



## **Command Line Interface Reference, Modes E - F, StarOS Release 21.27**

**First Published:** 2022-04-14

**Last Modified:** 2022-04-19

### **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 NON-INFRINGEMENT 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](http://www.cisco.com/go/offices).

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

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

© 2022 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### PREFACE

<a href="#">About this Guide</a>	xxxvii
<a href="#">CLI Command Sections</a>	xxxviii
<a href="#">Conventions Used</a>	xxxviii
<a href="#">Supported Documents and Resources</a>	xl
<a href="#">Related Documentation</a>	xl
<a href="#">Contacting Customer Support</a>	xli

---

### CHAPTER 1

<a href="#">EAP Authentication Configuration Mode Commands</a>	1
<a href="#">eap-aka</a>	1
<a href="#">eap-gtc</a>	2
<a href="#">eap-md5</a>	3
<a href="#">end</a>	4
<a href="#">exit</a>	4

---

### CHAPTER 2

<a href="#">EAP Configuration Mode Commands</a>	5
<a href="#">end</a>	5
<a href="#">exit</a>	5
<a href="#">max-retry</a>	6
<a href="#">mode</a>	6

---

### CHAPTER 3

<a href="#">EAP Mode Configuration Mode Commands</a>	9
<a href="#">end</a>	9
<a href="#">exit</a>	9
<a href="#">method</a>	10

---

### CHAPTER 4

<a href="#">EDR Format Configuration Mode Commands</a>	11
--	----

- attribute 11
- delimiter 24
- end 25
- event-label 26
- exit 26
- rule-variable 27

---

**CHAPTER 5 EDR Module Configuration Mode Commands 39**

- cdr 39
- end 44
- exit 44
- file 44

---

**CHAPTER 6 eGTP Service Configuration Mode Commands 51**

- associate 51
- allow-lte-m-rat 53
- collision-handling 53
- cups-enabled 54
- end 55
- exit 56
- gtpc 56
- interface-type 63
- pool 65
- ran-nas decode proto-type-spare cause-value-length 67
- validation-mode 67

---

**CHAPTER 7 EDNS Configuration Mode Commands 69**

- end 69
- exit 70
- fields 70
- format 71
- security-profile 72

---

**CHAPTER 8 EDNS Fields Configuration Mode Commands 73**



end 73  
exit 74  
tag 74

---

**CHAPTER 9 EDNS Format Configuration Mode Commands 77**

end 77  
exit 78  
fields 78

---

**CHAPTER 10 EIR Profile Configuration Mode Commands 81**

check-imei-every-n-events 82  
end 82  
eir-address 83  
exit 84  
include-imsi 84  
map-include-imsi 84

---

**CHAPTER 11 eNB Group Configuration Mode Commands 87**

end 87  
exit 87  
global-enb-id 88  
relative-mme-capacity 88

---

**CHAPTER 12 eNBID List Configuration Mode Commands 91**

end 91  
exit 91  
enbid 92  
enb-id-range 92

---

**CHAPTER 13 EPDG Service Configuration Mode Commands 95**

aaa 96  
allow 96  
associate 97

bind	98
data-buffering	99
dns-pgw	99
end	100
exit	101
fqdn	101
interworking-5g	102
ip	102
max-sessions	103
mobile-access-gateway	104
newcall	105
pdn-type	106
pgw-selection	106
plmn	108
reporting-action	109
setup-timeout	109
subscriber	110
threshold	111
timeout idle	112
username	113
vendor-specific-attr	114

---

**CHAPTER 14 Ethernet Interface Configuration Mode Commands 117**

bfd	118
crypto-map	119
description	120
end	121
exit	121
ip access-group	121
ip address	122
ip igmp profile	123
ip mtu	123
ip ospf authentication-key	125
ip ospf authentication-type	125

ip ospf bfd	126
ip ospf cost	127
ip ospf dead-interval	127
ip ospf hello-interval	128
ip ospf message-digest-key	129
ip ospf network	129
ip ospf priority	130
ip ospf retransmit-interval	131
ip ospf transmit-delay	132
ipv6 access-group	132
ipv6 address	133
ipv6 ospf	134
ipv6 router advertisement	136
logical-port-statistics	136
mpls ip	137
policy-forward	138
pool-share-protocol	139
port-switch-on-L3-fail	140
vlan-map	141

---

**CHAPTER 15****Ethernet Port Configuration Mode Commands 143**

bind interface	144
breakout-cable	144
boxertap	146
description	146
do show	147
end	147
exit	148
fault-unidirect-mode	148
flow-control	149
ingress-mode	150
link-aggregation	150
media	154
medium	155

preferred slot	156
shutdown	157
snmp trap link-status	158
srp virtual-mac-address	158
threshold high-activity	159
threshold monitoring	160
threshold rx-utilization	161
threshold tx-utilization	163
vlan	164

---

**CHAPTER 16****Exec Mode Commands (A-C) 167**

aaa test	171
abort	173
active-charging service	173
alarm	174
aps	175
autoconfirm	176
bulkstats force	177
call-home send	178
call-home test	178
card busy-out	179
card halt	181
card migrate	182
card reboot	183
card restart	184
card switch	186
card upgrade	187
cdr-push	188
chassis	189
clear aaa	190
clear active-charging analyzer statistics	190
clear active-charging charging-action statistics	202
clear active-charging content-filtering server-group statistics	202
clear active-charging credit-control statistics	203

clear active-charging dns-learnt-ip-addresses	204
clear active-charging edr-format statistics	205
clear active-charging edr-udr-file statistics	206
clear active-charging firewall statistics	206
clear active-charging firewall track-list	208
clear active-charging fw-and-nat policy statistics	208
clear active-charging group-of-ruledefs statistics	209
clear active-charging nat statistics	210
clear active-charging regex statistics	211
clear active-charging rulebase statistics	211
clear active-charging ruledef statistics	212
clear active-charging subsystem	213
clear active-charging tcp-proxy statistics	214
clear active-charging tethering-detection statistics	215
clear active-charging tpo policy statistics	215
clear active-charging tpo profile statistics	215
clear active-charging blockedlisting statistics	215
clear active-charging video detailed-statistics	216
clear administrator	217
clear alarm	218
clear alcap	219
clear asngw-service	219
clear asnpc-service	220
clear apn statistics	221
clear bcmcs statistics	222
clear blockedlisted-gtpu-bind- address	222
clear bssap+ statistics	223
clear bssgp statistics	224
clear bulkstats	225
clear ca-certificate-list statistics	226
clear cae-group statistics server	226
clear call-home statistics	227
clear cdr statistics	227
clear cli history	228

