packets*

Specify the DSCP value to be applied to packets. For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ud-encaps-header *dscp_for_encaps_header*

Specify the DSCP value to be applied to encaps header.

Usage Guidelines Use this command to the DSCP value to be applied to user datagram.

profile qos qosflow qi5 arp-priority-level dscp-info uplink encaps-header

Configures the DSCP value to be applied to encaps header.

Command Modes Exec > Global Configuration (config)

Syntax Description **encaps-header** *dscp_for_encaps_header*

dscp-marking *dscp_for_packets*

Specify the DSCP value to be applied to packets. For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

encap-copy-inner

Specify to copy inner DSCP to outer.

encap-copy-outer

Specify to copy outer DSCP to inner.

encaps-header *dscp_for_encaps_header*

Specify the DSCP value to be applied to encaps header.

Usage Guidelines Configures downlink/uplink DSCP information. Use this command to configure the DSCP value to be applied to encaps header.

profile qos qosflow qi5 arp-priority-level dscp-info uplink user-datagram

Configures the DSCP value to be applied to user datagram.

Command Modes Exec > Global Configuration (config)

Syntax Description **`user-datagram ud-dscp`** *`dscp_for_packets`* **`ud-encaps-header`** *`dscp_for_encaps_header`*

dscp-marking *dscp_for_packets*

Specify the DSCP value to be applied to packets. For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

encap-copy-inner

Specify to copy inner DSCP to outer.

encap-copy-outer

Specify to copy outer DSCP to inner.

ud-dscp *dscp_for_packets*

Specify the DSCP value to be applied to packets. For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ud-encaps-header *dscp_for_encaps_header*

Specify the DSCP value to be applied to encaps header.

Usage Guidelines Use this command to the DSCP value to be applied to user datagram.

profile qos qosflow qi5 arp-priority-level flow-parameter gfbr

Configures the Guaranted Bit Rate (GFBR).

Command Modes Exec > Global Configuration (config)

Syntax Description **flow-parameter gfbr { [ul** *gfbr_uplink_threshold* **] [dl** *gfbr_downlink_threshold* **] }**

dl *gfbr_downlink_threshold*

Specify the GFBR downlink threshold.

Must be a string in the pattern '[0-9]+.[0-9]+ (bps|Kbps|Mbps|Gbps|Tbps)'.

ul *gfbr_uplink_threshold*

Specify the GFBR uplink threshold.

Must be a string in the pattern '[0-9]+.[0-9]+ (bps|Kbps|Mbps|Gbps|Tbps)'.

Usage Guidelines Use this command to configure the GFBR.

profile qos qosflow qi5 arp-priority-level flow-parameter mfbr

Configures the Maximum Bit Rate (MFBR).

Command Modes Exec > Global Configuration (config)

Syntax Description **flow-parameter mfbr { [ul** *mfbr_uplink_threshold* **] [dl** *mfbr_downlink_threshold* **] }**

dl *mfbr_downlink_threshold*

Specify the MFBR downlink threshold.

Must be a string in the pattern '[0-9]+.[0-9]+ (bps|Kbps|Mbps|Gbps|Tbps)'.

ul *mfbr_uplink_threshold*

Specify the MFBR uplink threshold.

Must be a string in the pattern '[0-9]+.[0-9]+ (bps|Kbps|Mbps|Gbps|Tbps)'.

Usage Guidelines Use this command to configure the MFBR.

profile qos qosflow qi5 dscp-info downlink encaps-header

Configures the DSCP value to be applied to encaps header.

Command Modes Exec > Global Configuration (config)

Syntax Description **encaps-header** *dscp_for_encaps_header*

dscp-marking *dscp_for_packets*

Specify the DSCP value to be applied to packets. For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

encap-copy-inner

Specify to copy inner DSCP to outer.

encap-copy-outer

Specify to copy outer DSCP to inner.

encaps-header *dscp_for_encaps_header*

Specify the DSCP value to be applied to encaps header.

Usage Guidelines Configures downlink/uplink DSCP information. Use this command to configure the DSCP value to be applied to encaps header.

profile qos qosflow qi5 dscp-info downlink user-datagram

Configures the DSCP value to be applied to user datagram.

Command Modes Exec > Global Configuration (config)

Syntax Description **`user-datagram ud-dscp`** *`dscp_for_packets`* **`ud-encaps-header`** *`dscp_for_encaps_header`*

dscp-marking *dscp_for_packets*

Specify the DSCP value to be applied to packets. For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

encap-copy-inner

Specify to copy inner DSCP to outer.

encap-copy-outer

Specify to copy outer DSCP to inner.

ud-dscp *dscp_for_packets*

Specify the DSCP value to be applied to packets. For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ud-encaps-header *dscp_for_encaps_header*

Specify the DSCP value to be applied to encaps header.

Usage Guidelines Use this command to the DSCP value to be applied to user datagram.

profile qos qosflow qi5 dscp-info uplink encaps-header

Configures the DSCP value to be applied to encaps header.

Command Modes Exec > Global Configuration (config)

Syntax Description **encaps-header** *dscp_for_encaps_header*

dscp-marking *dscp_for_packets*

Specify the DSCP value to be applied to packets. For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

encap-copy-inner

Specify to copy inner DSCP to outer.

encap-copy-outer

Specify to copy outer DSCP to inner.

encaps-header *dscp_for_encaps_header*

Specify the DSCP value to be applied to encaps header.

Usage Guidelines Configures downlink/uplink DSCP information. Use this command to configure the DSCP value to be applied to encaps header.

profile qos qosflow qi5 dscp-info uplink user-datagram

Configures the DSCP value to be applied to user datagram.

Command Modes Exec > Global Configuration (config)

Syntax Description **user-datagram ud-dscp** *dscp_for_packets* **ud-encaps-header** *dscp_for_encaps_header*

dscp-marking *dscp_for_packets*

Specify the DSCP value to be applied to packets. For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

encap-copy-inner

Specify to copy inner DSCP to outer.

encap-copy-outer

Specify to copy outer DSCP to inner.

ud-dscp *dscp_for_packets*

Specify the DSCP value to be applied to packets. For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ud-encaps-header *dscp_for_encaps_header*

Specify the DSCP value to be applied to encaps header.

Usage Guidelines Use this command to the DSCP value to be applied to user datagram.

profile qos qosflow qi5 flow-parameter gfbr

Configures the Guaranted Bit Rate (GFBR).

Command Modes Exec > Global Configuration (config)

Syntax Description **`flow-parameter gfbr { [ ul`** *`gfbr_uplink_threshold`* **`] [ dl`** *`gfbr_downlink_threshold`* **`] }`**

dl *gfbr_downlink_threshold*

Specify the GFBR downlink threshold.

Must be a string in the pattern '[0-9]+.[0-9]+ (bps|Kbps|Mbps|Gbps|Tbps)'.

ul *gfbr_uplink_threshold*

Specify the GFBR uplink threshold.

Must be a string in the pattern '[0-9]+.[0-9]+ (bps|Kbps|Mbps|Gbps|Tbps)'.

Usage Guidelines Use this command to configure the GFBR.

profile qos qosflow qi5 flow-parameter mfbr

Configures the Maximum Bit Rate (MFBR).

Command Modes Exec > Global Configuration (config)

Syntax Description **`flow-parameter mfbr { [ ul`** *`mfbr_uplink_threshold`* **`] [ dl`** *`mfbr_downlink_threshold`* **`] }`**

dl *mfbr_downlink_threshold*

Specify the MFBR downlink threshold.

Must be a string in the pattern '[0-9]+.[0-9]+ (bps|Kbps|Mbps|Gbps|Tbps)'.

ul *mfbr_uplink_threshold*

Specify the MFBR uplink threshold.

Must be a string in the pattern '[0-9]+.[0-9]+ (bps|Kbps|Mbps|Gbps|Tbps)'.

Usage Guidelines Use this command to configure the MFBR.

profile radius

Configures RADIUS client profile.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile radius [[algorithm** *server_selection_algorithm* **] [deadtime** *deadtime_interval* **] [enable-packet-dump] [dictionary** *dictionary_name* **] [max-retry** *max_retries* **] [timeout** *timeout_interval* **]]**

algorithm *server_selection_algorithm*

Specify the algorithm for selecting the RADIUS server. Default Value: first-server.

Must be one of the following:

- **first-server**
- **round-robin**

deadtime *deadtime_interval*

Specify the time interval, in minutes, between the RADIUS server being marked unreachable and connection can be re-attempted.

Must be an integer in the range of 0-65535.

enable-packet-dump

Specify to enable packet dump.

dictionary

Specify the dictionary name as ISE.

max_retries

Specify the maximum number of times the system will attempt retry with the RADIUS server.

Must be an integer in the range of 0-65535.

timeout_interval

Specify the time interval to elapse for a response from the RADIUS server before re-transmitting.

Must be an integer in the range of 1-65535.

Usage Guidelines Use this command to configure RADIUS client profile. The CLI prompt changes to the RADIUS Configuration mode (config-radius).

profile radius accounting

Configures RADIUS accounting parameters.

Command Modes Exec > Global Configuration

Syntax Description **accounting** *options*

algorithm *server_selection_algorithm*

Specify the algorithm for selecting the RADIUS server. Default Value: first-server.

Must be one of the following:

- **first-server**
- **round-robin**

deadtime *deadtime_interval*

Specify the time interval, in minutes, between the RADIUS server being marked unreachable and connection can be re-attempted.

Must be an integer in the range of 0-65535.

max_retries

Specify the maximum number of times the system will attempt retry with the RADIUS server.

Must be an integer in the range of 0-65535.

timeout_interval

Specify the time interval to elapse for a response from the RADIUS server before re-transmitting.

Must be an integer in the range of 1-65535.

Usage Guidelines Use this command to configure the RADIUS accounting parameters.

profile radius accounting attribute

Configures RADIUS identification parameters.

Command Modes Exec > Global Configuration (config) > RADIUS Configuration (config-radius)

Syntax Description **attribute { nas-identifier** *nas_id* **| nas-ip** *aaa_nas_ipv4_address* **}**

nas-identifier *nas_identifier*

Specify the attribute name by which the system will be identified in Auth or Accounting Request messages.

Must be a string in the fmtstr pattern. For information on the fmtstr pattern, see the *Input Pattern Types* chapter.

nas-identifier *nas_identifier*

Specify the attribute name by which the system will be identified in Auth or Accounting Request messages.

Must be a string in the fmtstr pattern. For information on the fmtstr pattern, see the *Input Pattern Types* chapter.

nas-ip *aaa_nas_ipv4_address*

Specify the AAA NAS IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure RADIUS identification parameters.

profile radius accounting attribute instance

Configures instance configuration parameters.

Command Modes Exec > Global Configuration > RADIUS Configuration (config-radius)

Syntax Description **`attribute instance`** *`instance_id`* **`nas-ip`** *`aaa_nas_ipv4_address`*

instance *instance_id*

Specify the instance ID.

Must be an integer in the range of 1-8.

nas-identifier *nas_identifier*

Specify the attribute name by which the system will be identified in Auth or Accounting Request messages.

Must be a string in the fmtstr pattern. For information on the fmtstr pattern, see the *Input Pattern Types* chapter.

instance *instance_id*

Specify the instance ID.

Must be an integer in the range of 1-8.

nas-identifier *nas_identifier*

Specify the attribute name by which the system will be identified in Auth or Accounting Request messages.

Must be a string in the fmtstr pattern. For information on the fmtstr pattern, see the *Input Pattern Types* chapter.

nas-ip *aaa_nas_ipv4_address*

Specify the AAA NAS IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure instance configuration parameters.

profile radius accounting detect-dead-server

Configures the response timeout duration, in seconds, to wait for a response from the RADIUS server after which it is marked as unreachable/dead.

Command Modes Exec > Global Configuration (config) > RADIUS Configuration (config-radius)

Syntax Description **`detect-dead-server response-timeout`** *`response_timeout`*

response-timeout *response_timeout*

Specify the time interval, in seconds, for response from RADIUS server to mark as unreachable.

Must be an integer in the range of 1-65535.

Usage Guidelines Use this command to configure the response timeout duration, in seconds, to wait for a response from the RADIUS server after which it is marked as unreachable/dead.

profile radius allow auth

Configures the allow-auth on RADIUS server.

Command Modes Exec > Global Configuration (config) > RADIUS Configuration (config-radius)

Syntax Description **`enable-allow-auth`**

enable-allow-auth

If allow-auth is enabled in the configuration, it allows the ongoing call to continue irrespective of authentication being successful, timed out, or any error message received. The default value is false, configuration is required to enable the allow-auth.

Usage Guidelines Use this command to enble allow-auth in RADIUS server.

radius profile server group allow auth

Configures the allow-auth on RADIUS server group.

Command Modes

Exec > Global Configuration (config) > RADIUS Configuration (config-radius) > Server Group (config server group)

Syntax Description

`enable-allow-auth`

enable-allow-auth

If allow-auth is enabled in the configuration, it allows the ongoing call to continue irrespective of authentication being successful, timed out, or any error message received. The default value is false, configuration is required to enable the allow-auth.

Usage Guidelines

Use this command to enble allow-auth on any of the RADIUS server group.

profile radius attribute

Configures RADIUS identification parameters.

Command Modes

Exec > Global Configuration (config) > RADIUS Configuration (config-radius)

Syntax Description

`attribute { nas-identifier` *`nas_id`* **`| nas-ip`** *`aaa_nas_ipv4_address`* **`}`**

nas-identifier *nas_identifier*

Specify the attribute name by which the system will be identified in Auth or Accounting Request messages.

Must be a string in the fmtstr pattern. For information on the fmtstr pattern, see the *Input Pattern Types* chapter.

nas-identifier *nas_identifier*

Specify the attribute name by which the system will be identified in Auth or Accounting Request messages.

Must be a string in the fmtstr pattern. For information on the fmtstr pattern, see the *Input Pattern Types* chapter.

nas-ip *aaa_nas_ipv4_address*

Specify the AAA NAS IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines

Use this command to configure RADIUS identification parameters.

profile radius attribute instance

Configures instance configuration parameters.

Command Modes Exec > Global Configuration > RADIUS Configuration (config-radius)

Syntax Description **attribute instance** *instance_id* **nas-ip** *aaa_nas_ipv4_address*

instance *instance_id*

Specify the instance ID.

Must be an integer in the range of 1-8.

nas-identifier *nas_identifier*

Specify the attribute name by which the system will be identified in Auth or Accounting Request messages.

Must be a string in the fmtstr pattern. For information on the fmtstr pattern, see the *Input Pattern Types* chapter.

instance *instance_id*

Specify the instance ID.

Must be an integer in the range of 1-8.

nas-identifier *nas_identifier*

Specify the attribute name by which the system will be identified in Auth or Accounting Request messages.

Must be a string in the fmtstr pattern. For information on the fmtstr pattern, see the *Input Pattern Types* chapter.

nas-ip *aaa_nas_ipv4_address*

Specify the AAA NAS IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure instance configuration parameters.

profile radius consecutive failure dead server detection

Configures the value of consecutive failreres in the RADIUS server, after the value is reached, the server is marked as unreachable/dead.

Command Modes Exec > Global Configuration (config) > RADIUS Configuration (config-radius)

Syntax Description **detect-dead-server consecutive-failures** *value*

detect-dead-server consecutive-failures *value*

When a server's failure count reaches the threshold for consecutive failures, the server is declared as dead server.

value: must be an integer in the range of 1–1000. Default: 10.

It is recommended to configure the consecutive failure value more than the request maxTransmissions value in the setup.

Usage Guidelines Use this command to configure the failure value before the server is marked as dead.

profile radius detect-dead-server

Configures the response timeout duration, in seconds, to wait for a response from the RADIUS server after which it is marked as unreachable/dead.

Command Modes Exec > Global Configuration (config) > RADIUS Configuration (config-radius)

Syntax Description **detect-dead-server response-timeout** *response_timeout*

response-timeout *response_timeout*

Specify the time interval, in seconds, for response from RADIUS server to mark as unreachable.

Must be an integer in the range of 1-65535.

Usage Guidelines Use this command to configure the response timeout duration, in seconds, to wait for a response from the RADIUS server after which it is marked as unreachable/dead.

profile radius dictionary

Configures RADIUS dictionary.

Command Modes Exec > Global Configuration (config) > RADIUS Configuration (config-radius)

Syntax Description **dictionary** *dictionary_name*

dictionary *dictionary_name*

Specify the name of the dictionary as: Identify Services Engine (ISE) or 3GPP dictionary.

If this dictionary is configured, the SMF service renders the RADIUS configuration and populates the request messages with selected dictionary specific parameters.

Must be a string.

Usage Guidelines Use this command to configure RADIUS dictionary.

profile radius max transmissions

Configures the max-transmissions in the RADIUS server.