clear cmp cert-name	228
clear cmp statistics	229
clear confdmgr confd cdb	230
clear confdmgr statistics	231
clear config	231
clear congestion-control statistics	232
clear content-filtering category statistics	234
clear crash	234
clear credit-control statistics	235
clear crypto	236
clear cs-network statistics	237
clear dhcp statistics	238
clear dhcpv6 statistics	239
clear diameter aaa-statistics	240
clear diameter route	241
clear diameter statistics	242
clear diameter-service	243
clear diameter tps-statistics	245
clear dns-client	246
clear dns-proxy statistics	247
clear dynamic-policy statistics	248
clear egtpc	249
clear event-notif statistics	251
clear event-record	251
clear firewall	252
clear fng-service statistics	252
clear gmb statistics	253
clear gmm-sm statistics	253
clear gprsns statistics	256
clear gprssf statistics	257
clear gtpc statistics	258
clear gtp statistics	259
clear gtp storage-server local file statistics	260
clear gtp storage-server statistics	261

clear gtpu statistics	261
clear hd-storage-policy	262
clear hcnbgw-access-service statistics	263
clear hcnbgw-network-service statistics	264
clear hexdump-module statistics	265
clear hnbgw sessions	266
clear hnbgw statistics	268
clear hsgw-service	270
clear hss-peer-service	271
clear ims-authorization	271
clear ims-sh-service statistics	272
clear ip access-group statistics	273
clear ip arp	273
clear ip bgp peer	274
clear ip localhosts	275
clear ip ospf process	276
clear ipne statistics	276
clear ipsg statistics	277
clear ipv6 neighbors	277
clear ipv6 ospf process	278
clear l2tp	278
clear lawful-intercept	280
clear llc statistics	280
clear lma-service statistics	281
clear local-policy	281
clear local-user	282
clear location-service	283
clear mag-service statistics	284
clear map statistics	284
clear maximum-temperatures	285
clear mipfa statistics	286
clear mipha statistics	286
clear mipmn statistics	287
clear mipv6ha statistics	288

clear mme-service db record	288
clear mme-service db statistics	289
clear mme-service statistics	290
clear multicast-sessions	292
clear nat-ip	294
clear pcc-policy service statistics	295
clear pcc-policy session	295
clear pcc-sp-endpoint statistics	296
clear pdg-service statistics	297
clear pgw-service	298
clear port	299
clear ppp statistics	300
clear prepaid 3gpp2 statistics	301
clear prepaid wimax	302
clear ps-network statistics	303
clear qos npu stats	304
clear radius accounting archive	304
clear radius counters	305
clear rlf-context-statistics	306
clear rohc statistics	307
clear rp service-option	308
clear rp statistics	309
clear rsvp statistics	309
clear saegw-service	310
clear samog-service statistics	311
clear sbc statistics	311
clear sccp statistics	312
clear security	313
clear session disconnect-reasons	314
clear session-event-record statistics	314
clear session setuptime	315
clear session subsystem	316
clear sgsn-fast-path statistics	316
clear sgsn-map-app	317



clear sgsn rlf-context-statistics	318
clear sgs-service	319
clear sgtpc statistics	320
clear sgtpu statistics	321
clear sgw-service statistics	322
clear sls-service statistics	323
clear sms statistics	324
clear sndcp statistics	324
clear snmp trap	325
clear srp	326
clear ss7-routing-domain	327
clear subscribers	328
clear super-charger	346
clear supplementary-service statistics	347
clear tacacs session	348
clear task resources	349
clear tcap statistics	353
clear wsg-service statistics	354
cli	355
clock set	356
cmp enroll current-cert	357
cmp fetch cert-name	358
cmp initialize	359
cmp poll	360
cmp update	361
commandguard	362
configure	363
context	365
copy	366
crash copy	369
crypto blockedlistfile update	371
crypto rsa-keygen modulus	371
crypto permitlistfile update	372
crypto-group	373

---

<b>CHAPTER 17</b>	<b>Exec Mode Commands (D-S)</b>	<b>375</b>
	debug bfd	378
	debug ip	379
	debug ip bgp	380
	debug ip ospf all	381
	debug ip ospf event	382
	debug ip ospf ism	383
	debug ip ospf lsa	384
	debug ip ospf nsm	385
	debug ip ospf packet	386
	debug ip ospf route	387
	debug ip ospf router	388
	debug ipv6 ospf all	389
	debug ipv6 ospf event	390
	debug ipv6 ospf ifsm	391
	debug ipv6 ospf lsa	392
	debug ipv6 ospf nsm	393
	debug ipv6 ospf packet	394
	debug ipv6 ospf route	395
	default terminal	396
	delete	397
	delete support record	398
	dhcp force	399
	dhcp test	400
	diameter disable endpoint	401
	diameter enable endpoint	401
	diameter-proxy conn-audit	402
	diameter reset connection	403
	diameter reset route failure	404
	directory	405
	disable radius	406
	dns-client	407
	egtpc test echo	408

enable radius 410

exit 411

filesystem 411

filesystem synchronize 412

gtpc test echo 414

gtpm interim now 415

gtpm interim now active-charging egcdr 417

gtpm storage-server commit 419

gtpm storage-server streaming start 419

gtpm test 420

gtpu test echo 422

gtpv0 test echo 424

hd raid 425

host 430

install plugin 430

interface 431

lawful-intercept 431

lawful-intercept packet-cable 432

lawful-intercept ssdf 432

license 432

link-aggregation port switch to 433

logging active 434

logging filter 435

logging trace 446

logging session fp-flow-state-change 448

logs checkpoint 449

lsp-ping 450

lsp-traceroute 451

mkdir 452

mme-mmedemux 453

mme disconnect 454

mme imsigr 455

mme offload 456

mme paging cache clear 458

mme relocate-ue imsi 458  
mme reset 459  
monitor interface 460  
monitor protocol 461  
monitor subscriber 465  
newcall policy 469  
password change 475  
patch plugin 476  
ping 478  
ping6 480  
port disable, port enable 481  
port switch to 482  
ppp echo-test 483  
push ssh-key 484  
radius interim accounting now 485  
radius test 486  
reload 488  
rename 489  
reset active-charging 490  
reset alcap-service 491  
reset diameter 492  
reset ims-authorization 492  
reveal disabled commands 493  
rlogin 494  
rmdir 495  
rollback module 496  
rotate-hd-file 496  
save configuration 497  
save logs 500  
session trace 513  
session trace random 517  
session trace signaling 519  
setup 520  
sgs offload 521

sgs vlr-failure	523
sgs vlr-recover	524
sgsn clear-congestion	526
sgsn clear-detached-subscriptions	526
sgsn insimgr	527
sgsn offload	528
sgsn op	531
sgsn retry-unavailable-ggsn	535
sgsn trigger-congestion	535
sgtpc test echo sgsn-address	536
shutdown	537
sleep	538
srp disable	539
srp enable	539
srp initiate-audit	540
srp initiate-switchover	541
srp reset-auth-probe-fail	542
srp reset-diameter-fail	542
srp reset-sx-fail	543
srp terminate-post-process	543
srp validate-configuration	544
srp validate-switchover	544
ssh	545
start crypto security-association	545
statistics-collection	546
system packet-dump	547
system ping	548
system ssh	549

**CHAPTER 18****Exec Mode Commands (T-Z) 551**

tcpdump kernel	552
telnet	552
telnet6	553
terminal	554

- test alarm 555
- test ggsn vapn 556
- test ipcf bindmux 556
- test ipsec tunnel ip-pool 557
- test mobile tunnel 558
- timestamps 559
- traceroute 560
- traceroute6 562
- update active-charging 563
- update firewall policy 566
- update ip access-list 566
- update ipv6 access-list 567
- update ip-pool apn 568
- update local-user database 569
- update module 570
- update qos policy map 570
- update qos tft 571
- update security 572
- upgrade content-filtering 573
- upgrade database 574
- upgrade tethering-detection 574
- upgrade url-blockedlisting database 575

---

**CHAPTER 19**

**Exec Mode show Commands (A-C) 577**

- show active-charging analyzer statistics 580
- show active-charging bandwidth-policy 592
- show active-charging charging-action 592
- show active-charging content-filtering category policy-id 593
- show active-charging content-filtering category statistics 594
- show active-charging content-filtering server-group 596
- show active-charging credit-control 597
- show active-charging dns-learnt-ip-addresses 599
- show active-charging edr-format 600
- show active-charging edr-udr-file 601

show active-charging file-space-usage	602
show active-charging firewall dos-protection	603
show active-charging firewall statistics	604
show active-charging firewall track-list	605
show active-charging flow-control-counters	606
show active-charging flow-kpi	607
show active-charging flow-mappings	608
show active-charging flows	609
show active-charging fw-and-nat policy	625
show active-charging group-of-objects	626
show active-charging group-of-prefixed-urls	627
show active-charging group-of-ruledefs	628
show active-charging nat statistics	629
show active-charging p2p-dynamic-rules	631
show active-charging packet-filter	631
show active-charging pcp-service	632
show active-charging qos-group-of-ruledefs	634
show active-charging regex	635
show active-charging rulebase	636
show active-charging ruledef	637
show active-charging service	639
show active-charging service-scheme	640
show active-charging sessions	641
show active-charging sessions credit-control server-unreachable	655
show active-charging subscribers	669
show active-charging subsystem	670
show active-charging tcp-proxy statistics	671
show active-charging tethering-detection	673
show active-charging timedef	674
show active-charging traffic-optimization counters sessmgr	675
show active-charging traffic-optimization info	676
show active-charging trigger-action	676
show active-charging trigger-condition	677
show active-charging udr-format	678

show active-charging url-blockedlisting statistics	679
show active-charging video detailed-statistics	681
show active-charging xheader-format	681
show administrators	682
show alarm	683
show alcap counters	685
show alcap-service	686
show alcap statistics	687
show apn	688
show apn counters ip-allocation	689
show apn statistics	690
show apn-profile	693
show apn-remap-table	694
show aps	695
show asngw-service	696
show asngw-service session	698
show asngw-service session counters	699
show asngw-service statistics	701
show asnpc-service	703
show asnpc-service session	704
show asnpc-service session counters	705
show asnpc-service session counters verbose	706
show asnpc-service statistics	708
show asnpc-service statistics verbose	709
show banner	710
show bcmcs counters	711
show bcmcs statistics	712
show bfd	712
show boot	713
show bssap+ statistics	714
show bssgp statistics	715
show bssgp status	716
show build	717
show bulkstats	718



show ca-certificate	725
show ca-crl	725
show cae-group server	726
show call-control-profile	727
show call-home	728
show camel-service	729
show card	730
show cbs counters	731
show cbs sessions	732
show cbs statistics	733
show cbs-service	735
show cdr	736
show certificate	737
show cgw-service	737
show cli	738
show clock	739
show cloud configuration	740
show cloud hardware	741
show cloud monitor	742
show cmp history	743
show cmp outstanding-req	744
show cmp statistics	745
show confdmgr	745
show configuration	746
show configuration errors	750
show congestion-control	754
show connectedapps	756
show content-filtering category database	757
show content-filtering category policy-id	758
show content-filtering category statistics	759
show content-filtering category url	760
show content-filtering server-group	762
show context	763
show cpu	763

show crash	765
show credit-control sessions	766
show credit-control statistics	767
show crypto blockedlist file	767
show crypto group	768
show crypto ikev1	769
show crypto ikev2-ikesa security-associations	771
show crypto ikev2-ikesa transform-set	773
show crypto ipsec security-associations	774
show crypto ipsec transform-set	777
show crypto isakmp keys	778
show crypto isakmp policy	779
show crypto isakmp security-associations	779
show crypto managers	780
show crypto map	782
show crypto statistics	784
show crypto template	785
show crypto vendor-policy	786
show crypto permitlist file	788
show cs-network	788
show cs-network counters	790
show cs-network statistics	791
show css delivery-sequence	792
show css server	792
show css service	792

---

**CHAPTER 20**
**Exec Mode show Commands (D-G) 793**

show dhcp	794
show dhcp-service	797
show dhcpv6	798
show dhcpv6-client-profile	800
show dhcpv6-server-profile	801
show dhcpv6-service	802
show diameter-hdd-module	803

show diameter aaa-statistics	804
show diameter accounting servers aaa-group	805
show diameter authentication servers aaa-group	805
show diameter dynamic-dictionary	806
show diameter endpoint	807
show diameter endpoints	807
show diameter message-queue	808
show diameter peers	810
show diameter procllet-map-memcache	811
show diameter procllet-map-table	812
show diameter route status	813
show diameter route table	814
show diameter statistics	815
show diameter-service	816
show diameter tps-statistics	817
show dns-client	819
show dynamic-policy statistics	820
show egtpc peers	821
show egtpc sessions	823
show egtpc statistics	825
show egtp-service	828
show emps-profile	829
show epdg-service	829
show event-record	832
show external-inline-servers	832
show fa-service	832
show fa-spi-list	833
show fans	834
show file	835
show fng-service	836
show fng-service session	838
show fng-service statistics	839
show freeze-ptmsi imsi	840
show ggsn sessmgr	841

show ggsn-service	841
show ggsn-service sgsn-table	842
show global-title-translation	843
show gmb statistics	844
show gmm-sm statistics	844
show gprsns statistics	847
show gprsns status	848
show gprs-service	849
show gprssf	850
show gs-service	852
show gtpc	853
show gtpc statistics	854
show gtp	856
show gtp accounting	857
show gtp counters	858
show gtp group	859
show gtp statistics	860
show gtp storage-server	862
show gtpu	863
show gtpu-service	865