Command Modes Exec > Global Configuration (config) > RADIUS Configuration (config-radius)

Syntax Description **max-transmissions** *value*

max-transmissions *value*

Max transmission allows to configure the transmission parameters for all the available servers. This feature helps to cross-check if the number of transmissions exceeds the number of retries once the retry cycle for a request is finished, and if so, it begins the subsequent retry cycle on a different server if one is available. If no server is available or if maxtransimissions limit is reached, then the server database sends out the timeout response.

value: must be an integer in the range of 0–65535. Default: 6.

Usage Guidelines Use this command to configure the value of max-transmissions in the RADIUS server.

profile radius server

Configures the external RADIUS server parameters.

Command Modes Exec > Global Configuration (config) > RADIUS Configuration (config-radius) > RADIUS Server Group Configuration (config-server-group-*group_name*)

Syntax Description **server** *radius_server_ip_address radius_server_port_number* **[[secret** *radius_server_secret* **] [priority** *radius_server_priority* **] [type** *server_type* **]]**

priority *radius_server_priority*

Specify the priority of the RADIUS server.

Must be an integer in the range of 1-100.

secret *radius_server_secret*

Specify the RADIUS server secret.

Must be a string.

type *server_type*

Specify the server type.

Must be one of the following:

- **acct**: Specify the server is used for Accounting requests.
- **auth**: Specify the server is used for Authentication/Author requests.

Default Value: auth.

radius_server_ip_address

Specify the IP address of the RADIUS server.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

radius_server_port_number

Specify the port number of the RADIUS server.

Must be an integer in the range of 1-65535.

Usage Guidelines Use this command to configure the external RADIUS server parameters.

profile radius server-group

Configures association of RADIUS servers to groups.

Command Modes Exec > Global Configuration (config) > RADIUS Configuration (config-radius)

Syntax Description **server-group** *server_group_name*

algorithm *sever_selection_algorithm*

Specify the algorithm for selecting the RADIUS server. Default Value: first-server.

Must be one of the following:

- **first-server**
- **round-robin**

server-group *server_group_name*

Specify name of the RADIUS server group.

Must be a string in the fmtstr pattern. For information on the fmtstr pattern, see the *Input Pattern Types* chapter.

max_retries

Specify the maximum number of times the system will attempt retry with the RADIUS server.

Must be an integer in the range of 0-65535.

timeout_interval

Specify the time interval to elapse for a response from the RADIUS server before re-transmitting.

Must be an integer in the range of 1-65535.

Usage Guidelines Use this command to configure the association of RADIUS servers to groups.

profile radius server-group accounting

Configures RADIUS accounting parameters.

Command Modes Exec > Global Configuration

Syntax Description **`accounting`** *`options`*

algorithm *sever_selection_algorithm*

Specify the algorithm for selecting the RADIUS server. Default Value: first-server.

Must be one of the following:

- **first-server**
- **round-robin**

max_retries

Specify the maximum number of times the system will attempt retry with the RADIUS server.

Must be an integer in the range of 0-65535.

timeout_interval

Specify the time interval to elapse for a response from the RADIUS server before re-transmitting.

Must be an integer in the range of 1-65535.

Usage Guidelines Use this command to configure the RADIUS accounting parameters.

profile radius server-group accounting attribute

Configures RADIUS identification parameters.

Command Modes Exec > Global Configuration (config) > RADIUS Configuration (config-radius)

Syntax Description **`attribute { nas-identifier`** *`nas_id`* **`| nas-ip`** *`aaa_nas_ipv4_address`* **`}`**

nas-identifier *nas_identifier*

Specify the attribute name by which the system will be identified in Auth or Accounting Request messages.

Must be a string in the fmtstr pattern. For information on the fmtstr pattern, see the *Input Pattern Types* chapter.

nas-identifier *nas_identifier*

Specify the attribute name by which the system will be identified in Auth or Accounting Request messages.

Must be a string in the fmtstr pattern. For information on the fmtstr pattern, see the *Input Pattern Types* chapter.

nas-ip *aaa_nas_ipv4_address*

Specify the AAA NAS IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure RADIUS identification parameters.

profile radius server-group accounting attribute instance

Configures instance configuration parameters.

Command Modes Exec > Global Configuration > RADIUS Configuration (config-radius)

Syntax Description **`attribute instance`** *`instance_id`* **`nas-ip`** *`aaa_nas_ipv4_address`*

instance *instance_id*

Specify the instance ID.

Must be an integer in the range of 1-8.

nas-identifier *nas_identifier*

Specify the attribute name by which the system will be identified in Auth or Accounting Request messages.

Must be a string in the fmtstr pattern. For information on the fmtstr pattern, see the *Input Pattern Types* chapter.

instance *instance_id*

Specify the instance ID.

Must be an integer in the range of 1-8.

nas-identifier *nas_identifier*

Specify the attribute name by which the system will be identified in Auth or Accounting Request messages.

Must be a string in the fmtstr pattern. For information on the fmtstr pattern, see the *Input Pattern Types* chapter.

nas-ip *aaa_nas_ipv4_address*

Specify the AAA NAS IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure instance configuration parameters.

profile radius server-group attribute

Configures RADIUS identification parameters.

Command Modes Exec > Global Configuration (config) > RADIUS Configuration (config-radius)

Syntax Description **`attribute { nas-identifier`** *`nas_id`* **`| nas-ip`** *`aaa_nas_ipv4_address`* **`}`**

nas-identifier *nas_identifier*

Specify the attribute name by which the system will be identified in Auth or Accounting Request messages.

Must be a string in the fmtstr pattern. For information on the fmtstr pattern, see the *Input Pattern Types* chapter.

nas-identifier *nas_identifier*

Specify the attribute name by which the system will be identified in Auth or Accounting Request messages.

Must be a string in the fmtstr pattern. For information on the fmtstr pattern, see the *Input Pattern Types* chapter.

nas-ip *aaa_nas_ipv4_address*

Specify the AAA NAS IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure RADIUS identification parameters.

profile radius server-group attribute instance

Configures instance configuration parameters.

Command Modes Exec > Global Configuration > RADIUS Configuration (config-radius)

Syntax Description **`attribute instance`** *`instance_id`* **`nas-ip`** *`aaa_nas_ipv4_address`*

instance *instance_id*

Specify the instance ID.

Must be an integer in the range of 1-8.

nas-identifier *nas_identifier*

Specify the attribute name by which the system will be identified in Auth or Accounting Request messages.

Must be a string in the fmtstr pattern. For information on the fmtstr pattern, see the *Input Pattern Types* chapter.

instance *instance_id*

Specify the instance ID.

Must be an integer in the range of 1-8.

nas-identifier *nas_identifier*

Specify the attribute name by which the system will be identified in Auth or Accounting Request messages.

Must be a string in the fmtstr pattern. For information on the fmtstr pattern, see the *Input Pattern Types* chapter.

nas-ip *aaa_nas_ipv4_address*

Specify the AAA NAS IPv4 address.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure instance configuration parameters.

profile radius server-group server

Configures the RADIUS server parameters.

Command Modes Exec > Global Configuration (config) > RADIUS Configuration (config-radius) > RADIUS Server Group Configuration (config-server-group-*group_name*)

Syntax Description **`server type`** *`server_type radius_server_ip_address radius_server_port_number`*

type *server_type*

Specify the RADIUS server type.

Must be one of the following:

- **acct**: Specify the server is used for Accounting requests.
- **auth**: Specify the server is used for Authentication/Author requests.

radius_server_ip_address

Specify the IP address of the RADIUS server.

radius_server_port_number

Specify the port number of the RADIUS server.

Usage Guidelines Use this command to configure the RADIUS server parameters.

profile radius server group max transmissions

Configures the max-transmissions on the RADIUS server group.

Command Modes Exec > Global Configuration (config) > RADIUS Configuration (config-radius) > Server Group (config server-group)

Syntax Description **`max-transmissions`** *`value`*

max-transmissions *value*

Max transmission allows to configure the transmission parameters for all the available server groups. This feature helps to cross-check if the number of transmissions exceeds the number of retries once the retry cycle for a request is finished, and if so, it begins the subsequent retry cycle on a different server group if one is available. If no server group is available or if maxtransimissions limit is reached, then the server database sends out the timeout response.

value: must be an integer in the range of 0–65535. Default: 6.

Usage Guidelines Use this command to configure the value of max-transmissions on the RADIUS server group.

profile radius-dynamic-author

Configures the RADIUS Dynamic Author/COA profile.

Command Modes Exec > Global Configuration (config)

Syntax Description **`profile radius-dynamic-author [ client`** *`client_ip_address`* **`| secret`** *`secret_key`* **`| nas-identifier`** *`nas_identifier`* **`]`**

nas-identifier *nas_id*

Specify the Dynamic Author NAS ID.

Must be a string in the fmtstr pattern. For information on the fmtstr pattern, see the *Input Pattern Types* chapter.

nas-identifier *nas_id*

Specify the Dynamic Author NAS ID.

Must be a string in the fmtstr pattern. For information on the fmtstr pattern, see the *Input Pattern Types* chapter.

secret *secret_key*

Specify the Dynamic Author server shared secret key.

Must be a string.

Usage Guidelines Use this command to configure the RADIUS Dynamic Author/COA profile.

profile radius-dynamic-author client

Configures the RADIUS Dynamic Author Client parameters.

Command Modes Exec > Global Configuration

Syntax Description **client ip** *radius_client_ip_address* **secret** *secret_key*

ip *radius_client_ip_address*

Specify the IP address of the RADIUS client.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

secret *secret_key*

Specify the client shared secret key.

Must be a string.

Usage Guidelines Use this command to configure the RADIUS Dynamic Author Client parameters.

profile sgw-qos-profile

Configures the SGW QoS profile configuration.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile sgw-qos-profile** *sgw_qos_profile_name*

sgw-qos-profile *sgw_qos_profile_name*

Specify name of the SGW QoS profile.

Must be a string.

Usage Guidelines Use this command to configure the SGW QoS profile configuration.

profile sgw-qos-profile dscp-map operator-defined-qci

Configures the non-standard QCI values.

Command Modes Exec > Global Configuration (config) > SGW QoS Profile Configuration (config-sgw-qos-profile-*profile_name*)

Syntax Description **dscp-map operator-defined-qci** *non_standard_qos_class_id*

operator-defined-qci *non_standard_qos_class_id*

Specify the non-standard QoS class identifier.

Must be an integer in the range of 128-254.

Usage Guidelines Use this command to configure the non-standard QCI values.

profile sgw-qos-profile dscp-map operator-defined-qci gbr arp-priority-level

Configures the ARP priority level.

Command Modes Exec > Global Configuration (config) > QoS Profile Configuration (config-qos-*profile_name*)

Syntax Description **dscp-map qi5** *qci_name* **arp-priority-level** *arp_priority_level*

arp-priority-level *arp_priority_level*

Specify the ARP priority level.

Must be an integer in the range of 1-15.

Usage Guidelines Configures the type of the QCI to GBR. Use this command to configure the ARP priority level.

profile sgw-qos-profile dscp-map operator-defined-qci gbr arp-priority-level dscp-info

Configures the Differentiated Services Code Point (DSCP) type.

Command Modes Exec > Global Configuration

Syntax Description **dscp-info type** *dscp_type*

dl-encap-ci-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-ci-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-ci-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-co-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-co-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-co-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-copy-inner

Specify to copy the inner DSCP to outer.

dl-encap-copy-outer

Specify to copy the outer DSCP to inner.

dl-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-dscp-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-dscp-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

dl-iq-copy-outer

Specify to copy the outer DSCP to inner.

dl-iq-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-iq-encap-type

Specify to copy the inner DSCP to outer.

dl-iq-encaps-header

Specify the DSCP value to be applied to encaps header.

dl-iq-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-iq-user-datagram

Specify DSCP value be applied to user datagram.

dl-priority *dl_priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-ud-encap-copy-inner

Specify to copy the inner DSCP to outer.

dl-ud-encap-copy-outer

Specify to copy the outer DSCP to inner.

dl-ud-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

dl-ud-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-user-datagram

Specify DSCP value be applied to user datagram.

dscp-marking-dl *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

type *dscp_type*

Specify the DCSP type.

Must be one of the following:

- **downlink**
- **uplink**

ul-encap-ci-dscp *dscp_value*

Specify the DSCP value to be applied to packets. A hexadecimal string starting with "0x". For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-ci-priority *ul_encap_ci_priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-ci-user-datagram

Specify DSCP value be applied to user datagram.

ul-encap-co-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-co-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-co-user-datagram

Specify DSCP value be applied to user datagram.

ul-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-dscp-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-dscp-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

ul-encap-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encaps-header *dscp_value*

Specify the DCSP value to be applied to encaps header.

ul-iq-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-iq-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-iq-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-iq-encaps-header

Specify the DSCP value to be applied to encaps header.

ul-iq-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-iq-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

ul-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets. A hexadecimal string starting with 0x. For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-ud-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-ud-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-ud-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-ud-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

ul-ud-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

Usage Guidelines Use this command to configure the DSCP type.

profile sgw-qos-profile dscp-map operator-defined-qci gbr dscp-info

Configures the Differentiated Services Code Point (DSCP) type.

Command Modes Exec > Global Configuration

Syntax Description **`dscp-info type`** *`dscp_type`*

dl-encap-ci-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-ci-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-ci-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-co-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-co-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-co-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-copy-inner

Specify to copy the inner DSCP to outer.

dl-encap-copy-outer

Specify to copy the outer DSCP to inner.

dl-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-dscp-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-dscp-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

dl-iq-copy-outer

Specify to copy the outer DSCP to inner.

dl-iq-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-iq-encap-type

Specify to copy the inner DSCP to outer.

dl-iq-encaps-header

Specify the DSCP value to be applied to encaps header.

dl-iq-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-iq-user-datagram

Specify DSCP value be applied to user datagram.

dl-priority *dl_priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-ud-encap-copy-inner

Specify to copy the inner DSCP to outer.

dl-ud-encap-copy-outer

Specify to copy the outer DSCP to inner.

dl-ud-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

dl-ud-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-user-datagram

Specify DSCP value be applied to user datagram.

dscp-marking-dl *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

type *dscp_type*

Specify the DCSP type.

Must be one of the following:

- **downlink**
- **uplink**

ul-encap-ci-dscp *dscp_value*

Specify the DSCP value to be applied to packets. A hexadecimal string starting with "0x". For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-ci-priority *ul_encap_ci_priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-ci-user-datagram

Specify DSCP value be applied to user datagram.

ul-encap-co-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-co-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-co-user-datagram

Specify DSCP value be applied to user datagram.

ul-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-dscp-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-dscp-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

ul-encap-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encaps-header *dscp_value*

Specify the DCSP value to be applied to encaps header.

ul-iq-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-iq-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-iq-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-iq-encaps-header

Specify the DSCP value to be applied to encaps header.

ul-iq-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-iq-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

ul-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets. A hexadecimal string starting with 0x. For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-ud-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-ud-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-ud-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-ud-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

ul-ud-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

Usage Guidelines Use this command to configure the DSCP type.

profile sgw-qos-profile dscp-map operator-defined-qci non-gbr

Configures the QCI type to non GBR.

Command Modes Exec > Global Configuration

Syntax Description **non-gbr** *options*

Usage Guidelines Use this command to configure the QCI type to non GBR.

profile sgw-qos-profile dscp-map operator-defined-qci non-gbr arp-priority-level

Configures the ARP priority level.

Command Modes Exec > Global Configuration (config) > QoS Profile Configuration (config-qos-*profile_name*)

Syntax Description **dscp-map qi5** *qci_name* **arp-priority-level** *arp_priority_level*

arp-priority-level *arp_priority_level*

Specify the ARP priority level.

Must be an integer in the range of 1-15.

Usage Guidelines Configures the type of the QCI to GBR. Use this command to configure the ARP priority level.

profile sgw-qos-profile dscp-map operator-defined-qci non-gbr arp-priority-level dscp-info

Configures the Differentiated Services Code Point (DSCP) type.

Command Modes Exec > Global Configuration

Syntax Description **dscp-info type** *dscp_type*

dl-encap-ci-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-ci-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-ci-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-co-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-co-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-co-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-copy-inner

Specify to copy the inner DSCP to outer.

dl-encap-copy-outer

Specify to copy the outer DSCP to inner.

dl-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-dscp-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-dscp-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

dl-iq-copy-outer

Specify to copy the outer DSCP to inner.

dl-iq-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-iq-encap-type

Specify to copy the inner DSCP to outer.

dl-iq-encaps-header

Specify the DSCP value to be applied to encaps header.

dl-iq-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-iq-user-datagram

Specify DSCP value be applied to user datagram.

dl-priority *dl_priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-ud-encap-copy-inner

Specify to copy the inner DSCP to outer.

dl-ud-encap-copy-outer

Specify to copy the outer DSCP to inner.

dl-ud-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

dl-ud-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-user-datagram

Specify DSCP value be applied to user datagram.

dscp-marking-dl *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

type *dscp_type*

Specify the DCSP type.