---

**CHAPTER 21**
**Exec Mode show Commands (H-L) 867**

show ha-service	869
show ha-spi-list	870
show hardware	871
show hd raid	872
show hd-storage-policy	872
show hcnbgw	873
show hcnbgw-access-service	875
show hcnbgw-network-service	877
show hexdump-module	879
show hcnbgw access-control-db	880
show hcnbgw counters	881
show hcnbgw-global	882

show hnbgw sessions	882
show hnbgw statistics hnbgw-service	885
show hnbgw statistics hnbid	887
show hnbgw-service	888
show hsgw-service	889
show hss-peer-service	891
show imei-profile	892
show ims-authorization policy-control	893
show ims-authorization policy-control misc-info	894
show ims-authorization policy-gate	895
show ims-authorization servers	897
show ims-authorization service	898
show ims-authorization sessions	900
show instance-logging	902
show inventory	903
show ip access-group statistics	903
show ip access-list	904
show ip arp	905
show ip as-path-access-list	906
show ip bgp	906
show ip framed-prefixes	909
show ip igmp group	910
show ip interface	910
show ip ipsp	912
show ip localhosts	913
show ip ospf	913
show ip policy-forward	915
show ip pool	916
show ip prefix-list	918
show ip route	919
show ip route-access-list	920
show ip static-route	921
show ip vrf	922
show ip vrf-list	923

show ipms status	923
show ipne peers	924
show ipsg service	925
show ipsg sessions	926
show ipsg statistics	927
show ipv6 access-group statistics	929
show ipv6 access-list	929
show ipv6 interface	930
show ipv6 neighbors	931
show ipv6 ospf	932
show ipv6 pool	934
show ipv6 prefix-list	935
show ipv6 route	936
show ipv6 route-access-list	937
show iups-service	938
show l2tp sessions	939
show l2tp statistics	941
show l2tp tunnels	942
show lac-service	944
show lawful-intercept	945
show lawful-intercept ssdf statistics	945
show ldap connection all	945
show leds	946
show license	947
show link-aggregation	949
show linkmgr	951
show llc statistics	951
show llc status	952
show lma-service	954
show lns-service	956
show local-policy	957
show local-user	957
show location-service	959
show logging	960

show logical-port utilization table 961  
 show logs 962  
 show lte-policy 974

---

**CHAPTER 22**
**Exec Mode show Commands (M-P) 979**

show mag-service 981  
 show map-service 983  
 show map statistics 983  
 show maximum-temperatures 984  
 show mbms bearer-service 985  
 show mipfa 987  
 show mipha 989  
 show mipv6ha 992  
 show mme-embms-service 994  
 show mme-hss session 996  
 show mme-service 998  
 show mme-service db record 999  
 show mme-service db statistics 1000  
 show mme-service enodeb-association 1001  
 show mme-service id 1002  
 show mme-service session 1003  
 show mme-service statistics 1006  
 show module 1008  
 show mpls cross-connect 1009  
 show mpls ftm 1010  
 show mpls ilm 1011  
 show mpls ldp 1012  
 show mpls nexthop-label-forwarding-entry 1013  
 show mrme-service 1014  
 show mrme-service active-session 1015  
 show mrme-service imsi-sticky 1015  
 show mrme-service mac-sticky 1016  
 show mseg-config 1017  
 show mseg-service 1017

show multicast-sessions	1017
show network-requested-pdp-context	1019
show network-service-entity	1020
show npu arp	1021
show npu error-counters	1021
show npu tm	1022
show npu utilization	1023
show ntp	1024
show nw-reachability server	1025
show operator-policy	1026
show orbem	1027
show patch progress	1028
show pcc-af service	1029
show pcc-af session	1030
show pcc-policy service	1032
show pcc-policy session	1033
show pcc-service	1034
show pcc-service session	1035
show pcc-service statistics	1037
show pcc-sp-endpoint	1038
show pcc-sp-endpoint connection	1039
show pdg-service	1040
show pdg-service statistics	1041
show pdif-service	1042
show pdn-connection-count	1043
show pdsn-service	1043
show pdsnclosedrp-service	1045
show peer-profile	1045
show pgw-service	1046
show plugin	1047
show port	1048
show power	1050
show ppp	1051
show prepaid 3gpp2	1053



show prepaid wimax	1054
show process status	1055
show profile-id-qci-mapping	1056
show ps-network	1057
show ps-network counters	1058
show ps-network statistics	1059

---

**CHAPTER 23**

<b>Exec Mode show Commands (Q-S)</b>	<b>1061</b>
show qci-qos-mapping	1063
show qos ip-dscp-iphb-mapping	1064
show qos l2-mapping-table	1064
show qos npu inter-subscriber traffic	1065
show qos npu stats	1065
show radius	1066
show radius charging servers	1068
show radius client	1069
show radius counters	1069
show rct stats	1071
show resources	1072
show rlf-context-statistics	1073
show rlf-memcache-statistics	1075
show rlf-template	1075
show rohc counters	1076
show rohc statistics	1077
show route-map	1079
show rp	1079
show rp service-option	1081
show rp statistics	1082
show rsvp counters	1083
show rsvp statistics	1084
show requirement pac daughtercard	1084
show s102-service	1085
show s4-sgsn statistics	1086
show saegw-service	1087

show samog-service	1088
show sbc-service	1089
show sbc statistics	1090
show sccp-network	1091
show sccp statistics	1092
show scef-service statistics	1093
show sctp-param-template	1094
show security	1095
show service all	1096
show session counters historical	1096
show session counters pcf-summary	1099
show session disconnect-reasons	1100
show session duration	1102
show session progress	1104
show session recovery status	1108
show session setup-time	1109
show session subsystem	1110
show session trace	1113
show session-event-record	1114
show sf	1115
show sgs-service	1115
show s4-sgsn statistics	1117
show sgsn fsm-statistics	1117
show sgsn sessmgr	1118
show sgsn-fast-path	1119
show sgsn-map-app	1120
show sgsn-mode	1120
show sgsn-operator-policy	1121
show sgsn-pool	1121
show sgsn-service	1122
show sctp-service	1123
show sgtpc statistics	1124
show sgtpu statistics	1125
show sgw-service	1127

show sls-service	1128
show sms statistics	1129
show sndcp statistics	1130
show snmp	1131
show software authenticity	1133
show srp	1134
show ss7-routing-domain	1136
show ssh	1139
show ssl cipher-suite	1140
show ssl connection	1140
show ssl map	1141
show ssl statistics	1142
show subscribers	1143
show subscribers samog-only	1196
show subscribers wsg-service	1197
show super-charger	1197
show supplementary-service statistics	1198
show support collection	1199
show support details	1200
show support record	1202
show system ssh key status	1203
show system uptime	1204
show sx peers	1204

---

**CHAPTER 24**
**Exec Mode show Commands (T-Z) 1207**

show tacacs	1207
show task	1209
show tcap statistics	1215
show temperature	1216
show terminal	1217
show threshold	1217
show transaction-rate	1218
show url-blacklisting database	1219
show version	1220

show wsg-application 1222  
show wsg-lookup 1223  
show wsg-service 1223  
show x2gw-service 1224

---

**CHAPTER 25****FA Service Configuration Mode Commands 1227**

advertise 1228  
authentication aaa 1230  
authentication mn-aaa 1231  
authentication mn-ha 1232  
bind 1233  
challenge-window 1234  
default subscriber 1235  
dynamic-ha-assignment 1236  
dynamic-mip-key-update 1237  
encapsulation allow gre 1238  
end 1238  
exit 1238  
fa-ha-spi 1239  
gre 1241  
ha-monitor 1243  
idle-timeout-mode 1245  
ignore-mip-key-data 1245  
ignore-stale-challenge 1246  
ip local-port 1247  
isakmp 1248  
limit-reg-lifetime 1249  
max-challenge-len 1250  
mn-aaa-removal-indication 1251  
multiple-reg 1252  
optimize tunnel-reassembly 1253  
private-address allow-no-reverse-tunnel 1253  
proxy-mip 1254  
reg-timeout 1256

reverse-tunnel 1257  
revocation 1258  
threshold reg-reply-error 1259

---

**CHAPTER 26 FNG Service Configuration Mode Commands 1263**

aaa aggregation 1263  
aaa authentication 1264  
bind 1265  
default 1266  
duplicate-session-detection 1267  
end 1268  
exit 1268  
ip source-violation 1269  
setup-timeout 1270

---

**CHAPTER 27 FTP Configuration Mode Commands 1271**

end 1271  
exit 1272  
max servers 1272  
timeout 1273

---

**CHAPTER 28 Firewall-and-NAT Action Configuration Mode Commands 1275**

end 1275  
exit 1276  
flow check-point 1276

---

**CHAPTER 29 Firewall-and-NAT Policy Configuration Mode Commands 1279**

access-rule 1280  
end 1284  
exit 1284  
firewall dos-protection 1284  
firewall flooding 1288  
firewall icmp-checksum-error 1290  
firewall icmp-destination-unreachable-message-threshold 1291

firewall icmp-echo-id-zero	1292
firewall icmp-fsm	1293
firewall ip-reassembly-failure	1293
firewall malformed-packets	1294
firewall max-ip-packet-size	1295
firewall mime-flood	1296
firewall policy	1297
firewall tcp-checksum-error	1299
firewall tcp-first-packet-non-syn	1300
firewall tcp-fsm	1300
firewall tcp-idle-timeout-action	1301
firewall tcp-options-error	1302
firewall tcp-partial-connection-timeout	1303
firewall tcp-reset-message-threshold	1304
firewall tcp-syn-flood-intercept	1305
firewall tcp-syn-with-ecn-cwr	1306
firewall udp-checksum-error	1307
firewall validate-ip-options	1308
nat binding-record	1309
nat check-point-info	1310
nat icnr-flow-recovery	1311
nat max-chunk-per-realm	1312
nat pkts-drop	1313
nat policy	1314
nat private-ip-flow-timeout	1315
nat suppress-aaa-update	1316
<b>CHAPTER 30</b>	<b>Firewall-and-NAT Access Ruledef Configuration Mode Commands</b> 1319
bearer 3gpp apn	1320
bearer 3gpp imsi	1321
bearer username	1322
create-log-record	1323
end	1324
exit	1324

icmp any-match	1325
icmp code	1326
icmp type	1327
icmpv6 any-match	1328
icmpv6 code	1329
icmpv6 type	1330
ip any-match	1331
ip downlink	1332
ip dst-address	1333
ip protocol	1334
ip server-ip-address	1335
ip server-ipv6-network-prefix	1336
ip src-address	1337
ip uplink	1339
ip version	1340
tcp any-match	1340
tcp client-port	1341
tcp dst-port	1343
tcp either-port	1344
tcp server-port	1346
tcp src-port	1347
udp any-match	1348
udp client-port	1349
udp dst-port	1351
udp either-port	1352
udp server-port	1353
udp src-port	1355







## About this Guide

---



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

---



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

---



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

---



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

---

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

This reference describes how to use the command line interface (CLI) to interact with the products supported by the StarOS™. The CLI commands are organized by command modes in the code and in this reference. The

command modes are presented alphabetically. The description of each command states the command's function, describes its syntax, presents limitations when applicable, and offers an example of its usage.

- [CLI Command Sections](#), on page xxxviii
- [Conventions Used](#), on page xxxviii
- [Supported Documents and Resources](#), on page xl
- [Contacting Customer Support](#), on page xli

## CLI Command Sections

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

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

## Conventions Used

The following tables describe the conventions used throughout this documentation.

Notice Type	Description
Information Note	Provides information about important features or instructions.
Caution	Alerts you of potential damage to a program, device, or system.
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 <b>commands</b>	This typeface represents commands that you enter, for example:  <b>show ip access-list</b>  This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a <b>command</b> <i>variable</i>	This typeface represents a variable that is part of a command, for example:  <b>show card slot_number</b>  <i>slot_number</i> 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 <b>File</b> menu, then click <b>New</b>

Command Syntax Conventions	Description
{ <b>keyword</b> or <i>variable</i> }	Required keyword options and variables are those components that are required to be entered as part of the command syntax.  Required keyword options and variables are surrounded by grouped braces { }. For example:  <b>sctp-max-data-chunks { limit max_chunks   mtu-limit }</b>  If a keyword or variable is not enclosed in braces or brackets, it is mandatory. For example:  <b>snmp trap link-status</b>

Command Syntax Conventions	Description
[ <b>keyword</b> or <i>variable</i> ]	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by brackets.
	<p>Some commands support multiple options. These are documented within braces or brackets by separating each option with a vertical bar.</p> <p>These options can be used in conjunction with required or optional keywords or variables. For example:</p> <pre>action activate-flow-detection {   intitiation   termination }</pre> <p>or</p> <pre>ip address [ count <i>number_of_packets</i>     size <i>number_of_bytes</i> ]</pre>

## Supported Documents and Resources

### Related Documentation

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

The following related product documents are also available:

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

# Contacting Customer Support

Use the information in this section to contact customer support.

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





# CHAPTER 1

## EAP Authentication Configuration Mode Commands

### Command Modes

The EAP Authentication Configuration Mode is used to configure the Extensible Authentication Protocol (EAP) authentication methods for the crypto template.

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > EAP Authentication Configuration

**configure** > **context** *context\_name* > **crypto template** *template\_name* **ikev2-dynamic** > **authentication eap-profile** *profile\_name*

Entering the above command sequence results in the following prompt:

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



### Important

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

- [eap-aka](#), on page 1
- [eap-gtc](#), on page 2
- [eap-md5](#), on page 3
- [end](#), on page 4
- [exit](#), on page 4

## eap-aka

Configures shared key values for the Extensible Authentication Protocol-Authentication and Key Agreement (EAP-AKA) authentication method used by subscribers using this crypto template.