Must be one of the following:

- **downlink**
- **uplink**

ul-encap-ci-dscp *dscp_value*

Specify the DSCP value to be applied to packets. A hexadecimal string starting with "0x". For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-ci-priority *ul_encap_ci_priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-ci-user-datagram

Specify DSCP value be applied to user datagram.

ul-encap-co-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-co-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-co-user-datagram

Specify DSCP value be applied to user datagram.

ul-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-dscp-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-dscp-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

ul-encap-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encaps-header *dscp_value*

Specify the DCSP value to be applied to encaps header.

ul-iq-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-iq-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-iq-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-iq-encaps-header

Specify the DSCP value to be applied to encaps header.

ul-iq-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-iq-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

ul-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets. A hexadecimal string starting with 0x. For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-ud-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-ud-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-ud-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-ud-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

ul-ud-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

Usage Guidelines Use this command to configure the DSCP type.

profile sgw-qos-profile dscp-map operator-defined-qci non-gbr dscp-info

Configures the Differentiated Services Code Point (DSCP) type.

Command Modes Exec > Global Configuration

Syntax Description **`dscp-info type`** *`dscp_type`*

dl-encap-ci-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-ci-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-ci-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-co-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-co-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-co-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-copy-inner

Specify to copy the inner DSCP to outer.

dl-encap-copy-outer

Specify to copy the outer DSCP to inner.

dl-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-dscp-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-dscp-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

dl-iq-copy-outer

Specify to copy the outer DSCP to inner.

dl-iq-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-iq-encap-type

Specify to copy the inner DSCP to outer.

dl-iq-encaps-header

Specify the DSCP value to be applied to encaps header.

dl-iq-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-iq-user-datagram

Specify DSCP value be applied to user datagram.

dl-priority *dl_priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-ud-encap-copy-inner

Specify to copy the inner DSCP to outer.

dl-ud-encap-copy-outer

Specify to copy the outer DSCP to inner.

dl-ud-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

dl-ud-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-user-datagram

Specify DSCP value be applied to user datagram.

dscp-marking-dl *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

type *dscp_type*

Specify the DCSP type.

Must be one of the following:

- **downlink**
- **uplink**

ul-encap-ci-dscp *dscp_value*

Specify the DSCP value to be applied to packets. A hexadecimal string starting with "0x". For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-ci-priority *ul_encap_ci_priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-ci-user-datagram

Specify DSCP value be applied to user datagram.

ul-encap-co-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-co-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-co-user-datagram

Specify DSCP value be applied to user datagram.

ul-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-dscp-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-dscp-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

ul-encap-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encaps-header *dscp_value*

Specify the DCSP value to be applied to encaps header.

ul-iq-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-iq-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-iq-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-iq-encaps-header

Specify the DSCP value to be applied to encaps header.

ul-iq-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-iq-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

ul-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets. A hexadecimal string starting with 0x. For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-ud-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-ud-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-ud-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-ud-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

ul-ud-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

Usage Guidelines Use this command to configure the DSCP type.

profile sgw-qos-profile dscp-map qci

Configures the standard QCI value.

Command Modes Exec > Global Configuration (config) > SGW QoS Profile Configuration (config-sgw-qos-profile-*profile_name*)

Syntax Description **dscp-map qci** *standard_qos_class_id options*

qci *standard_qos_class_id*

Specify the standard QoS class identifier.

Must be an integer from the following: 1-9, 65, 66, 69, 70, 80, 82, 83.

Usage Guidelines Use this command to configure the standard QCI value.

profile sgw-qos-profile dscp-map qci arp-priority-level

Configures the ARP priority level.

Command Modes Exec > Global Configuration (config) > QoS Profile Configuration (config-qos-*profile_name*)

Syntax Description **dscp-map qi5** *qci_name* **arp-priority-level** *arp_priority_level*

arp-priority-level *arp_priority_level*

Specify the ARP priority level.

Must be an integer in the range of 1-15.

Usage Guidelines Configures the type of the QCI to GBR. Use this command to configure the ARP priority level.

profile sgw-qos-profile dscp-map qci arp-priority-level dscp-info

Configures the Differentiated Services Code Point (DSCP) type.

Command Modes Exec > Global Configuration

Syntax Description **dscp-info type** *dscp_type*

dl-encap-ci-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-ci-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-ci-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-co-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-co-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-co-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-copy-inner

Specify to copy the inner DSCP to outer.

dl-encap-copy-outer

Specify to copy the outer DSCP to inner.

dl-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-dscp-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-dscp-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

dl-iq-copy-outer

Specify to copy the outer DSCP to inner.

dl-iq-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-iq-encap-type

Specify to copy the inner DSCP to outer.

dl-iq-encaps-header

Specify the DSCP value to be applied to encaps header.

dl-iq-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-iq-user-datagram

Specify DSCP value be applied to user datagram.

dl-priority *dl_priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-ud-encap-copy-inner

Specify to copy the inner DSCP to outer.

dl-ud-encap-copy-outer

Specify to copy the outer DSCP to inner.

dl-ud-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

dl-ud-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-user-datagram

Specify DSCP value be applied to user datagram.

dscp-marking-dl *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

type *dscp_type*

Specify the DCSP type.

Must be one of the following:

- **downlink**
- **uplink**

ul-encap-ci-dscp *dscp_value*

Specify the DSCP value to be applied to packets. A hexadecimal string starting with "0x". For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-ci-priority *ul_encap_ci_priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-ci-user-datagram

Specify DSCP value be applied to user datagram.

ul-encap-co-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-co-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-co-user-datagram

Specify DSCP value be applied to user datagram.

ul-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-dscp-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-dscp-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

ul-encap-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encaps-header *dscp_value*

Specify the DCSP value to be applied to encaps header.

ul-iq-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-iq-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-iq-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-iq-encaps-header

Specify the DSCP value to be applied to encaps header.

ul-iq-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-iq-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

ul-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets. A hexadecimal string starting with 0x. For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-ud-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-ud-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-ud-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-ud-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

ul-ud-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

Usage Guidelines Use this command to configure the DSCP type.

profile sgw-qos-profile dscp-map qci default

Configures the default QCI parameter.

Command Modes Exec > Global Configuration

Syntax Description **`default`** *`options`*

Usage Guidelines Use this command to configure the default QCI parameter.

profile sgw-qos-profile dscp-map qci default dscp-info

Configures the Differentiated Services Code Point (DSCP) type.

Command Modes Exec > Global Configuration

Syntax Description **`dscp-info type`** *`dscp_type`*

dl-encap-ci-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-ci-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-ci-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-co-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-co-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-co-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-copy-inner

Specify to copy the inner DSCP to outer.

dl-encap-copy-outer

Specify to copy the outer DSCP to inner.

dl-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-dscp-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-dscp-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

dl-iq-copy-outer

Specify to copy the outer DSCP to inner.

dl-iq-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-iq-encap-type

Specify to copy the inner DSCP to outer.

dl-iq-encaps-header

Specify the DSCP value to be applied to encaps header.

dl-iq-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-iq-user-datagram

Specify DSCP value be applied to user datagram.

dl-priority *dl_priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-ud-encap-copy-inner

Specify to copy the inner DSCP to outer.

dl-ud-encap-copy-outer

Specify to copy the outer DSCP to inner.

dl-ud-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

dl-ud-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-user-datagram

Specify DSCP value be applied to user datagram.

dscp-marking-dl *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

type *dscp_type*

Specify the DCSP type.

Must be one of the following:

- **downlink**
- **uplink**

ul-encap-ci-dscp *dscp_value*

Specify the DSCP value to be applied to packets. A hexadecimal string starting with "0x". For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-ci-priority *ul_encap_ci_priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-ci-user-datagram

Specify DSCP value be applied to user datagram.

ul-encap-co-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-co-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-co-user-datagram

Specify DSCP value be applied to user datagram.

ul-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-dscp-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-dscp-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

ul-encap-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encaps-header *dscp_value*

Specify the DCSP value to be applied to encaps header.

ul-iq-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-iq-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-iq-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-iq-encaps-header

Specify the DSCP value to be applied to encaps header.

ul-iq-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-iq-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

ul-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets. A hexadecimal string starting with 0x. For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-ud-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-ud-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-ud-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-ud-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

ul-ud-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

Usage Guidelines

Use this command to configure the DSCP type.

profile sgw-qos-profile dscp-map qci gbr dscp-info

Configures the Differentiated Services Code Point (DSCP) type.

Command Modes

Exec > Global Configuration

Syntax Description

dscp-info type *dscp_type*

dl-encap-ci-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-ci-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-ci-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-co-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-co-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-co-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-copy-inner

Specify to copy the inner DSCP to outer.

dl-encap-copy-outer

Specify to copy the outer DSCP to inner.

dl-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-dscp-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-dscp-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

dl-iq-copy-outer

Specify to copy the outer DSCP to inner.

dl-iq-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-iq-encap-type

Specify to copy the inner DSCP to outer.

dl-iq-encaps-header

Specify the DSCP value to be applied to encaps header.

dl-iq-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-iq-user-datagram

Specify DSCP value be applied to user datagram.

dl-priority *dl_priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-ud-encap-copy-inner

Specify to copy the inner DSCP to outer.

dl-ud-encap-copy-outer

Specify to copy the outer DSCP to inner.

dl-ud-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

dl-ud-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-user-datagram

Specify DSCP value be applied to user datagram.

dscp-marking-dl *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

type *dscp_type*

Specify the DCSP type.

Must be one of the following:

- **downlink**
- **uplink**

ul-encap-ci-dscp *dscp_value*

Specify the DSCP value to be applied to packets. A hexadecimal string starting with "0x". For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-ci-priority *ul_encap_ci_priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-ci-user-datagram

Specify DSCP value be applied to user datagram.

ul-encap-co-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-co-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-co-user-datagram

Specify DSCP value be applied to user datagram.

ul-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-dscp-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-dscp-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

ul-encap-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encaps-header *dscp_value*

Specify the DCSP value to be applied to encaps header.

ul-iq-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-iq-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-iq-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-iq-encaps-header

Specify the DSCP value to be applied to encaps header.

ul-iq-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-iq-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

ul-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets. A hexadecimal string starting with 0x. For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-ud-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-ud-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-ud-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-ud-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

ul-ud-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

Usage Guidelines

Use this command to configure the DSCP type.

profile sgw-qos-profile dscp-map qci non-gbr dscp-info

Configures the Differentiated Services Code Point (DSCP) type.

Command Modes

Exec > Global Configuration

Syntax Description

`dscp-info type` *`dscp_type`*

dl-encap-ci-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-ci-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-ci-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-co-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-co-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-co-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-copy-inner

Specify to copy the inner DSCP to outer.

dl-encap-copy-outer

Specify to copy the outer DSCP to inner.

dl-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encap-dscp-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-encap-dscp-user-datagram

Specify DSCP value be applied to user datagram.

dl-encap-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

dl-iq-copy-outer

Specify to copy the outer DSCP to inner.

dl-iq-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-iq-encap-type

Specify to copy the inner DSCP to outer.

dl-iq-encaps-header

Specify the DSCP value to be applied to encaps header.

dl-iq-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-iq-user-datagram

Specify DSCP value be applied to user datagram.

dl-priority *dl_priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

dl-ud-encap-copy-inner

Specify to copy the inner DSCP to outer.

dl-ud-encap-copy-outer

Specify to copy the outer DSCP to inner.

dl-ud-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

dl-ud-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

dl-user-datagram

Specify DSCP value be applied to user datagram.

dscp-marking-dl *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

type *dscp_type*

Specify the DCSP type.

Must be one of the following:

- **downlink**
- **uplink**

ul-encap-ci-dscp *dscp_value*

Specify the DSCP value to be applied to packets. A hexadecimal string starting with "0x". For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-ci-priority *ul_encap_ci_priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-ci-user-datagram

Specify DSCP value be applied to user datagram.

ul-encap-co-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-co-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-co-user-datagram

Specify DSCP value be applied to user datagram.

ul-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encap-dscp-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-encap-dscp-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

ul-encap-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-encaps-header *dscp_value*

Specify the DCSP value to be applied to encaps header.

ul-iq-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-iq-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-iq-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-iq-encaps-header

Specify the DSCP value to be applied to encaps header.

ul-iq-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-iq-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

ul-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-ud-dscp *dscp_value*

Specify the DSCP value to be applied to packets. A hexadecimal string starting with 0x. For example, 0x3F.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-ud-encap-copy-inner

Specify to copy the inner DSCP to outer.

ul-ud-encap-copy-outer

Specify to copy the outer DSCP to inner.

ul-ud-encap-dscp-marking *dscp_value*

Specify the DSCP value to be applied to packets.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

ul-ud-encaps-header *dscp_value*

Specify the DSCP value to be applied to encaps header.

ul-ud-priority *priority*

Specify the priority.

Must be a string in the pattern '[0-7]{1}'.

ul-user-datagram *dscp_value*

Specify DSCP value be applied to user datagram.

Usage Guidelines

Use this command to configure the DSCP type.

profile smf

Configures SMF profile.

Command Modes

Exec > Global Configuration (config)

Syntax Description

smf *profile_name* **[[dnn-selection-mode** *dnn_selection_mode* **] [load-profile** *load_profile_name* **] [locality** *locality* **] [mode** *mode_of_operation* **] [nf-services** *nf_services* **] [overload-profile** *overload_profile_name* **] [ue-authorization** *ue_authorization* **]]**

dnn-selection-mode *dnn_selection_mode*

NOTE: This command/keyword is deprecated from SMF Profile and has been added under DNN Profile. Specify the selection mode for subscription.

Must be one of the following:

- **network-provided**
- **ue-provided**
- **verified**

load-profile *load_profile_name*

Specify the name of the load profile.

Must be a string.

locality *locality*

Specify the locality for geo support.

Must be a string.

mode *mode_of_operation*

Specify the mode of operation.

Must be one of the following:

- **offline**: Offline mode. New sessions will be rejected.

nf-services *nf_services*

Specify the NF services.

Must be a string.

overload-profile *overload_profile_name*

Specify the name of the overload profile. Note that the load-profile configuration is mandatory to configure the overload-profile configuration.

Must be a string.

smf *profile_name*

Specify name of the SMF profile.

Must be a string.

ue-authorization *ue_authorization*

The SMF supports PDU sessions with IPv4v6 type in addition to IPv4 and IPv6 PDU session types for UEs. When a UE requests establishment of PDU session with a specific session type, the SMF checks the UE request against the UE subscription information maintained as default and allowed listPDU session types in the UDM. The SMF performs UE authorization and allocates IP address when the requested PDN type is matching with the values in the UDM. The SMF communicates about the allocated IP address to all other network functions.

Must be one of the following:

- **none**

Usage Guidelines Use this command to configure the SMF network function profile parameters.

profile smf instances

Configures the Geographic Redundancy (GR) instance ID.

Command Modes Exec > Global Configuration (config) > SMF Profile Configuration (config-smf-*profile_name*)

Syntax Description **instances** *gr_instance_id* **[[allowed-nssai** *allowed_nssai* **] [fqdn** *fqdn* **] [inter-plmn-fqdn** *inter_plmn_fqdn* **[node-id** *node_id*] **[supported-features** *supported_features* **]]**

allowed-nssai *nssai*

Specify the Network Slice Selection Assistance Information (NSSAI).

Must be a string.

fqdn *fqdn*

Specify the SMF+PGW-C FQDN.

Must be a string.

inter-plmn-fqdn *inter_plmn_fqdn*

Specify the inter-PLMN-FQDN, which is used in home and visiting SMF communication via SEPP.

Must be a string.

node-id *node_id*

Specify the SMF's node ID. For example, 1A2B3c.

Must be a string in the hex-string6 pattern. For information on the hex-string6 pattern, see the *Input Pattern Types* chapter.

supported-features *supported_features*

Specify the supported features.

Must be one of the following:

- **vsmf**

gr_instance_id

Specify the GR instance ID.

Usage Guidelines Use this command to configure the GR instance ID.

profile smf instances deactivate-features

Disables the UPCP and UPIP features on SMF despite receiving Up security policy from the UDM.

Command Modes Exec > Global Configuration (config) > SMF Profile Configuration (config-smf-*profile_name*)

Syntax Description

```
profile smf profile_name [ no ] instances gr_instance_iddeactivate-features {
 upcp | upip }
```

instances *gr_instance_id*

Specifies the GR instance ID of the SMF.

[no]

It is an optional command. It enables the deactivated UPCP or UPIP features on SMF to honor the UDM instructions again.

deactivate-features

Deactivates the UP security mechanism on SMF. It has two options:

- **upcp**: Deactivates User-Plane Confidentiality Protection.
- **upip**: Deactivates User-Plane Integrity Protection.



Note The commands **deactivate-features** and **no instances** are applicable only on the new sessions. The current sessions are not impacted with these CLIs.