### Product

PDIF

### Privilege

Security Administrator, Administrator

### Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > EAP Authentication Configuration

```
configure > context context_name > crypto template template_name ikev2-dynamic > authentication
eap-profile profile_name
```

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description**    **eap-aka { encrypted key *hex* | key *hex* }**

**encrypted key *hex***

Specifies that the shared key is to be encrypted as a 16-character alphanumeric string or a hexadecimal number beginning with "0x".

**key *hex***

Specifies that the shared key is to be transmitted in clear text as a 16-character alphanumeric string or a hexadecimal number beginning with "0x".

---

**Usage Guidelines**    Use this command to set shared key parameters for subscribers using the EAP-AKA authentication method.

**Example**

The following command configures a clear-text shared key value for the EAP-AKA method:

```
eap-aka key aa11223344556677
```

## eap-gtc

Configures shared key values for the EAP-GTC authentication method used by subscribers using this crypto template.

---

**Product**    ASN-GW

PDIF

---

**Privilege**    Security Administrator, Administrator

---

**Command Modes**    Exec > Global Configuration > Context Configuration > Crypto Template Configuration > EAP Authentication Configuration

```
configure > context context_name > crypto template template_name ikev2-dynamic > authentication
eap-profile profile_name
```

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description**    **eap-gtc { encrypted key *value* | key *value* }**

**encrypted key *value***

Specifies that the shared key is to be encrypted as a 16-character alphanumeric string.



**key value**

Specifies that the shared key is to be transmitted in clear text as a 16-character alphanumeric string.

**Usage Guidelines**

Use this command to set shared key parameters for subscribers using the EAP-GTC authentication method.

**Example**

The following command configures a clear-text shared key value for the EAP-GTC method:

```
eap-gtc key aa11223344556677
```

## eap-md5

Configures shared key values for the EAP-MD5 authentication method used by subscribers using this crypto template.

**Product**

ASN-GW  
PDIF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > EAP Authentication Configuration

```
configure > context context_name > crypto template template_name ikev2-dynamic > authentication eap-profile profile_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
eap-md5 { encrypted key value | key value }
```

**encrypted key value**

Specifies that the shared key is to be encrypted as a 16-character alphanumeric string.

**key value**

Specifies that the shared key is to be transmitted in clear text as a 16-character alphanumeric string.

**Usage Guidelines**

Use this command to set shared key parameters for subscribers using the EAP-MD5 authentication method.

**Example**

The following command configures a clear-text shared key value for the EAP-MD5 method:

```
eap-md5 key aa11223344556677
```

**end**

## end

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

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Syntax Description</b>	<b>end</b>
<b>Usage Guidelines</b>	Use this command to return to the Exec mode.

## exit

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

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Syntax Description</b>	<b>exit</b>
<b>Usage Guidelines</b>	Use this command to return to the parent configuration mode.



## CHAPTER 2

# EAP Configuration Mode Commands

The EAP Configuration Mode is used to configure parameters comprising an Extensible Authentication Protocol (EAP) used to support authentication on the system.

### Command Modes

Exec > Global Configuration > Context Configuration > EAP Profile Configuration

**configure** > **context** *context\_name* > **eap-profile** *profile\_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-eap-profile)#
```



### Important

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

- [end, on page 5](#)
- [exit, on page 5](#)
- [max-retry, on page 6](#)
- [mode, on page 6](#)

## end

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

### Product

All

### Privilege

Security Administrator, Administrator

### Syntax Description

**end**

### Usage Guidelines

Use this command to return to the Exec mode.

## exit

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

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Syntax Description</b>	<b>exit</b>
<b>Usage Guidelines</b>	Use this command to return to the parent configuration mode.

## max-retry

Configures the maximum number of times the system will retry communicating with another EAP device.

<b>Product</b>	ASN-GW PDIF
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > Global Configuration > Context Configuration > EAP Profile Configuration <b>configure &gt; context</b> <i>context_name</i> > <b>eap-profile</b> <i>profile_name</i> Entering the above command sequence results in the following prompt: <pre>[context_name]host_name(cfg-ctx-eap-profile)#</pre>
<b>Syntax Description</b>	<b>max-retry</b> <i>num</i> <b>default max-retry</b>  <b>max-retry</b> <i>num</i> Specifies the number of times to retry EAP communication with another device as an integer from 1 to 65535. Default: 16
<b>Usage Guidelines</b>	Use this command to set a maximum retry number for communicating with other EAP devices.

### Example

The following command sets the maximum number of retries to 50:

```
max-retry 50
```

## mode

Configures the system as one of three types of EAP devices: authenticator pass-through, authenticator server, or peer.

<b>Product</b>	ASN-GW PDIF
----------------	----------------

<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > Global Configuration > Context Configuration > EAP Profile Configuration <b>configure &gt; context</b> <i>context_name</i> > <b>eap-profile</b> <i>profile_name</i> Entering the above command sequence results in the following prompt: <i>[context_name]host_name(cfg-ctx-eap-profile)#</i>
<b>Syntax Description</b>	<b>mode { authenticator-pass-through   authenticator-server   peer }</b> <b>default mode</b>  <b>default</b> Configures the default mode of Authenticator-pass-through.  <b>authenticator-pass-through</b> Configures the system as an authenticator pass-through allowing EAP authentication to be performed by another server. This is the default setting for this command.  <b>authenticator-server</b> Configures the system as an authenticator server. This allows the system to respond to EAP requests.  <b>peer</b> Configures the system as a peer device requiring it to make EAP requests of another server or pass-through device.
<b>Usage Guidelines</b>	Use this command to configure the system to perform as one of three types of EAP devices and configure settings in an EAP mode. EAP Mode Configuration Mode commands are defined in the EAP Mode Configuration Mode Commands chapter.  <b>Example</b> The following command configures the system to perform as an authenticator pass-through: <b>mode authenticator-pass-through</b>

mode



## CHAPTER 3

# EAP Mode Configuration Mode Commands

The EAP Mode Configuration Mode is used to configure the Extensible Authentication Protocol (EAP) authentication method supported by the system.

### Command Modes

Exec > Global Configuration > Context Configuration > EAP Profile Configuration

**configure** > **context** *context\_name* > **eap-profile** *profile\_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-eap-profile)#
```



### Important

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

- [end, on page 9](#)
- [exit, on page 9](#)
- [method, on page 10](#)

## end

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

### Product

All

### Privilege

Security Administrator, Administrator

### Syntax Description

**end**

### Usage Guidelines

Use this command to return to the Exec mode.

## exit

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

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Syntax Description</b>	<b>exit</b>
<b>Usage Guidelines</b>	Use this command to return to the parent configuration mode.

## method

Configures the EAP method used for authentication.