Usage Guidelines Use this command to disable the UPCP or UPIP features on SMF to ignore the UDM instructions.

profile smf plmn-id

Configures the definition for public land mobile network identifier (PLMN ID) and the preferred radio access technology (RAT). This is one of PLMNs which is considered by the mobile as equivalent to the visited PLMN for cell reselection and network selection. When configured, the equivalent PLMN list will be sent to the UE in NAS ATTACH ACCEPT / TAU ACCEPT messages.

Command Modes Exec > Global Configuration (config) > SMF Profile Configuration (config-smf-*profile_name*)

Syntax Description **plmn-id { [mcc** *mobile_country_code* **] [mnc** *mobile_network_code* **] }**

mcc *mobile_country_code*

Specify the Mobile Country Code (MCC) portion of the PLMN ID.

Must be a string in the three-digit pattern. For information on the three-digit pattern, see the *Input Pattern Types* chapter.

mnc *mobile_network_code*

Specify the Mobile Network Code (MNC) portion of the PLMN ID.

Must be a string in the two-or-three-digit pattern. For information on the two-or-three-digit pattern, see the *Input Pattern Types* chapter.

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

profile smf plmn-list

Configures the SMF proflie PLMN list parameters.

Command Modes Exec > Global Configuration (config) > SMF Profile Configuration (config-smf-*profile_name*)

Syntax Description **plmn-list mcc** *mobile_country_code* **mnc** *mobile_network_code*

mcc *mobile_country_code*

Specify the 3-digit Mobile Country Code.

mnc *mobile_network_code*

Specify the 2- or 3-digit Mobile Country Network.

Usage Guidelines Use this command to configure the SMF proflie PLMN list parameters. If configured, both PLMN ID and PLMN list are used.

You can configure a maximum of 32 elements with this command.

profile smf service

Configures the session management network function services.

Command Modes

Exec > Global Configuration (config) > SMF Profile Configuration (config-smf-*profile_name*)

Syntax Description

service name *service_name* **[access-profile** *profile_name* **| capacity** *capacity* **| compliance-profile** *compliance_profile_name* **| icmpv6-profile** *profile_name* **| nf-service** *nf_service_name* **| priority** *priority* **| schema** *schema_name* **| service-id** *service_id* **| subscriber-policy** *policy_name* **| type** *service_type* **| version** *version* **]**

access-profile *profile_name*

Specify name of the access profile.

Must be a string.

capacity *capacity*

Specify the static weight relative to other NFs of the same type.

Must be an integer in the range of 0-65535.

Default Value: 10.

compliance-profile *compliance_profile_name*

Specify name of the compliance profile.

Must be a string.

icmpv6-profile *profile_name*

Specify name of the ICMPv6 profile.

Must be a string.

name *nf_service_name*

Specify name of the NF service.

Must be a string.

priority *priority*

Specify the priority relative to other NFs of the same type.

Must be an integer in the range of 0-65535.

Default Value: 1.

schema *schema_name*

Specify name of the schema.

Must be a string.

service-id *service_id*

Specify the service ID.

Must be a string.

Default Value: 1.

subscriber-policy *policy_name*

Specify name of the subscriber policy.

Must be a string.

type *service_type*

Specify the service type.

Must be one of the following:

- **pdu-session**
- **sm-event-exposure**

version *version*

Specify the version.

Must be a string.

Usage Guidelines Use this command to configure the N1, N2, and N11 interfaces in compliance with the 3GPP. The service names are specified in 3GPPTS 29.510 V15.2.0, Section 6.1.6.3.11. The CLI prompt changes to the Service Configuration mode (config-service-<service_name>).

profile smf service http-endpoint

Configures the SMF HTTP REST endpoint parameters.

Command Modes Exec > Global Configuration (config) > SMF Profile Configuration (config-smf-*profile_name*) > Service Configuration (config-service-*service_name*)

Syntax Description **`http-endpoint base-url`** *`base_url`*

base-url *base_url*

Specify the SMF base URL that is exposed and accessible externally.

Must be a string.

Usage Guidelines Use this command to configure the SMF HTTP REST endpoint parameters.

profile tai-group

Configures TAI group profile parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description **profile tai-group** *tai_group_name* **[priority** *tai_group_priority* **]**

priority *tai_group_priority*

Specify the priority of this TAI group.

Must be an integer in the range of 0-65535.

tai-group *tai_group_name*

Specify name of the TAI group.

Must be a string.

Usage Guidelines Use this command to configure the TAI group profile parameters.

profile tai-group tais

Configures the list of MCC and MNC.

Command Modes Exec > Global Configuration (config) > TAI Group Profile Configuration (config-tai-group-*profile_name*)

Syntax Description **tais { mcc** *mobile_country_code* **| mnc** *mobile_network_code* **}**

mcc *mobile_country_code*

Specify the Mobile Country Code (MCC).

Must be a string in the three-digit pattern. For information on the three-digit pattern, see the *Input Pattern Types* chapter.

mnc *mobile_network_code*

Specify the Mobile Network Code (MNC).

Must be a string in the two-or-three-digit pattern. For information on the two-or-three-digit pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure the list of MCC and MNC.

You can configure a maximum of 16 elements with this command.

profile tai-group tais tac

Configures the TAC Group parameters.

Command Modes Exec > Global Configuration (config) > TAI Group Profile Configuration (config-tai-group-*profile_name*)

Syntax Description **tac** *tac_values*

tac *tac_values*

Specify the list of TAC values.

Must be a string in the hex-stringtac pattern. For information on the hex-stringtac pattern, see the *Input Pattern Types* chapter.

You can configure a maximum of 64 elements with this keyword.

Usage Guidelines Use this command to configure the TAC Group parameters.

profile tai-group tais tac range

Configures TAC ranges.

Command Modes Exec > Global Configuration (config) > TAI Group Profile Configuration (config-tai-group-*profile_name*)

Syntax Description **range start** *tac_range_start* **end** *tac_range_end*

end *tac_range_end*

Specify the TAC range end value.

Must be a string in the hex-stringtac pattern. For information on the hex-stringtac pattern, see the *Input Pattern Types* chapter.

start *tac_range_start*

Specify the TAC range start value.

Must be a string in the hex-stringtac pattern. For information on the hex-stringtac pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure a TAC range.

You can configure a maximum of 64 elements with this command.

profile upf-group

Configures the UPF group profile.

Command Modes Exec > Global Configuration (config)

Syntax Description

profile upf-group *upf_group_name* **[dcnr { false | true } | location-area-group-list** *location_area_group_list* **| pdn-session-type** *pdn_session_type* **| slice-group-list** *slice_group_list* **| supported-features** *supported_features* **]**

dcnr { false | true }

Specify to enable or disable support for dual connectivity with new radio.

Must be one of the following:

- **false**
- **true**

Default Value: false.

location-area-group-list *location_area_group_list*

Specify the list of Location Area Group supported by UPF node.

Must be a string.

pdn-session-type *pdn_session_type*

Specify the list of PDN session type supported by UPF node.

Must be one of the following:

- **ipv4**
- **ipv4v6**
- **ipv6**

slice-group-list *slice_group_list*

Specify the list of slice group supported by UPF node.

Must be a string.

supported-features *supported_features*

Specify the list of features supported by the UPF node.

upf-group *upf_group_name*

Specify name of the UPF group.

Must be a string.

Usage Guidelines

Use this command to configure the UPF group profile.

profile upf-group failure-profile

Configures the UPF Group failure profile.

Command Modes Exec > Global Configuration (config) > UPF Group Profile Configuration (config-upf-group-*profile_name*)

Syntax Description **failure-profile** *failure_profile_name*

failure-profile *failure_profile_name*

Specify name of the UPF failure profile.

Must be a string.

Usage Guidelines Use this command to configure the UPF Group failure profile.

profile upf-group heartbeat

Enables PFCP path management.

Command Modes Exec > Global Configuration (config) > UPF Group Profile Configuration (config-upf-group-*profile_name*)

Syntax Description **heartbeat [interval** *heartbeat_interval* **| retransmission-timeout** *retransmission_timeout* **| max-retransmissions** *max_retransmissions* **]**

interval *heartbeat_interval*

Specify the heartbeat interval in seconds. To disable, set to 0.

Must be an integer from the following: 0, 60-360.

max-retransmissions *max_retransmissions*

Specify the maximum number retries for PFCP heartbeat request.

Must be an integer in the range of 0-10.

retransmission-timeout *retransmission_timeout*

Specify the heartbeat retransmission timeout period in seconds.

Must be an integer in the range of 1-20.

Usage Guidelines Use this command to enable PFCP path management.

profile wps

Configures the Wireless Priority Service (WPS) profile parameters.

Command Modes Exec > Global Configuration (config)

Syntax Description

```
profile wps wps_service_name [ arp arp_level_range [ qci ]
message-priority-profile  profile_name    ] ]
     profile message-prioritymsg_priority_profile_name
     interface [ any | pfcp | sbi [ { create | update | delete } ] ]
       priority value range
```

arp *arp_level_range*

Specify the range of ARP levels (separated by comma (,) or hyphen (-)).

Specify the ARP value in integer from 1 to 15.

-Or-

Must be a string.

qci message-priority-profile *profile_name* : Wireless Priority session is decided based on the ARP and optionally on the QCI.

message-priority-profile *profile_name* : This parameter is used only if the message priority profile is not associated. For example, message-priority-profile [pfcp gtpc].

Important If you are upgrading SMF from Release 2023.03.0 to a later release, make sure you manually reconfigure the ARP parameter in the WPS profile after the upgrade is complete.

wps *wps_service_name*

Specify name of the WPS service.

Must be a string.

interface [any | pfcp | sbi [{ create | update | delete }]]

- **interface [any | pfcp | sbi]** : Specify priority value per interface and in case of SBI interface, configure based on a procedure. If procedure is not configured, same value is applied for all procedures. Interface type is optional and if not configured, same value is applied across all interfaces.
- **priority** *value*: Specifies the range of priority levels from 0 to 31 for sbi or 0 to 15 for pfcp, gtp, or any, where 0 indicates the highest priority, while 31 or 15 indicates the lowest priority.

Note Priority is not populated in outbound messages, which are self-triggered. For example, outbound messages triggered by timer expiry.

Usage Guidelines

Use this command to configure the WPS profile parameters. The CLI prompt changes to the WPS Profile Configuration mode (config-wps-<profile_name>).

profile wps dscp

Configures the DSCP marking values.

Command Modes Exec > Global Configuration (config) > WPS Profile Configuration (config-wps-*profile_name*)

Syntax Description **dscp { [n3** *up_dscp_marking* **] [n4** *cp_dscp_marking* **] [s2b** *dscp_marking* **] [s5** *dscp_marking* **] [s5e** *cp_dscp_marking* **] [s8** *dscp_marking* **] [s11** *cp_dscp_marking* **] [sxa** *cp_dscp_marking* **]]**

message-priority *message_priority*

Specify the message priority for GTP-C and UP.

Must be one of the following:

- **gtpc**
- **pfcp**

You can configure a maximum of two elements with this keyword.

n3 *up_dscp_marking*

Specify the N3 UP DSCP marking value.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

n4 *cp_dscp_marking*

Specify the N4 CP DSCP marking value.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

s11 *cp_dscp_marking*

Specify the S11 CP DSCP marking value.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

s2b *dscp_marking*

Specify the S2B DSCP marking value.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

s5 *dscp_marking*

Specify the S5 DSCP marking value.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

s5e *cp_dscp_marking*

Specify the S5E CP DSCP marking value.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

s8 *dscp_marking*

Specify the S8 DSCP marking value.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

sxa *cp_dscp_marking*

Specify the SXA CP DSCP marking value.

Must be a string in the hex-stringdscp pattern. For information on the hex-stringdscp pattern, see the *Input Pattern Types* chapter.

Usage Guidelines Use this command to configure the DSCP marking values.

service name type

Configures UDM services.

Command Modes Exec > UDM message handling profile configuration.

Syntax Description **`service name type { nudm-ee | nudm-pp | nudm-sdm | nudm-ueau | nudm-uecm }`** *`service_type`*

service name type { nudm-ee | nudm-pp | nudm-sdm | nudm-ueau | nudm-uecm } *service_type*

Configure the UDM services based on the use case scenario.

SMF allows configuration of these different UDM service types:

- **nudm-ee**—Specify this service for NEFs to subscribe to or unsubscribe from UDM event notifications.
- **nudm-pp**—Specify this service to provision information, which can be used for the UE in 5GS.
- **nudm-sdm**— Specify this service to retrieve UE subscription data relevant to their operation from the UDM. The **nudm-sdm** service type enables the UDM local configuration.
- **nudm-ueau**—Specify this service to inform the UDM of authentication results, to query authentication results, and to purge authentication results.

Note The Nudm_UEAuthentication service is used by SMF to obtain UE authentication vectors from the UDM.

- **nudm-uecm**—Specify this service to allow the SMF to register and deregister itself as serving the UE, and to update the UE context information in the UDM.

Usage Guidelines Use this command to configure different types of UDM services.

radius

Displays RADIUS Client information.

Command Modes Exec

Syntax Description `show radius`

Usage Guidelines Use this command to view RADIUS Client information.

radius acct-server

Displays RADIUS Accounting Server information.

Command Modes Exec

Syntax Description `show radius acct-server`

Usage Guidelines Use this command to view RADIUS Accounting Server information.

radius auth-server

Displays RADIUS Authentication Server information.

Command Modes Exec

Syntax Description `show radius auth-server`

Usage Guidelines Use this command to view RADIUS Authentication Server information.

radius-dyn-auth

Displays RADIUS Dynamic Author data.

Command Modes Exec

Syntax Description `show radius-dyn-auth`

Usage Guidelines Use this command to view the RADIUS Dynamic Author data.

radius-dyn-auth clients

Displays RADIUS Authentication Server information.

Command Modes Exec

Syntax Description `show radius auth-server`

Usage Guidelines Use this command to view RADIUS RADIUS Authentication Server information.

rcm switchover

Configures Redundancy and Configuration Manager (RCM) switchover operation.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `rcm switchover source ip_address destination ip_address`

source *ip_address*

Specify the source IP address.

Must be an IP address.

destination *ip_address*

Specify the destination IP address.

Must be an IP address.

Usage Guidelines Use this command to configure RCM switchover operation.

reconcile ipam

Reconciles IPAM data with CDL records.

Command Modes Exec > Global Configuration (config)

Syntax Description `reconcile ipam`

Usage Guidelines Use this command to reconcile IPAM data with CDL records.

resource pod

Configures Pod resource parameter.

Command Modes Exec > Global Configuration (config)

Syntax Description `pod podtype pod_type`

podtype *pod_type*

Specify the pod type.

Usage Guidelines Use this command to configure Pod resource parameter.

resource pod cpu

Configures CPU resource request parameter.

Command Modes Exec > Global Configuration (config) > Pod Resource Configuration (config-resource-*pod_type*)

Syntax Description **cpu request** *cpu_resource_request*

request *cpu_resource_request*

Specify the CPU resource request in millicores.

Must be an integer in the range of 100-1000000.

Usage Guidelines Use this command to configure CPU resource request parameter.

resource pod labels

Configures K8 Node Affinity label configuration.

Command Modes Exec > Global Configuration (config) > Pod Resource Configuration (config-resource-*pod_type*)

Syntax Description **labels key** *label_key* **value** *label_value*

key *label_key*

Specify the key for the label.

Must be a string.

value *label_value*

Specify the value for the label.

Must be a string.

Usage Guidelines Use this command to configure K8 Node affinity label configuration.

resource pod memory

Configures memory resource request parameter.

Command Modes Exec > Global Configuration (config) > Pod Resource Configuration (config-resource-*pod_type*)

Syntax Description **memory request** *memory_resource_request*

request *memory_resource_request*

Specify the memory resource request in megabytes.

Must be an integer in the range of 100-200000.

Usage Guidelines Use this command to configure memory resource request parameter.

resources info

Displays resource information.

Command Modes Exec

Syntax Description **show resources [info]**

Usage Guidelines Use this command to view information about the configured resources.

router bgplist

Configures BGP speaker configuration.

Command Modes Exec > Global Configuration (config)

Syntax Description **router bgp** *bgp* **[learnDefaultRoute { false | true } | loopbackBFDPort** *bfd_local_port_number* **| loopbackPort** *bgp_local_port_number* **]**

bgp *bgp*

Specify the BGP.

Must be an integer.

learnDefaultRoute { false | true }

Specify whether to enable or disable learning default route and adding it in kernel space.

Must be one of the following:

- **false**
- **true**

Default Value: false.

loopbackBFDPort *bfd_local_port_number*

Specify the BFD local port number.

Must be an integer.

Default Value: 3784.

loopbackPort *bgp_local_port_number*

Specify the BGP local port number.

Must be an integer.

Default Value: 179.

Usage Guidelines Use this command to configure the BGP speaker configuration.

router bgplist bfd

Configures BFD configuration.