<b>Product</b>	ASN-GW PDIF
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > Global Configuration > Context Configuration > EAP Profile Configuration <b>configure &gt; context</b> <i>context_name</i> > <b>eap-profile</b> <i>profile_name</i> Entering the above command sequence results in the following prompt: <i>[context_name]host_name (cfg-ctx-eap-profile) #</i>

**Syntax Description** **method { eap-aka | eap-gtc | eap-md5 } [ priority *num* ]**

### **eap-aka | eap-gtc | eap-md5**

Specifies one of the following methods:

- **eap-aka**: Specifies that the EAP-AKA method is to be used for authentication.
- **eap-gtc**: Specifies that the EAP-GTC method is to be used for authentication.
- **eap-md5**: Specifies that the EAP-MD5 method is to be used for authentication.

### **priority *num***

Specifies a priority order for a specific EAP authentication method an integer from 1 though 65535.

**Usage Guidelines** Use this command to specify the EAP authentication method(s) to use and to place multiple methods in priority order.

### **Example**

The following command sets EAP-AKA as one of the EAP authentication methods and places it as priority of 3:

```
method eap-aka priority 3
```





## CHAPTER 4

# EDR Format Configuration Mode Commands

The EDR Format Configuration Mode enables configuring Event Data Record (EDR) formats.

### Command Modes

Exec > ACS Configuration > EDR Format Configuration

**active-charging service** *service\_name* > **edr-format** *format\_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acs-edr)#
```



### Important

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

- [attribute](#), on page 11
- [delimiter](#), on page 24
- [end](#), on page 25
- [event-label](#), on page 26
- [exit](#), on page 26
- [rule-variable](#), on page 27

## attribute

This command allows you to specify the fields and their order in EDRs.

### Product

All

### Privilege

Security Administrator, Administrator

### Command Modes

Exec > ACS Configuration > EDR Format Configuration

**active-charging service** *service\_name* > **edr-format** *format\_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acs-edr)#
```

**Syntax Description**

```
attribute attribute { [ format { MM/DD/YY-HH:MM:SS | MM/DD/YY-HH:MM:SS:sss
| MM/DD/YYYY-HH:MM:SS | MM/DD/YYYY-HH:MM:SS:sss | YYYY/MM/DD-HH:MM:SS |
MM/DD/YYYY-HH:MM:SS:sss | YYYYMMDDHHMMSS | YYYYMMDDHHMMSSsss | seconds
} ] [ localtime ] | [ { ip | tcp } { bytes | pkts } { downlink | uplink
} ] priority priority }
no attribute attribute [ { ip | tcp } { bytes | pkts } { downlink | uplink
} ] [ priority priority ]
```

**no**

If added previously, removes the specified attribute from the EDR format.

**attribute**

Specifies the attribute.

*attribute* must be one of the following:

Attributes	Description
<b>bandwidth-policy</b>	This attribute reports the bandwidth policy name of subscriber.  Bandwidth policy can be configured or applied to subscriber by — <ul style="list-style-type: none"> <li>• binding with APN (static)</li> <li>• binding with Rulebase (static)</li> <li>• receiving from AAA server (dynamic)</li> </ul> <b>Important</b> This attribute field is customer specific. For more information, contact your Cisco account representative.
<b>radius-called-station-id</b>	This attribute reports the Called Station ID of the mobile handling the flow.
<b>radius-calling-station-id</b>	This attribute reports the Calling Station ID of the mobile handling the flow.
<b>radius-fa-nas-identifier</b>	This attribute reports the RADIUS NAS identifier of Foreign Agent (FA).
<b>radius-fa-nas-ip-address</b>	This attribute reports the RADIUS IP address of Foreign Agent (FA).
<b>radius-nas-identifier</b>	This attribute reports the RADIUS NAS identifier.
<b>radius-nas-ip-address</b>	This attribute reports the RADIUS NAS IP address.  Note that this attribute is interchangeable with <b>sn-st16-ip-addr</b> for the user.
<b>radius-user-name</b>	This attribute reports the user name associated with the flow.

Attributes	Description
<b>sn-3gpp2-always-on</b>	This option has been deprecated. To configure this attribute see the <a href="#">rule-variable, on page 27</a> command.
<b>sn-3gpp2-bsid</b>	This option has been deprecated. To configure this attribute see the <a href="#">rule-variable, on page 27</a> command.
<b>sn-3gpp2-esn</b>	This option has been deprecated. To configure this attribute see the <a href="#">rule-variable, on page 27</a> command.
<b>sn-3gpp2-ip-qos</b>	This option has been deprecated. To configure this attribute see the <a href="#">rule-variable, on page 27</a> command.
<b>sn-3gpp2-ip-technology</b>	This option has been deprecated. To configure this attribute see the <a href="#">rule-variable, on page 27</a> command.
<b>sn-3gpp2-release-indicator</b>	This option has been deprecated. To configure this attribute see the <a href="#">rule-variable, on page 27</a> command.
<b>sn-3gpp2-service-option</b>	This option has been deprecated. To configure this attribute see the <a href="#">rule-variable, on page 27</a> command.
<b>sn-3gpp2-session-begin</b>	This option has been deprecated. To configure this attribute see the <a href="#">rule-variable, on page 27</a> command.
<b>sn-3gpp2-session-continue</b>	This option has been deprecated. To configure this attribute see the <a href="#">rule-variable, on page 27</a> command.
<b>sn-acct-session-id</b>	This attribute reports the unique session identifier for accounting.

Attributes	Description
sn-app-protocol	

Attributes	Description
	<p>This attribute reports the application protocol for the flow. A value indicating the protocol, such as one of the following:</p> <ul style="list-style-type: none"> <li>• ACS_PROTO_UNKNOWN = 0</li> <li>• ACS_PROTO_GTP = 1</li> <li>• ACS_PROTO_IP = 2</li> <li>• ACS_PROTO_TCP = 3</li> <li>• ACS_PROTO_UDP = 4</li> <li>• ACS_PROTO_HTTP = 5</li> <li>• ACS_PROTO_HTTPS = 6</li> <li>• ACS_PROTO_FTP = 7</li> <li>• ACS_PROTO_FTP_CONTROL = 8</li> <li>• ACS_PROTO_FTP_DATA = 9</li> <li>• ACS_PROTO_WTP = 10</li> <li>• ACS_PROTO_WSP = 11</li> <li>• ACS_PROTO_WIP_WSP_CONNECTION_ORIENTED = 12</li> <li>• ACS_PROTO_WSP_CONNECTION_LESS = 13</li> <li>• ACS_PROTO_DNS = 14</li> <li>• ACS_PROTO_ICMP = 15</li> <li>• ACS_PROTO_POP3 = 16</li> <li>• ACS_PROTO_SIP = 17</li> <li>• ACS_PROTO_SDP = 18</li> <li>• ACS_PROTO_SMTP = 19</li> <li>• ACS_PROTO_EMAIL = 20</li> <li>• ACS_PROTO_MMS = 21</li> <li>• ACS_PROTO_FILE_TRANSFER = 22</li> <li>• ACS_PROTO_WWW = 23</li> <li>• ACS_PROTO_RTP = 24</li> <li>• ACS_PROTO_RTSP = 25</li> <li>• ACS_PROTO_IMAP = 26</li> </ul>