Command Modes Exec > Global Configuration (config) > Router Configuration (config-router-*router*)

Syntax Description **bfd { interval** *bfd_interval* **| min_rx** *bfd_min_rx* **| multiplier** *bfd_interval_multiplier* **}**

interval *bfd_interval*

Specify, in microseconds, the BFD interval.

Must be an integer.

Default Value: 250000.

min_rx *bfd_min_rx*

Specify, in microseconds, the BFD minimum RX.

Must be an integer.

Default Value: 250000.

multiplier *bfd_interval_multiplier*

Specify the BFD interval multiplier.

Must be an integer.

Default Value: 3.

Usage Guidelines Use this command to configure the BFD configuration.

router bgplist interfaceList

Configures bonding interface configuration.

Command Modes Exec > Global Configuration (config) > Router Configuration (config-router-*router*)

Syntax Description **interface** *bgp_local_interface*

interface *bgp_local_interface*

Specify the BGP local interface.

Must be a string.

Usage Guidelines Use this command to configure the bonding interface configuration.

router bgplist interfaceList bondingInterfaces

Configures bonding interface configuration.

Command Modes Exec > Global Configuration (config) > Router Configuration (config-router-*router*) > Router Interface Configuration (config-router-*interface*)

Syntax Description **bondingInterface** *linked_bonding_interface*

bondingInterface *linked_bonding_interface*

Specify the linked bonding interface.

Must be a string.

Usage Guidelines Use this command to configure the bonding interface configuration.

router bgplist interfaceList neighbors

Configures neighbor parameters.

Command Modes Exec > Global Configuration (config) > Router Configuration (config-router-*router*) > Router Interface Configuration (config-router-*interface*)

Syntax Description **neighbor** *neighbor_ip_address* **[fail-over** *failover_type* **| remote-as** *remote_as_number* **]**

fail-over *failover_type*

Specify the failover type.

Must be one of the following:

- **bfd**

neighbor *neighbor_ip_address*

Specify the IP address of the neighbor.

Must be a string.

remote-as *remote_as_number*

Specify the Autonomous System (AS) number of the BGP neighbor.

Must be an integer.

Default Value: 65000.

Usage Guidelines Use this command to configure the neighbor parameters.

router bgplist policies

Configures policy parameters.

Command Modes Exec > Global Configuration (config) > Router Configuration (config-router-*router*)

Syntax Description

```
policy-name policy_name [ as-path-set as_path_set | gateWay gateway_address |
interface interface | ip-prefix ip_prefix | isStaticRoute { false | true } |
 mask-range mask_range | modifySourceIp { false | true } ]
```

as-path-set *as_path_set*

Specify the Autonomous System (AS) path set.

Must be a string.

gateWay *gateway_address*

Specify the gateway address.

Must be a string.

interface *interface*

Specify the interface to set as source ip.

Must be a string.

ip-prefix *ip_prefix*

Specify the IP prefix.

Must be a string.

isStaticRoute { false | true }

Specify whether to enable or disable adding static route into kernel space.

Must be one of the following:

- **false**
- **true**

Default Value: false.

mask-range *mask_range*

Specify the mask range.

Must be a string.

modifySourceIp { false | true }

Specify whether to enable or disable modifying source IP of incoming route.

Must be one of the following:

- **false**
- **true**

Default Value: false.

policy-name *policy_name*

Specify name of the policy.

Must be a string.

source-prefix *source_ip_prefix*

Specify the source IP prefix.

Must be a string.

Usage Guidelines Use this command to configure the policy parameters.

rpc all

Displays RPC configuration information.

Command Modes Exec

Syntax Description `show rpc [ all ]`

Usage Guidelines Use this command to view RPC configuration information for all RPCs.

running-status info

Displays the system's current status information.

Command Modes Exec

Syntax Description `show running-status [ info ]`

Usage Guidelines Use this command to view the system's current status information.

screen-length

Configures the number of rows of text that the terminal screen displays.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **screen-length** *number_of_rows*

number_of_rows

Specify the number of rows that the terminal screen displays.

Must be an integer.

Usage Guidelines Use this command to set the number of rows that the terminal screen displays.

screen-width

Configures the number of columns that the terminal screen displays.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **screen-width** *number_of_columns*

number_of_columns

Specify the number of columns that the terminal screen displays.

Must be an integer.

Usage Guidelines Use this command to set the number of columns that the terminal screen displays.

send

Sends messages to the terminal of a specific user or all users.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **send** *user message*

user

Specify the user to whom the message must be sent.

Must be a string. Select from the possible completion options.

message

Specify the message that must be sent.

Must be a string.

Usage Guidelines Use this command to send messages to the terminal of a specific user or to all users.

sessions affinity

Displays the affinity count per instance.

Command Modes Exec

Syntax Description `show sessions affinity`

Usage Guidelines Use this command to view the affinity count per instance.

sessions commit-pending

Displays information for sessions for which the commits are in pending state.

Command Modes Exec

Syntax Description `show sessions commit-pending`

Usage Guidelines Use this command to view information for sessions that are pending commits.

quit

Exits the management session.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `quit`

Usage Guidelines Use this command to exit the management session.

show

Displays the system information.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **show** *system_component*

system_component

Specify the component to view the information.

Must be a string. Select from the possible completion options.

Usage Guidelines Use this command to view the system information.

show bfd-neighbor

Displays Bidirectional Forwarding Detection (BFD) status of neighbors.

Command Modes Exec

Syntax Description **show bfd-neigbor [ip** *ip_address* **]**

ip *ip_address*

Specify the IP address of the neighbor.

Must be a string.

Usage Guidelines Use this command to view the BFD status of neighbors. If no IP address is specified, the command displays the BFD status for all neighbors.

show bgp-advertised-routes

Displays the BGP routes that are advertised to neighbors.

Command Modes Exec

Syntax Description **show bgp-advertised-routes [ipv4 | ipv6 | vrf** *vrf_name* **]**

ipv4

Option to display details for IPv4 address family.

ipv6

Option to display details for IPv6 address family.

vrf *vrf_name*

Specify the Virtual Routing and Forwarding (VRF) of the advertised routes. *vrf_name* must be a valid VRF name string.

Usage Guidelines Use this command to view the BGP routes being advertised to neighbors. You can filter the output by address family (IPv4/IPv6) or by VRF. If no option is specified, the command displays all advertised routes.

show bgp-global

Displays BGP global configuration.

Command Modes Exec

Syntax Description `show bgp-global`

Usage Guidelines Use this command to view BGP global configuration.

show bgp-kernel-route

Displays BGP kernel-configured routes.

Command Modes Exec

Syntax Description `show bgp-kernel-route [ application { false | true } ]`

application { false | true }

Specify whether to display application added routes.

Must be one of the following:

- **false**
- **true**

Default Value: false.

Usage Guidelines Use this command to view BGP kernel-configured routes.

show bgp-learned-routes

Displays the BGP routes that are learned from neighbors.

Command Modes Exec

Syntax Description **`show bgp-learned-routes [ ipv4 | ipv6 | vrf vrf_name ]`**

ipv4

Option to display details for IPv4 address family. Must be followed by the **vrf** keyword.

ipv6

Option to display details for IPv6 address family. Must be followed by the **vrf** keyword.

vrf *vrf_name*

Specify the Virtual Routing and Forwarding (VRF) of the advertised routes. *vrf_name* must be a valid VRF name string.

Usage Guidelines Use this command to view the BGP routes learned from neighbors. You can filter the output by address family (IPv4/IPv6) or by VRF. If no option is specified, the command displays all learned routes.

show bgp-neighbors

Displays BGP neighbor's status.

Command Modes Exec

Syntax Description **`show bgp-neighbors [ ip ip_address ]`**

ip *ip_address*

Specify the IP address of the neighbor.

Must be a string.

Usage Guidelines Use this command to view BGP neighbor's status.

show bgp-route-summary

Displays BGP route summary.

Command Modes Exec

Syntax Description **`show bgp-route-summary`**

Usage Guidelines Use this command to view BGP route summary.

show bgp-routes

Displays BGP routes information.

Command Modes Exec

Syntax Description **`show bgp-routes`**

Usage Guidelines Use this command to view BGP routes information.

show diameter routes all

Displays the route details.

Command Modes Exec

Syntax Description **`show diameter routes all`**

Usage Guidelines Use this command to view the diameter route details.

show edr

Displays EDR Transaction Procedure Event fields.

Command Modes Exec

Syntax Description **`show edr { [ event`** *`transaction_procedure_event`* **`] [ transaction-procedure`** *`transaction_procedure`* **`] }`**

event *transaction_procedure_event*

Specify the transaction procedure event name/id/all.

Must be a string.

transaction-procedure *transaction_procedure*

Specify the transaction procedure name/id/all.

Must be a string.

Usage Guidelines Use this command to view EDR Transaction Procedure Event fields.

show geo-maintenance-mode

Displays maintenance mode enable/disable.

Command Modes Exec

Syntax Description **`show geo-maintenance-mode`**

Usage Guidelines Use this command to view maintenance mode status.

show georeplication-status

Displays result as Pass / Fail after comparing ETCD and Cache checksum with peer rack.

Command Modes Exec

Syntax Description `show georeplication-status`

Usage Guidelines Use this command to view replication status between peer racks for ETCD and cache.

show georeplication

Displays ETCD/Cache checksum.

Command Modes Exec

Syntax Description `show georeplication checksum instance-id` *instance_id*

checksum

Specify checksum.

instance-id *instance_id*

Specify the instance ID for which checksum will be displayed.

Must be a string.

Usage Guidelines Use this command to view ETCD/Cache checksum.

show idmgr-debug

Displays internal information of IDMGR.

Command Modes Exec

Syntax Description `show idmgr-debug all`

Usage Guidelines Use this command to view the internal details of IDMGR.

show ipam dp

Displays IPAM data-plane utilization information for all data planes.

Command Modes Exec

Syntax Description **show ipam dp**

Usage Guidelines Use this command to view IPAM data-plane utilization information for all data planes.

show ipam dp name

Displays IPAM data-plane allocations details.

Command Modes Exec

Syntax Description **show ipam dp** *dp_name*

dp *dp_name*

Specify the IPAM data-plane name.

Usage Guidelines Use this command to view IPAM data-plane allocations details.

show ipam dp name ipv4-addr

Displays IPv4 address ranges assigned to a data plane.

Command Modes Exec

Syntax Description **show ipam dp** *dp_name* **ipv4-addr**

Usage Guidelines Use this command to view the IPv4 address ranges assigned to a data plane.

show ipam dp name ipv6-addr

Displays IPv6 address ranges assigned to a data plane.

Command Modes Exec

Syntax Description **show ipam dp** *dp_name* **ipv6-addr**

Usage Guidelines Use this command to view the IPv6 address ranges assigned to a data plane.

show ipam dp name ipv6-prefix

Displays IPv6 prefix ranges assigned to a data plane.

Command Modes Exec

Syntax Description **show ipam dp** *dp_name* **ipv6-prefix**

Usage Guidelines Use this command to view the IPv6 prefix ranges assigned to a data plane.

show ipam dp tag

Displays IPAM data-plane utilization information for all data-plane and tag combination. Tag represents DNN, NSSAI, or serving area.

Command Modes Exec

Syntax Description **show ipam dp tag** *tag_name*

dp tag ***tag_name***

Specify the data-plnae tag name.

Usage Guidelines Use this command to view IPAM data-plane utilization information for all data plane and tag combination.

show ipam dp tag tag-name

Displays IPAM data-plane utilization information for specific DP and tag combination. Tag represents DNN, NSSAI, or serving area.

Command Modes Exec

Syntax Description **show ipam dp tag name** *tag_name*

dp tag name ***tag_name***

Specify the specific data-plnae tag name.

Usage Guidelines Use this command to view IPAM data-plane utilization information for specific dp and tag combination.

show ipam dp tag ipv4-addr

Displays IPv4 address information for specific DP and Tag combination. Tag represents DNN, NSSAI, or serving area.

Command Modes Exec

Syntax Description **show ipam dp tag** *tag_name* **ipv4-addr**

Usage Guidelines Use this command to view IPv4 address information for specific DP and Tag combination.

show ipam dp tag ipv6-addr

Displays IPv6 address information for specific DP and Tag combination. Tag represents DNN, NSSAI, or serving area.

Command Modes Exec

Syntax Description **show ipam dp tag** *tag_name* **ipv6-addr**

Usage Guidelines Use this command to view IPv6 address information for specific DP and Tag combination.

show ipam dp tag ipv6-prefix

Displays IPv6 prefix ranges for specific DP and Tag combination. Tag represents DNN, NSSAI, or serving area.

Command Modes Exec

Syntax Description **show ipam dp tag** *tag_name* **ipv6-prefix**

Usage Guidelines Use this command to view IPv6 prefix ranges for specific DP and Tag combination.

show ipam pool

Displays IPAM pool utilization information for all pools.

Command Modes Exec

Syntax Description **show ipam pool**

Usage Guidelines Use this command to view IPAM pool utilization information for all pools.

show ipam pool name

Displays IPAM pool allocation information for specific pool.

Command Modes Exec

Syntax Description **show ipam pool** *pool_name*

pool ***pool_name***

Specify the IPAM pool name.

Usage Guidelines Use this command to view IPAM pool allocation information for specific pool.

show ipam pool name ipv4-addr

Displays IPAM pool IPv4 address information for specific pool.

Command Modes Exec

Syntax Description **show ipam pool** *pool_name* **ipv4-addr**

Usage Guidelines Use this command to view IPAM pool IPv4 address information.

show ipam pool name ipv6-addr

Displays IPAM pool IPv6 address information for specific pool.

Command Modes Exec

Syntax Description **show ipam pool** *pool_name* **ipv6-addr**

Usage Guidelines Use this command to view IPAM pool IPv6 address information.

show ipam pool name ipv6-prefix

Displays IPAM pool IPv6 prefix ranges details of specific pool.

Command Modes Exec

Syntax Description **show ipam pool** *pool_name* **ipv6-prefix**

Usage Guidelines Use this command to view IPAM pool IPv6 prefix ranges information.

show ipam-staticdb

Displays static IP information of a pool.

Command Modes Exec

Syntax Description **show ipam-staticdb pool-name** *pool_name* **[ipv4-addr | ipv6-addr | ipv6-prefix] start-index [index]**

ipv4-addr

Option to display static IP information of Ipv4 address.

ipv6-addr

Option to display static IP information of Ipv6 address.

ipv6-prefix

Option to display static IP information of Ipv6 prefix.

start-index

Option to display subscribe-key and IP. Max 1000 subkeys and IPs are displayed starting from index.

Usage Guidelines Use this command to view static IP information for a pool.

show peers

Displays additional diameter information.

Command Modes Exec

Syntax Description **`show peers`**

Usage Guidelines Use this command to view additional diameter information.

show role

Displays current role for the specified instance.

Command Modes Exec

Syntax Description **`show role instance-id`** *`instance_id`*

instance-id *instance_id*

Specify the instance ID for which role must be displayed.

Usage Guidelines Use this command to view current role for the specified instance.

show subscriber

Displays subscriber information.

Command Modes Exec

Syntax Description **`show subscriber { [ all ] [ gr-instance`** *`gr_instance`* **`] [ imei`** *`imei_id`* **`] [ nf-service`** *`nf_service`* **`] [ supi`** *`supi_id`* **`] [`** *`config_specific_options`* **`] }`**

access *access_technology*

Specify the access technology.

Must be a string of 11-25 characters.

all

Specify all SUPIs or IMEIs.

amf *amf_address*

Specify the AMF address.

Must be a string of 7-39 characters.

apn *apn_name*

Specify name of the APN.

Must be a string of 1-255 characters.

auth-status *radius_auth_status*

Specify the RADIUS authentication status - authenticated or unauthenticated.

Must be a string of 13, or 15 characters.

chf *chf_address*

Specify the CHF address.

Must be a string of 7-39 characters.

connectivity *connectivity_type*

Specify the connectivity type.

Must be a string of 2 characters.

count *count*

Specify the count.

Must be one of the following:

- **count**

debug-info *debug_info*

Specify print the debug info.

Must be one of the following:

- **debug-info**

dnn *dnn_value*

Specify the DNN value.

Must be a string of 1-255 characters.

emergency { false | true }

Specify emergency session indication.

Must be one of the following:

- **false**
- **true**

gpsi *gpsi*

Specify the Generic Public Subscription Identifier (GPSI).

Must be a string of 1-255 characters.

gr-instance *gr_instance*

Specify the network function service under which to search.

gtp-peer *gtp_peer_address*

Specify address of the GTP peer.

Must be a string of 7-39 characters.

imei *imei_id*

Specify the International Mobile Equipment Identity.

Must be a string of 15-16 characters.

imsi *imsi*

Specify the International Mobile Subscriber Identifier (IMSI).

Must be a string.

ipv4-addr *ipv4_address*

Specify the IPv4 address in the format *pool_name*/*ipv4_address*.

Must be a string of 1-255 characters.

ipv4-pool *ipv4_pool_name*

Specify name of the IPv4 pool.

Must be a string of 1-255 characters.

ipv4-range *ipv4_address_range*

Specify the IPv4 address range in the format *pool_name*/*start_ip_address*.

Must be a string of 1-255 characters.

ipv6-pfx *ipv6_pfx*

Specify the IPv6 prefix in the format *pool_name*/*ipv6_prefix*.

Must be a string of 1-255 characters.

ipv6-pool *ipv6_pool_name*

Specify name of the IPv6 pool.

Must be a string of 1-255 characters.

ipv6-range *ipv6_prefix_range*

Specify the IPv6 prefix range in the format *pool_name*/*start_prefix*.

Must be a string of 1-255 characters.

msid *msid*

Specify the Mobile Subscriber Identification Number (MSID).

Must be a string of 1-255 characters.

msisdn *msisdn*

Specify the Mobile Station International Subscriber Directory Number (MSISDN).

Must be a string of 1-255 characters.

namespace *namespace*

NOTE: This keyword is deprecated, use nf-service instead. Specify the product namespace under which to search.

Default Value: cisco-mobile-infra:none.

nf-service *nf_service*

Specify the network function service under which to search.

Default Value: cisco-mobile-infra:none.

pcf *pcf_address*

Specify the PCF address.

Must be a string of 7-39 characters.

peerGtpuEpKey *gtpu_peer_address*

Specify address of the GTPU peer in the *upf_addr:gptu_peer_addr* format.

Must be a string of 1-255 characters.

pei *permanent_equipment_id*

Specify the Permanent Equipment Identifier.

Must be a string of 1-255 characters.

policy *policy_type*

Specify the subscriber policy type information.

Must be one of the following:

- **local**
- **pcf**

rat *rat_type*

Specify the RAT type.

Must be a string of 2, 4, or 7 characters.

roaming-status *ue_roaming_status*

Specify the UE roaming status.

Must be a string of 5, 6, 10, or 11 characters.

smf *smf_address*

Specify address of the SMF.

Must be a string of 7-39 characters.

supi *supi_id*

Specify the subscriber's SUPI ID.

Must be a string.

udm-sdm *udm_sdm_address*

Specify the UDM-SDM address.

Must be a string of 7-39 characters.

udm-sdm *udm_uecm_address*

Specify the UDM-UECM address.

Must be a string of 7-39 characters.

ue-type *ue_type*

Specify device capability - 4G-only / NR-capable.

Must be a string of 7, or 10 characters.

upf *upf_address*

Specify the UPF address.

Must be a string of 7-39 characters.

Usage Guidelines Use this command to view subscriber information by SUPI, IMEI, or all.

show subscriber count-opt

Displays subscriber session count information.

Command Modes Exec

Syntax Description **show subscriber count { all | access** *access_technology* **| amf** *amf_address* **| apn** *apn_name* **| auth-status** *radius_auth_status* **| chf** *chf_address* **| connectivity** *connectivity_type* **| dnn** *dnn_value* **| emergency { false | true } | gpsi** *gpsi* **| gtp-peer** *gtp_peer_address* **| ipv4-addr** *ipv4_address* **| ipv4-pool** *ipv4_pool_name* **| ipv4-range** *ipv4_address_range* **| ipv6-pfx** *ipv6_prefix* **| ipv6-pool** *ipv6_pool_name* **| ipv6-range** *ipv6_prefix_range* **| msid** *msid* **| msisdn** *msisdn* **| pcf** *pcf_address* **| peerGtpuEpKey** *gtpu_peer_address* **| pei** *permanent_equipment_id* **| policy** *policy_type* **| psid** *pdu_session_id* **| rat** *rat_type* **| roaming-status** *ue_roaming_status* **| supi** *supi* **| udm-sdm** *udm_sdm_address* **| udm-uecm** *udm_uecm_address* **| upf** *upf_address* **}**

access *access_technology*

Specify the access technology.

Must be a string of 11-25 characters.

all

Specify all SUPIs.

amf *amf_address*

Specify the AMF address.

Must be a string of 7-39 characters.

apn *apn_name*

Specify name of the APN.

Must be a string of 1-255 characters.

auth-status *radius_auth_status*

Specify the RADIUS authentication status - authenticated or unauthenticated.

Must be a string of 13, or 15 characters.

chf *chf_address*

Specify the CHF address.

Must be a string of 7-39 characters.

connectivity *connectivity_type*

Specify the connectivity type.

Must be a string of 2 characters.

dnn *dnn_value*

Specify the DNN value.

Must be a string of 1-255 characters.

emergency { false | true }

Specify emergency session indication.

Must be one of the following:

- **false**
- **true**

gpsi *gpsi*

Specify the Generic Public Subscription Identifier (GPSI).

Must be a string.

gtp-peer *gtp_peer_address*

Specify address of the GTP peer.

Must be a string of 7-39 characters.

ipv4-addr *ipv4_address*

Specify the IPv4 address in the format *pool_name*/*ipv4_address*.

Must be a string of 1-255 characters.

ipv4-pool *ipv4_pool_name*

Specify name of the IPv4 pool.

Must be a string of 1-255 characters.

ipv4-range *ipv4_address_range*

Specify the IPv4 address range in the format *pool_name*/*start_ip_address*.

Must be a string of 1-255 characters.

ipv6-pfx *ipv6_pfx*

Specify the IPv6 prefix in the format *pool_name*/*ipv6_prefix*.

Must be a string of 1-255 characters.

ipv6-pool *ipv6_pool_name*

Specify name of the IPv6 pool.

Must be a string of 1-255 characters.

ipv6-range *ipv6_prefix_range*

Specify the IPv6 prefix range in the format *pool_name*/*start_prefix*.

Must be a string of 1-255 characters.

msid *msid*

Specify the Mobile Station Identifier (MSID).

Must be a string.

msisdn *msisdn*

Specify the Mobile Station International Subscriber Directory Number (MSISDN).

Must be a string.

pcf *pcf_address*

Specify the PCF address.

Must be a string of 7-39 characters.

peerGtpuEpKey *gtpu_peer_address*

Specify address of the GTPU peer in the *upf_addr:gptu_peer_addr* format.

Must be a string of 1-255 characters.

pei *permanent_equipment_id*

Specify the Permanent Equipment Identifier.

Must be a string of 1-255 characters.

policy *policy_type*

Specify the subscriber policy type information.

Must be one of the following:

- **local**
- **pcf**

psid *pdu_session_id*

Specify the PDU Session Identifier.

Must be an integer in the range of 1-255.

rat *rat_type*

Specify the RAT type.

Must be a string of 2, 4, or 7 characters.

roaming-status *ue_roaming_status*

Specify the UE roaming status.

Must be a string of 5, 6, 10, or 11 characters.

smf *smf_address*

Specify address of the SMF.

Must be a string of 7-39 characters.

supi *supi*

Specify the Subscription Permanent Identifier (SUPI), the value must include the IMSI prefix.

Must be a string.

udm-sdm *udm_sdm_address*

Specify the UDM-SDM address.

Must be a string of 7-39 characters.

udm-sdm *udm_uecm_address*

Specify the UDM-UECM address.

Must be a string of 7-39 characters.

ue-type *ue_type*

Specify device capability - 4G-only / NR-capable.

Must be a string of 7, or 10 characters.

upf *upf_address*

Specify the UPF address.

Must be a string of 7-39 characters.

Usage Guidelines Use this command to view subscriber session count information.

show subscriber debug-opt

Displays debug option.

Command Modes Exec

Syntax Description **debug-opt { supi** *supi* **| msid** *msid* **| pei** *pei_imei* **| gpsi** *gpsi* **| msisdn** *msisdn* **| imsi** *imsi* **}**

gpsi *gpsi*

Specify the GPSI.

Must be a string.

imsi *imsi*

Specify the International Mobile Subscriber Identifier (IMSI).

Must be a string.

msid *msid*

Specify the Mobile Station Identifier (MSID).

Must be a string.

msisdn *msisdn*

Specify the Mobile Station International Subscriber Directory Number (MSISDN).

Must be a string.

pei *pei_imei*

Specify the Permanent Equipment Identifier (PEI)/International Mobile Equipment Identifier (IMEI).

Must be a string.

psid *psid*

Specify the PDU Session ID.

Must be an integer in the range of 1-255.

supi *supi*

Specify the Subscription Permanent Identifier (SUPI), the value must include the IMSI prefix.

Must be a string.

Usage Guidelines Use this command to view debug option.

show subscriber gpsi-opt policy-opt

Displays policy option.

Command Modes Exec

Syntax Description **show subscriber supi** *supi_id* **policy** *policy_option*

policy *policy_option*

Specify the policy option.

Must be one of the following:

- **flow**
- **rules**

Usage Guidelines Use this command to view policy option.

show subscriber imsi-opt

Displays subscriber data based on IMSI.

Command Modes Exec

Syntax Description **show subscriber imsi-options** *imsi_option*

imsi-options *imsi_option*

Specify the IMSI option.

Must be one of the following:

- **full**

Usage Guidelines Use this command to view subscriber data based on IMSI.

show subscriber msid-opt policy-opt

Displays policy option.

Command Modes Exec

Syntax Description **show subscriber supi** *supi_id* **policy** *policy_option*

policy *policy_option*

Specify the policy option.

Must be one of the following:

- **flow**
- **rules**

Usage Guidelines Use this command to view policy option.

show subscriber msisdn-opt policy-opt

Displays policy option.

Command Modes Exec

Syntax Description **show subscriber supi** *supi_id* **policy** *policy_option*

policy *policy_option*

Specify the policy option.

Must be one of the following:

- **flow**
- **rules**

Usage Guidelines Use this command to view policy option.

show subscriber pei-opt policy-opt

Displays policy option.

Command Modes Exec

Syntax Description **show subscriber supi** *supi_id* **policy** *policy_option*

policy *policy_option*

Specify the policy option.

Must be one of the following:

- **flow**
- **rules**

Usage Guidelines Use this command to view policy option.

show subscriber supi-opt

Displays subscriber data.

Command Modes Exec

Syntax Description **show subscriber supi [** *detail_option* **| psid** *pdu_session_id* **]**

psid *pdu_session_id*

Specify the PDU Session ID.

Must be an integer in the range of 1-255.

detail_option

Specify the detail option.

Must be one of the following:

- **charging**
- **full**
- **policy**
- **summary**
- **userplane**

Usage Guidelines Use this command to view subscriber data.

show subscriber supi-opt policy-opt

Displays policy option.

Command Modes Exec

Syntax Description **show subscriber supi** *supi_id* **policy** *policy_option*

policy *policy_option*

Specify the policy option.

Must be one of the following:

- **flow**
- **rules**

Usage Guidelines Use this command to view policy option.

show userplane userplane

Displays userplane information.

Command Modes Exec

Syntax Description **show userplane all**

all

Specify all.

Usage Guidelines Use this command to view userplane information.

show vrf-info

Displays information about Virtual Routing and Forwarding (VRF).

Command Modes Exec

Syntax Description **`show vrf-info [ all | ipv4 | ipv6 ]`**

all

Show details for all VRFs.

ipv4

Show details for VRFs associated with the IPv4 address family.

ipv6

Show details for VRFs associated with the IPv6 address family.

Usage Guidelines Use this command to view VRF information. You can filter the output by selecting all VRFs, IPv4 VRFs, or IPv6 VRFs. If no option is specified, the command displays all VRF details.

show vrf-route-info

Displays detailed routing information for Virtual Routing and Forwarding (VRFs).

Command Modes Exec

Syntax Description **`show vrf-route-info [ ipv4 | ipv6 | name`** *`vrf_name`* **`]`**

ipv4

Option to display routing information for the IPv4 address family.

ipv6

Option to display routing information for the IPv6 address family.

name *vrf_name*

Specify the Virtual Routing and Forwarding (VRF) of the advertised routes. *vrf_name* must be a valid VRF name string.

Usage Guidelines Use this command to view the VRF routing information. You can filter the output by choosing the IPv4 or IPv6 address family or by specifying a particular VRF name. If no option is specified, the command displays all VRF routing details.

show-defaults

Displays the default configuration.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description

```
show-defaults { false | true }
```

{ false | true }

Specify whether to display or hide the default values. To display, select true. Otherwise, select false.

Must be either "false" or "true".

Usage Guidelines Use this command to view the default configuration.

show confd-state

Displays ConfD status information.

Command Modes Exec

Syntax Description

```
show confd-state
```

show confd-state

Shows the current status information of the ConfD service.

Usage Guidelines Use this command to view ConfD status information.

show dns-cache

Displays DNS cache information.

Command Modes Exec

Syntax Description

```
show dns-cache
```

show dns-cache

Shows the current contents of the DNS cache, including cached domain name resolutions and related details.

Usage Guidelines Use this command to view DNS cache information.

show dns-query

Displays FQDN resolution.

Command Modes Exec

Syntax Description `show dns-query`

show dns-query

Shows the resolution details of Fully Qualified Domain Names (FQDN), including information about recent DNS queries and their resolved IP addresses.

Usage Guidelines Use this command to view FQDN resolution.

show gtpp-ep

Displays information related to GTPP CDR.

Command Modes Exec

Syntax Description `show gtpp-ep`

show gtpp-ep

Shows information related to GTPP CDR (Call Detail Record) file operations, such as the status, details, or summary of existing GTPP CDR files.

Usage Guidelines Use this command to view information related to GTPP CDR.

show helm

Displays helm configuration parameters.

Command Modes Exec

Syntax Description `show helm`

show helm

Shows the current helm configuration parameters, including settings and values used for helm deployments and management.

Usage Guidelines Use this command to view helm configuration parameters.

show history

Displays CLI command history.

Command Modes Exec

Syntax Description `show history`

show history

Shows the the history of previously executed CLI commands in the current session.

Usage Guidelines Use this command to view CLI command history.

show jobs

Displays background jobs.

Command Modes Exec

Syntax Description `show jobs`

show jobs

Shows a list of background jobs currently running or suspended in the system.

Usage Guidelines Use this command to view background jobs.

show last-logins

Displays last logged in users.

Command Modes Exec

Syntax Description `show last-logins`

show last-logins

Shows information about the most recent user login attempts, including details of the last users who logged into the system.

Usage Guidelines Use this command to view last logged in users.

show license

Displays licensing information.

Command Modes Exec

Syntax Description `show license`

show license

Shows licensing information for the system, including current license status, types, and expiration details.

Usage Guidelines Use this command to view licensing information.

show local-interface-status

Displays local interface status.

Command Modes Exec

Syntax Description `show local-interface-status`

show local-interface-status

Shows the status and details of all local network interfaces, including their operational state, IP addresses, and other relevant information.

Usage Guidelines Use this command to view local interface status.

show mode

Displays privelege based operational CLI.

Command Modes Exec

Syntax Description `show mode`

show mode

Shows the current operational mode of the CLI based on user privilege level.

Usage Guidelines Use this command to view privelege based operational CLI.

show nacm

Displays Network Access Control Model (NACM) settings and information.

Command Modes Exec

Syntax Description `show nacm`

show nacm

Shows Network Access Control Model (NACM) settings and information, including user permissions and access control configurations.

Usage Guidelines Use this command to view Network Access Control Model (NACM) settings and information.

show netconf-state

Displays NETCONF statistics.

Command Modes Exec

Syntax Description `show netconf-state`

show netconf-state

Shows statistics and status information about NETCONF operations, including session details, message counts, and related metrics.

Usage Guidelines Use this command to view NETCONF statistics.

show nf-tls

Displays TLS keystore configuration for interfaces.

Command Modes Exec

Syntax Description `show nf-tls`

show nf-tls

Shows the TLS keystore configuration for network interfaces, including details about certificates, keys, and their status used for securing interface communications.

Usage Guidelines Use this command to view TLS keystore configuration for interfaces.

show notification

Displays system notifications.

Command Modes Exec

Syntax Description `show notification`

show notification

Shows system notifications, including recent alerts and messages generated by the system.

Usage Guidelines Use this command to view system notifications.

show nrf

Displays operational data for the NRF.

Command Modes Exec

Syntax Description `show nrf`

show nrf

Shows operational data for the NRF client, including status, registrations, and related information.

Usage Guidelines Use this command to view operational data for the NRF.

show ops

Displays a list of ops centers installed in the cluster.

Command Modes Exec

Syntax Description `show ops`

show ops

Shows a list of ops centers installed in the cluster, including their names, statuses, and relevant details.

Usage Guidelines Use this command to view list of ops centers installed in the cluster.

show overload-info

Displays system overload information.

Command Modes Exec

Syntax Description `show overload-info`

show overload-info

Shows system overload information, including current overload status, affected components, and relevant metrics.

Usage Guidelines Use this command to view system overload information.

show parser

Displays information about the system parser.

Command Modes Exec

Syntax Description `show parser`

show parser

Shows information about the system parser, including its current status, configuration, and recent parsing activities.

Usage Guidelines Use this command to view information about the system parser.

show pcscf

Displays information about failed Proxy-Call Session Control Function (P-CSCF) addresses.

Command Modes Exec

Syntax Description `show pcscf`

show pcscf

Shows information about failed P-CSCF addresses, including details on failures and their statuses.

Usage Guidelines Use this command to view information about failed Proxy-Call Session Control Function (P-CSCF) addresses.

show resources

Displays system resource information.

Command Modes Exec

Syntax Description `show resources`

show resources

Shows system resource information, including CPU, memory, storage usage, and other relevant resource metrics.

Usage Guidelines Use this command to view system resource information.

show restconf-state

Displays statistics and status information about RESTCONF operations.

Command Modes Exec

Syntax Description **show restconf-state**

show restconf-state

Shows statistics and status information about RESTCONF operations, including session details, request counts, and related metrics.

Usage Guidelines Use this command to view statistics and status information about RESTCONF operations.

show running-config

Displays the current active configuration of the system.

Command Modes Exec

Syntax Description **show running-config**

show running-config

Shows the current active configuration of the system, including all runtime settings and parameters.

Usage Guidelines Use this command to view the current active configuration of the system.

smiuser

Configures the Subscriber Microservices Infrastructure (SMI) user account parameters.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **smiuser { add-group groupname** *group_name* **| add-user { username** *username* **| password** *password* **} | change-password { username** *username* **| current_password** *current_password* **| new_password** *new_password* **| confirm_password** *new_password* **| password_expire_days** *expire_days* **} | change-self-password { current_password** *current_password* **| new_password** *new_password* **| confirm_password** *new_password* **| password_expire_days** *expire_days* **} | delete-group groupname** *group_name* **| delete-user username** *username* **| unassign-user-group { groupname** *groupname_pam* **| username** *username_pam* **} | update-password-length length** *password_length* **}**

username *username*

Specify the username.

Must be a string.

password *password*

Specify the user password.

Must be a string.

confirm_password *new_password*

Confirm the new password.

Must be a string.

current_password *current_password*

Specify the current password.

Must be a string.

new_password *new_password*

Specify the new password.

Must be a string.

password_expire_days *expire_days*

Specify the number of days before the password expires.

Must be an integer.

groupname *group_name*

Specify the group name.

Must be a string.

groupname *groupname_pam*

Specify the group name in PAM.

Must be a string.

username *username_pam*

Specify the user name in PAM.

Must be a string.

length *password_length*

Specify the minimum password length.

Must be an integer.

Usage Guidelines Use this command to configure the smiuser parameters.

system

Configures the NF's system operations.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **`system { ops-center stop | synch { start | stop } | upgrade | uuid-override new-uuid`** *`uuid_value`* **`}`**

ops-center stop

Stop the synching of configuration.

synch { start | stop }

Starts or stops the synching of configuration,

upgrade

Initiates the upgrade of a product.

uuid-override new-uuid *uuid_value*

Change the Universally Unique Identifier (UUID) to a new value.

Must be a string.

Usage Guidelines Use this command to display the NF's system operations.

system-diagnostics event-trace

Configures Event Trace configuration.

Syntax Description **`system-diagnostics event-trace`** *`event_trace_state`*

event-trace *event_trace_state*

Specify to enable or disable Event Trace configuration.

Must be one of the following:

- **disable**
- **enable**

Usage Guidelines Use this command to enable or disable Event Trace configuration.

system-diagnostics idmgr-secondary-recon

Configures to trigger secondary reconciliation in NodeMgr using unique key.

Command Modes Exec > Global Configuration (config)

Syntax Description `system-diagnostics idmgr-secondary-recon { false | true }`

idmgr-secondary-recon { false | true }

Triggers secondary reconciliation in NodeMgr using unique key.

Usage Guidelines Use this command to enable or disable secondary reconciliation in NodeMgr using unique key.

system-diagnostics ip-validation

Configures IP address validation with CDL.

Syntax Description `ip-validation { enable | ignore-mismatch-responses }`

enable

Specify to enable new IP address validation with CDL.

ignore-mismatch-responses

Specify to ignore CDL inconsistencies during address validation.

Usage Guidelines Use this command to configure IP address validation with CDL.

system-diagnostics pod type

Configures and enables your required pod from a cluster of the supported pods.

Command Modes Exec > Global Configuration (config)

Syntax Description `system-diagnostics` *`pod_type`*

pod_type

Specify the required type of service pods for system diagnostics.

Must be one of the following:

- diameter
- gtp
- pfcp

- service
- sgw-service

Usage Guidelines Use this command to enable and configure your required pod from a cluster of the supported pods.

system-diagnostics pod type fault

Enables system fault panic recovery while session processing.

Command Modes Exec > Global Configuration (config) > System Diagnostics Configuration (config-system-diagnostics-*pod_type*)

Syntax Description **fault { action** *action_on_fault* **| file-detail** *file_names_line_numbers* **| interval** *interval_duration* **| num** *max_fault_tolerance* **}**

action *action_on_fault*

Specify the action to take on fault occurence.

Must be one of the following:

- **abort**
- **cleanup**
- **graceful-Reload**
- **reload**

file-detail *file_names_line_numbers*

Specify the list of file names with line number to exclude from recovery. For example, procedures/pduim/procedure.go:1902.

Must be a string.

You can configure a maximum of 10 elements with this keyword.

interval *interval_duration*

Specify the duration of the interval in minutes.

Must be an integer in the range of 1-3600.

num *max_fault_tolerance*

Specify the maximum number of times fault can be tolerated in an interval.

Must be an integer in the range of 0-50.

Usage Guidelines Use this command to enable and configure system fault panic recovery while session processing.

system-diagnostics protocol supi

Configures the list of SUPI values for which config has to be applied.

Syntax Description **supi** *subscription_permanent_id*

subscription_permanent_id

Specify the Subscription Permanent Identifier (SUPI).

Must be an integer in the range of 100000000000000-999999999999999.

Usage Guidelines Use this command to configure the list of SUPI values for which config has to be applied.

system-diagnostics protocol supi preferred-up

Configures the preferred user plane node ID.

Syntax Description **preferred-up node-id** *node_id*

node-id *node_id*

Specify node ID of the preferred user plane node.

Must be a string.

Usage Guidelines Use this command to configure the preferred user plane node ID.

system-diagnostics session-consistency

Enables and configures inconsistency checks on session data.

Syntax Description **system-diagnostics session-consistency action** *action_on_inconsistent_data*

action *action_on_inconsistent_data*

Specify the action to take on inconsistent data.

Must be one of the following:

- **cleanup**
- **disabled**
- **monitor**

Usage Guidelines Use this command to enable and configure inconsistency checks on session data.

terminal

Configures the type of terminal.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description **terminal** *terminal_type*

terminal_type

Specify the terminal type.

Must be one of the following:

- ansi
- generic
- linux
- vt100
- xterm

Usage Guidelines Use this command to configure the terminal type.

test dns-query

Tests FQDN resolution.

Command Modes Exec

Syntax Description **test dns-query { fqdn** *fqdn* **| num-ipv4** *ipv4_count* **| num-ipv4v6** *ipv4v6_count* **| num-ipv6** *ipv6_count* **}**

fqdn *fqdn*

Specify the Fully Qualified Domain Name (FQDN) of the node for which DNS query has to be sent.

Must be a string of 1-255 characters.

num-ipv4 *ipv4_count*

Specify the number of IPv4 to be used for DNS query.

Must be an integer in the range of 1-9.

num-ipv4v6 *ipv4v6_count*

Specify the number of IPv4v6 to be used for DNS query.

Must be an integer in the range of 1-9.

num-ipv6 *ipv6_count*

Specify the number of IPv6 to be used for DNS query.

Must be an integer in the range of 1-9.

Usage Guidelines Use this command to test FQDN of the node for which dns query has to be sent.

test gtpc echo

Tests the connectivity of GTP-C peer nodes.

Command Modes Exec

Syntax Description **test gtpc echo instance-id** *instance_id* **interface** *interface_type* **peer-address** *ip_address*

instance-id *instance_id*

Specifies the instance ID of a GR instance that is configured on the system.

interface *interface_type*

Specifies the type of GTP-C interface, such as S11, S5e, S5, S2b, or S8.

peer-address *ip_address*

Specifies IPv4 or IPv6 address of a specific peer to which GTP-C echo request is sent.

Usage Guidelines Use this command to test connectivity of GTP-C peer nodes.

test gtpp echo

Tests the connectivity of a CGF server that is not configured in a GTPP profile.

Command Modes Exec

Syntax Description **test gtpp echo instance-id** *instance_id* **ca-address** *ip_address* **[ca-port** *port* **]** **[cgf-address** *ip_address* **] [cgf-port** *port* **]**

instance-id *instance_id*

Specifies the instance ID of a GR instance that is configured on the system.

ca-address *ip_address*

Specifies the IPv4 address of charging agent configured within GTPP profile.

ca-port *port*

Specifies the port of charging agent configured within GTPP profile, ranging 1–65535. By default, the port is 49999.

cgf-address *ip_address*

Specifies the IPv4 address of a specific CGF server to which GTPP echo request is sent.

cgf-port *port*

Specifies the port of CGF server, ranging from 1– 65535. By default, the port is 3386.

Usage Guidelines Use this command to check the connectivity of CGF server.

test-radius accounting

Tests RADIUS accounting server function.

Command Modes Exec

Syntax Description **test-radius accounting { all [[client-nas** *ip_address* **] [username** *user_name* **]] | server** *server_ip_address* **[[client-nas** *ip_address* **] [port** *port_number* **] [username** *user_name* **]] | server-group [[client-nas** *ip_address* **] [username** *user_name* **]] }**

all

Specify to test all configured servers.

Must be one of the following:

- **all**

client-nas *ip_address*

Specify IP address of the client NAS.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

port *server_port_number*

Specify the port number of the RADIUS server.

Must be an integer in the range of 1-65535.

server-group *server_group_name*

Specify name of the server group.

Must be a string of 1-64 characters.

server *server_ip_address*

Specify the IP address of the RADIUS server.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

username *user_name*

Specify the user name.

Must be a string of 1-64 characters.

Default Value: test.

Usage Guidelines

Use this command to test RADIUS accounting server function.

test-radius authentication

Tests RADIUS authentication server function.

Command Modes

Exec

Syntax Description

test-radius authentication { all [[client-nas *ip_address* **] [password** *password* **] [username** *user_name* **]] | server** *server_ip_address* **[[client-nas** *ip_address* **] [password** *password* **] [port** *port_number* **] [username** *user_name* **]] | server-group [[client-nas** *ip_address* **] [password** *password* **] [username** *user_name* **]] }**

all

Specify to test all configured servers.

Must be one of the following:

- **all**

client-nas *ip_address*

Specify IP address of the client NAS.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

password *password*

Specify the password for user with authentication verified.

Must be a string of 1-64 characters.

Default Value: test.

port *server_port_number*

Specify the port number of the RADIUS server.

Must be an integer in the range of 1-65535.

server-group *server_group_name*

Specify name of the server group.

Must be a string of 1-64 characters.

server *server_ip_address*

Specify the IP address of the RADIUS server.

Must be a string in the ipv4-address pattern. For information on the ipv4-address pattern, see the *Input Pattern Types* chapter.

-Or-

Must be a string in the ipv6-address pattern. For information on the ipv6-address pattern, see the *Input Pattern Types* chapter.

username *user_name*

Specify the user name.

Must be a string of 1-64 characters.

Default Value: test.

Usage Guidelines Use this command to test RADIUS authentication server function.

timestamp

Configures the timestamp parameters.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description

```
timestamp { disable | enable }
```

{ disable | enable }

Enable or disable the timestamp display.

Usage Guidelines Use this command to configure the timestamp.

who

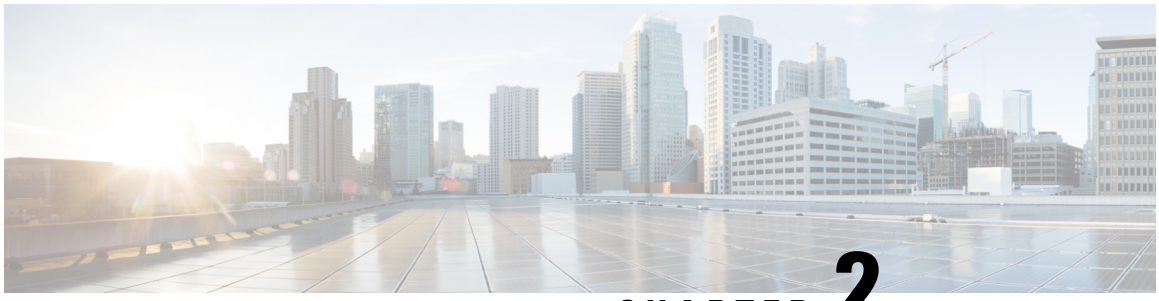
Displays information on currently logged on users.

Privilege Security Administrator, Administrator

Command Modes Exec

Syntax Description `who`

Usage Guidelines Use this command to view information on currently logged on users. The command output displays the Session, User, Context, From (IP address), Protocol, Date, and Mode information.



CHAPTER 2

Input Pattern Types

- arg-type, on page 633
- crypt-hash, on page 634
- date-and-time, on page 635
- domain-name, on page 635
- dotted-quad, on page 636
- hex-list, on page 636
- hex-string, on page 637
- ipv4-address, on page 637
- ipv4-address-and-prefix-length, on page 637
- ipv4-address-no-zone, on page 637
- ipv4-prefix, on page 637
- ipv6-address, on page 638
- ipv6-address-and-prefix-length, on page 638
- ipv6-address-no-zone, on page 639
- ipv6-prefix, on page 639
- mac-address, on page 640
- object-identifier, on page 640
- object-identifier-128, on page 640
- octet-list, on page 641
- phys-address, on page 641
- sha-256-digest-string, on page 641
- sha-512-digest-string, on page 642
- size, on page 642
- uuid, on page 643
- yang-identifier, on page 643

arg-type

```
Pattern:
'[^\*].*|..+'; // must not be single '*'

Pattern:
'\*'
```

This statement can be used to hide a node from some, or all, northbound interfaces. All nodes with the same value are considered a hide group and are treated the same with regards to being visible or not in a northbound interface.

A node with an hidden property is not shown in the northbound user interfaces (CLI and Web UI) unless an 'unhide' operation is performed in the user interface.

The hidden value 'full' indicates that the node must be hidden from all northbound interfaces, including programmatical interfaces such as NETCONF. The value '*' is not valid. A hide group can be unhidden only if this is explicitly allowed in the confd.conf(5) daemon configuration.

Multiple hide groups can be specified by giving this statement multiple times. The node is shown if any of the specified hide groups is given in the 'unhide' operation. If a mandatory node is hidden, a hook callback function (or similar) might be needed in order to set the element

crypt-hash

```
Pattern:
'$0$.*'
  '|$1$[a-zA-Z0-9./]{1,8}$[a-zA-Z0-9./]{22}'
  '|$5$(rounds=\d+$)?[a-zA-Z0-9./]{1,16}$[a-zA-Z0-9./]{43}'
  '|$6$(rounds=\d+$)?[a-zA-Z0-9./]{1,16}$[a-zA-Z0-9./]{86}'
```

The **crypt-hash** type is used to store passwords using a hash function. The algorithms for applying the hash function and encoding the result are implemented in various UNIX systems as the function crypt(3).

A value of this type matches one of the forms:

- 0<clear text password>
- $<id>$<salt>$<password hash>
- $<id>$<parameter>$<salt>$<password hash>

The '0' prefix signals that the value is clear text. When such a value is received by the server, a hash value is calculated, and the string '$<id>$<salt>$' or $<id>$<parameter>$<salt>$ is prepended to the result. This value is stored in the configuration data store.

If a value starting with '$<id>$', where <id> is not '0', is received, the server knows that the value already represents a hashed value, and stores it as is in the data store.

When a server needs to verify a password given by a user, it finds the stored password hash string for that user, extracts the salt, and calculates the hash with the salt and given password as input. If the calculated hash value is the same as the stored value, the password given by the client is accepted.

This type defines the following hash functions:

Id	Hash Function	Feature
1	MD5	crypt-hash-md5
5	SHA-256	crypt-hash-sha-256
6	SHA-512	crypt-hash-sha-512

The server indicates support for the different hash functions by advertising the corresponding feature.

Reference:

- IEEE Std 1003.1-2008 - crypt() function
- RFC 1321: The MD5 Message-Digest Algorithm
- FIPS.180-3.2008: Secure Hash Standard

date-and-time

```
Pattern:
'\d{4}-\d{2}-\d{2}T\d{2}:\d{2}:\d{2}(\.\d+)?'
 '(Z|[\+\-]\d{2}:\d{2})'
```

The date-and-time type is a profile of the ISO 8601 standard for representation of dates and times using the Gregorian calendar. The profile is defined by the date-time production in Section 5.6 of RFC 3339. The date-and-time type is compatible with the dateTime XML schema type with the following notable exceptions:

1. The date-and-time type does not allow negative years.
2. The date-and-time time-offset -00:00 indicates an unknown time zone (see RFC 3339) while -00:00 and +00:00 and Z all represent the same time zone in dateTime.
3. The canonical format (see below) of data-and-time values differs from the canonical format used by the dateTime XML schema type, which requires all times to be in UTC using the time-offset 'Z'.

This type is not equivalent to the DateAndTime textual convention of the SMIv2 since RFC 3339 uses a different separator between full-date and full-time and provides higher resolution of time-secfrac. The canonical format for date-and-time values with a known time zone uses a numeric time zone offset that is calculated using the device's configured known offset to UTC time.

A change of the device's offset to UTC time will cause date-and-time values to change accordingly. Such changes might happen periodically in case a server follows automatically daylight saving time (DST) time zone offset changes. The canonical format for date-and-time values with an unknown time zone (usually referring to the notion of local time) uses the time-offset -00:00.

Reference:

- RFC 3339: Date and Time on the Internet: Timestamps
- RFC 2579: Textual Conventions for SMIv2
- XSD-TYPES: XML Schema Part 2: Datatypes Second Edition

domain-name

```
Pattern:
'((([a-zA-Z0-9_]([a-zA-Z0-9\-_]){0,61})?[a-zA-Z0-9]\.)*'
 '([a-zA-Z0-9_]([a-zA-Z0-9\-_]){0,61})?[a-zA-Z0-9]\.?)'
 '|\.'
```

The domain-name type represents a DNS domain name. The name must fully qualified whenever possible. Internet domain names are only loosely specified. Section 3.5 of RFC 1034 recommends a syntax (modified in Section 2.1 of RFC 1123). The Pattern above is intended to allow for current practice in domain name use, and some possible future expansion. It is designed to hold various types of domain names, including names used for A or AAAA records (host names) and other records, such as SRV records.

The Internet host names have a stricter syntax (described in RFC 952) than the DNS recommendations in RFCs 1034 and 1123, and that systems that want to store host names in schema nodes using the domain-name type are recommended to adhere to this stricter standard to ensure interoperability.

The encoding of DNS names in the DNS protocol is limited to 255 characters. Since the encoding consists of labels prefixed by a length bytes and there is a trailing NULL byte, only 253 characters can appear in the textual dotted notation.

The description clause of schema nodes using the domain-name type must describe when and how these names are resolved to IP addresses. The resolution of a domain-name value may require to query multiple DNS records. For example, A for IPv4 and AAAA for IPv6. The order of the resolution process and which DNS record takes precedence can either be defined explicitly or may depend on the configuration of the resolver.

Domain-name values use the US-ASCII encoding. Their canonical format uses lowercase US-ASCII characters. Internationalized domain names MUST be A-labels as per RFC 5890.

Reference:

- RFC 952: DoD Internet Host Table Specification
- RFC 1034: Domain Names - Concepts and Facilities
- RFC 1123: Requirements for Internet Hosts -- Application and Support
- RFC 2782: A DNS RR for specifying the location of services (DNS SRV)
- RFC 5890: Internationalized Domain Names in Applications (IDNA): Definitions and Document Framework

dotted-quad

Pattern:

```
'(([0-9]|[1-9][0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5])\.){3}'
 '([0-9]|[1-9][0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5])'
```

An unsigned 32-bit number expressed in the dotted-quad notation, that is, four octets written as decimal numbers and separated with the '.' (full stop) character.

hex-list

Pattern:

```
'(([0-9a-fA-F]){2}(:([0-9a-fA-F]){2})*)?'
```

DEPRECATED: Use yang:hex-string instead. There are no plans to remove tailf:hex-list. A list of colon-separated hexa-decimal octets, for example '4F:4C:41:71'.

The statement tailf:value-length can be used to restrict the number of octets. Using the 'length' restriction limits the number of characters in the lexical representation

hex-string

Pattern:
'([0-9a-fA-F]{2}(:[0-9a-fA-F]{2})*)?'

A hexadecimal string with octets represented as hex digits separated by colons. The canonical representation uses lowercase characters.

ipv4-address

Pattern:
'(([0-9]|[1-9][0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5])\.){3}'
'([0-9]|[1-9][0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5])'
'(%[\p{N}\p{L}]+)?'

The ipv4-address type represents an IPv4 address in dotted-quad notation. The IPv4 address may include a zone index, separated by a % sign. The zone index is used to disambiguate identical address values. For link-local addresses, the zone index will typically be the interface index number or the name of an interface. If the zone index is not present, the default zone of the device will be used. The canonical format for the zone index is the numerical format.

ipv4-address-and-prefix-length

Pattern:
'(([0-9]|[1-9][0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5])\.){3}'
'([0-9]|[1-9][0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5])'
'/(([0-9])|([1-2][0-9])|(3[0-2]))'

The ipv4-address-and-prefix-length type represents a combination of an IPv4 address and a prefix length. The prefix length is given by the number following the slash character and must be less than or equal to 32.

ipv4-address-no-zone

Pattern:
'[0-9\.]*'

An IPv4 address is without a zone index and derived from ipv4-address that is used in situations where the zone is known from the context and hence no zone index is needed.

ipv4-prefix

Pattern:
'(([0-9]|[1-9][0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5])\.){3}'
'([0-9]|[1-9][0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5])'
'/(([0-9])|([1-2][0-9])|(3[0-2]))'

The ipv4-prefix type represents an IPv4 address prefix. The prefix length is given by the number following the slash character and must be less than or equal to 32.

A prefix length value of 'n' corresponds to an IP address mask that has n contiguous 1-bits from the most significant bit (MSB) and all other bits set to 0.

The canonical format of an IPv4 prefix has all bits of the IPv4 address set to zero that are not part of the IPv4 prefix.

ipv6-address

```
Pattern:
'((:|[0-9a-fA-F]{0,4}):)([0-9a-fA-F]{0,4}:){0,5}'
  '(([0-9a-fA-F]{0,4}:)?(:|[0-9a-fA-F]{0,4}))|'
  '((25[0-5]|2[0-4][0-9]|[01]?[0-9]?[0-9])\.){3}'Pattern:
  '(25[0-5]|2[0-4][0-9]|[01]?[0-9]?[0-9])))'
  '(%[\p{N}\p{L}]+)?'
```

```
Pattern:
'(([^:]+:){6}(([^:]+:[^:]+)|(.*\..*)))|'
 '(([^:]+:)*[^:]+)?::(([^:]+:)*[^:]+)?)'
 '(%.+)?'
```

The ipv6-address type represents an IPv6 address in full, mixed, shortened, and shortened-mixed notation. The IPv6 address may include a zone index, separated by a % sign.

The zone index is used to disambiguate identical address values. For link-local addresses, the zone index will typically be the interface index number or the name of an interface. If the zone index is not present, the default zone of the device will be used.

The canonical format of IPv6 addresses uses the textual representation defined in Section 4 of RFC 5952. The canonical format for the zone index is the numerical format as described in Section 11.2 of RFC 4007.

Reference:

- RFC 4291: IP Version 6 Addressing Architecture
- RFC 4007: IPv6 Scoped Address Architecture
- RFC 5952: A Recommendation for IPv6 Address Text Representation

ipv6-address-and-prefix-length

```
Pattern:
'((:|[0-9a-fA-F]{0,4}):)([0-9a-fA-F]{0,4}:){0,5}'
 '(([0-9a-fA-F]{0,4}:)?(:|[0-9a-fA-F]{0,4}))|'
 '((25[0-5]|2[0-4][0-9]|[01]?[0-9]?[0-9])\.){3}'
 '(25[0-5]|2[0-4][0-9]|[01]?[0-9]?[0-9])))'
 '(/(([0-9])|([0-9]{2})|(1[0-1][0-9])|(12[0-8])))'
```

```
Pattern:
'(([^:]+:){6}(([^:]+:[^:]+)|(.*\..*)))|'
```

```
'((([^:]+:)*[^:]+)?::(([^:]+:)*[^:]+)?)'
'(/.+)'
```

The ipv6-address-and-prefix-length type represents a combination of an IPv6 address and a prefix length. The prefix length is given by the number following the slash character and must be less than or equal to 128.

ipv6-address-no-zone

Pattern:

```
'[0-9a-fA-F:\.]*'
```

An IPv6 address without a zone index. This type, derived from ipv6-address, may be used in situations where the zone is known from the context and hence no zone index is needed.

Reference:

- RFC 4291: IP Version 6 Addressing Architecture
- RFC 4007: IPv6 Scoped Address Architecture
- RFC 5952: A Recommendation for IPv6 Address Text Representation

ipv6-prefix

Pattern:

```
'((:|[0-9a-fA-F]{0,4}):)([0-9a-fA-F]{0,4}:){0,5}'
 '((([0-9a-fA-F]{0,4}:)?(:|[0-9a-fA-F]{0,4}))|'
 '(((25[0-5]|2[0-4][0-9]|[01]?[0-9]?[0-9])\.){3}'Pattern:
 '(25[0-5]|2[0-4][0-9]|[01]?[0-9]?[0-9])))'
 '(/(([0-9])|([0-9]{2})|(1[0-1][0-9])|(12[0-8])))';
```

Pattern:

```
'(([^:]+:){6}(([^:]+:[^:]+)|(.*\..*))|'
 '((([^:]+:)*[^:]+)?::(([^:]+:)*[^:]+)?)'
 '(/.+)'
```

The ipv6-prefix type represents an IPv6 address prefix. The prefix length is given by the number following the slash character and must be less than or equal to 128.

A prefix length value of n corresponds to an IP address mask that has n contiguous 1-bits from the most significant bit (MSB) and all other bits set to 0.

The IPv6 address should have all bits that do not belong to the prefix set to zero. The canonical format of an IPv6 prefix has all bits of the IPv6 address set to zero that are not part of the IPv6 prefix. Furthermore, the IPv6 address is represented as defined in Section 4 of RFC 5952

Reference:

- RFC 5952: A Recommendation for IPv6 Address Text Representation

mac-address

Pattern:
'[0-9a-fA-F]{2}(:[0-9a-fA-F]{2}){5}'

The mac-address type represents an IEEE 802 MAC address. The canonical representation uses lowercase characters. In the value set and its semantics, this type is equivalent to the MacAddress textual convention of the SMIv2.

Reference:

- IEEE 802: IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture
- RFC 2579: Textual Conventions for SMIv2

object-identifier

Pattern:
'(([0-1](\.[1-3]?[0-9]))|(2\.(0|([1-9]\d*))))'
'(\.(0|([1-9]\d*)))*'

The object-identifier type represents administratively assigned names in a registration-hierarchical-name tree. The values of this type are denoted as a sequence of numerical non-negative sub-identifier values. Each sub-identifier value MUST NOT exceed 2^32-1 (4294967295). The Sub-identifiers are separated by single dots and without any intermediate whitespace.

The ASN.1 standard restricts the value space of the first sub-identifier to 0, 1, or 2. Furthermore, the value space of the second sub-identifier is restricted to the range 0 to 39 if the first sub-identifier is 0 or 1. Finally, the ASN.1 standard requires that an object identifier has always at least two sub-identifiers. The pattern captures these restrictions.

Although the number of sub-identifiers is not limited, module designers should realize that there may be implementations that stick with the SMIv2 limit of 128 sub-identifiers.

This type is a superset of the SMIv2 OBJECT IDENTIFIER type since it is not restricted to 128 sub-identifiers. Hence, this type SHOULD NOT be used to represent the SMIv2 OBJECT IDENTIFIER type; the object-identifier-128 type SHOULD be used instead.

Reference:

- ISO9834-1: Information technology - Open Systems
- Interconnection - Procedures for the operation of OSI
- Registration Authorities: General procedures and top arcs of the ASN.1 Object Identifier tree

object-identifier-128

Pattern:
'\d*(\.\d*){1,127}'

This type represents object-identifiers restricted to 128 sub-identifiers. In the value set and its semantics, this type is equivalent to the OBJECT IDENTIFIER type of the SMIv2.

Reference:

- RFC 2578: Structure of Management Information Version 2 (SMIv2)

octet-list

Pattern:
'(\d*(.\d*)*)?'

A list of dot-separated octets, for example '192.168.255.1.0'. The statement tailf:value-length can be used to restrict the number of octets. Using the 'length' restriction limits the number of characters in the lexical representation.

phys-address

Pattern:
'([0-9a-fA-F]{2}(:[0-9a-fA-F]{2})*)?'

Represents media- or physical-level addresses represented as a sequence octets, each octet represented by two hexadecimal numbers. Octets are separated by colons. The canonical representation uses lowercase characters. In the value set and its semantics, this type is equivalent to the PhysAddress textual convention of the SMIv2.

Reference:

- RFC 2579: Textual Conventions for SMIv2

sha-256-digest-string

Pattern:
'0.*'
'|5(rounds=\d+$)?[a-zA-Z0-9./]{1,16}$[a-zA-Z0-9./]{43}'

The sha-256-digest-string type automatically computes a SHA-256 digest for a value adhering to this type. A value of this type matches one of the forms:

- 0<clear text password>
- 5<salt>$<password hash>
- 5rounds=<number>$<salt>$<password hash>

The '0' prefix signals that this is plain text. When a plain text value is received by the server, a SHA-256 digest is calculated, and the string '5<salt>$' is prepended to the

result, where <salt> is a random 16 character salt used to generate the digest. This value is stored in the configuration data store. The algorithm can be tuned through the /confdConfig/cryptHash/rounds parameter, which if set to a number other than the default will cause '5rounds=<number>$<salt>$' to be prepended instead of only '5<salt>$'.

If a value starting with '5' is received, the server knows that the value already represents a SHA-256 digest, and stores it as is in the data store.

If a default value is specified, it must have a '5' prefix.

The digest algorithm used is the same as the SHA-256 crypt function used for encrypting passwords for various UNIX systems.

Reference:

- IEEE Std 1003.1-2008 - crypt() function FIPS.180-3.2008: Secure Hash Standard

sha-512-digest-string

Pattern:

```
'$0$.*'
 '|$6$(rounds=\d+$)?[a-zA-Z0-9./]{1,16}$[a-zA-Z0-9./]{86}'
```

The sha-512-digest-string type automatically computes a SHA-512 digest for a value adhering to this type. A value of this type matches one of the forms

- 0<clear text password>
- 6<salt>$<password hash>
- 6rounds=<number>$<salt>$<password hash>

The '0' prefix signals that this is plain text. When a plain text value is received by the server, a SHA-512 digest is calculated, and the string '6<salt>$' is prepended to the

result, where <salt> is a random 16 character salt used to generate the digest. This value is stored in the configuration data store. The algorithm can be tuned through the

/confdConfig/cryptHash/rounds parameter, which if set to a number other than the default will cause '6rounds=<number>$<salt>$' to be prepended instead of only '6<salt>$'.

If a value starting with '6' is received, the server knows that the value already represents a SHA-512 digest, and stores it as is in the data store.

If a default value is specified, it must have a '6' prefix. The digest algorithm used is the same as the SHA-512 crypt function used for encrypting passwords for various UNIX systems.

Reference:

- IEEE Std 1003.1-2008 - crypt() function FIPS.180-3.2008: Secure Hash Standard

size

Pattern:

```
'S(\d+G)?(\d+M)?(\d+K)?(\d+B)?'
```

A value that represents a number of bytes. An example could be S1G8M7K956B; meaning 1GB + 8MB + 7KB + 956B = 1082138556 bytes.

The value must start with an S. Any byte magnifier can be left out, for example, S1K1B equals 1025 bytes. The order is significant though, that is S1B56G is not a valid byte size.

In ConfD, a 'size' value is represented as an uint64.

uuid

Pattern:
```
'[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-'
 '[0-9a-fA-F]{4}-[0-9a-fA-F]{12}'
```

A Universally Unique IDentifier in the string representation defined in RFC 4122. The canonical representation uses lowercase characters. The following is an example of a UUID in string representation: f81d4fae-7dec-11d0-a765-00a0c91e6bf6.

Reference:

- RFC 4122: A Universally Unique IDentifier (UUID) URN Namespace

yang-identifier

Pattern:
```
'[a-zA-Z_][a-zA-Z0-9\-_.]*'
```

Pattern:
```
'.|..|[^xX].*|.[^mM].*|..[^lL].*'
```

A YANG identifier string as defined by the 'identifier' rule in Section 12 of RFC 6020. An identifier must start with an alphabetic character or an underscore followed by an arbitrary sequence of alphabetic or numeric characters, underscores, hyphens, or dots. A YANG identifier MUST NOT start with any possible combination of the lowercase or uppercase character sequence 'xml'.

Reference:

- RFC 6020: YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)