Attributes	Description
	<ul style="list-style-type: none"> <li>• ACS_PROTO_FLOW = 27</li> <li>• ACS_PROTO_CCA = 28</li> <li>• ACS_PROTO_P2P = 29</li> <li>• ACS_PROTO_RTCP = 30</li> <li>• ACS_PROTO_ICMPV6 = 31</li> <li>• ACS_PROTO_TFTP = 32</li> <li>• ACS_PROTO_PPTP = 33</li> </ul>
	<ul style="list-style-type: none"> <li>• ACS_PROTO_GREv1 = 34</li> <li>• ACS_PROTO_PPTP_GRE = 35</li> <li>• ACS_PROTO_SIP_ADV = 36</li> <li>• ACS_PROTO_SIP_BASIC_ADV = 37</li> <li>• ACS_PROTO_H323 = 38</li> <li>• ACS_PROTO_ESP = 39</li> <li>• ACS_PROTO_AH = 40</li> <li>• ACS_PROTO_RTSPSTREAM = 41</li> </ul>
<b>sn-cf-category-classification-used</b>	<p>For Category-based Content Filtering, this attribute reports the last classification used by system for the flow, or blank if classification was never successfully performed.</p> <p>For URL Blacklisting, specifies category of the blacklisted URL in the Blacklist database.</p>

Attributes	Description
<b>sn-cf-category-flow-action</b>	<p>For Category-based Content Filtering, this attribute reports the last action taken for the flow, or blank if content filtering was never performed. The following are the possible values:</p> <ul style="list-style-type: none"> <li>• allow</li> <li>• content-insert</li> <li>• discard</li> <li>• redirect-url</li> <li>• terminate-flow</li> </ul> <p>For URL Blacklisting, this attribute reports the last action taken for the flow, or blank if Blacklist matching was never performed. The following are the possible values:</p> <ul style="list-style-type: none"> <li>• discard</li> <li>• terminate-flow</li> <li>• redirect-url</li> <li>• www-reply-code-terminate-flow</li> </ul>
<b>sn-cf-category-policy</b>	<p>For Category-based Content Filtering, this attribute reports the category policy identifier that was used for the flow, or blank if content filtering was never attempted for the flow.</p>
<b>sn-cf-category-rating-type</b>	<p>For Category-based Content Filtering, this attribute reports the type, either "static" or "dynamic" that was last successfully performed for the flow, or blank if content filtering was never successful for the flow.</p> <p>For URL Blacklisting, specifies "blacklisting".</p>
<b>sn-cf-category-unknown-url</b>	<p>This attribute reports the identifier for unknown URL under content filtering action. It holds either "1" for unknown URLs or "0" for the URLs having static rating in its database.</p>
<b>sn-charge-volume</b>	<p>This attribute reports the total charge volume excluding bytes/packets dropped/retransmitted by ECS.</p> <p>This behavior can be changed by configuring to allow dropped/retransmitted bytes/packets to be included in the net volume. See the <b>edr sn-charge-volume</b> command in the <i>ACS Rulebase Configuration Mode Commands</i> chapter.</p>

Attributes	Description
<b>sn-charging-action</b>	<p>This attribute reports the name of last charging action matched against flow.</p> <p><b>Important</b> This attribute configuration currently supports only static and predefined rules and ruledefs. It will NOT be supported for dynamic rules installed by PCRF.</p>
<b>sn-closure-reason</b>	<p>This attribute reports the reason for termination of the flow/EDR:</p> <ul style="list-style-type: none"> <li>• 0: Normal end of flow</li> <li>• 1: End of flow by handoff processing</li> <li>• 2: Subscriber session terminated</li> <li>• 3: Inter-chassis Session Recovery switchover</li> <li>• 12: Completion of transaction</li> <li>• 13: End of VoIP call event This is supported only in release 12.2.</li> <li>• 14: End of VoIP call event This is supported in 14.0 and later releases.</li> <li>• 16: ACS_EDR_OCS_REACHABLE</li> <li>• 17: ACS_EDR_OCS_UNREACHABLE</li> <li>• 18: ACS_EDR_INTERIM_VOLUME_EXHAUST</li> <li>• 19: ACS_EDR_INTERIM_TIME_EXHAUST</li> <li>• 20: ACS_EDR_OCS_STATUS_UNKNOWN</li> <li>• 21: ACS_EDR_TETHERING_SIGNATURE_CHANGE</li> </ul>
<b>sn-correlation-id</b>	<p>This attribute reports the RADIUS correlation identifier.</p>
<b>sn-direction</b>	<p>This attribute reports the direction of the first packet for the flow. It has following values:</p> <ul style="list-style-type: none"> <li>• <b>toMobile</b>: This value appears when direction of first packet is towards mobile node.</li> <li>• <b>fromMobile</b>: This value appears when direction of first packet is towards mobile node.</li> <li>• <b>unknown</b>: This value appears when the original originator of a flow can not be determined (for example, a flow that is interrupted due to a Inter-chassis Session Recovery switchover).</li> </ul>



Attributes	Description
<b>sn-duration</b>	This attribute reports the duration between the last and first packet for the record.
<b>sn-end-time [ format <i>format</i> ] localtime</b>	This attribute reports the timestamp for last packet of flow in UTC.
<b>sn-fa-correlation-id</b>	This attribute reports the RADIUS Correlation Identifier of the Foreign Agent (FA).
<b>sn-fa-ip-address</b>	This attribute reports IP address of the Foreign Agent (FA).
<b>sn-filler-blank</b>	This attribute inserts a blank filler field, generates an empty EDR field.
<b>sn-filler-zero</b>	This attribute inserts a "0" in the EDR field.
<b>sn-flow-end-time</b>	<p>This attribute reports the time of flow-end EDR generation—when EDRs are generated at hagr, session-end, timeout, or normal-end-signaling conditions.</p> <p><b>sn-start-time</b> and <b>sn-end-time</b> fields of flow end-condition EDRs cannot be used to determine the duration of the flow if intermediate EDRs are generated (rule-match or transaction-complete or any other intermediate EDR).</p> <p><b>sn-start-time</b> field in an EDR gives the time the first packet was received after the last EDR was generated. So, whenever an EDR is generated, this field is reset to the time the EDR gets generated. So the <b>sn-start-time</b> field in flow end-condition EDRs may not have the time of the first packet received on that flow. It will have the time at which the last EDR was generated or the first packet time if no EDR was generated for that flow.</p> <p><b>sn-end-time</b> field gives the time at which the last packet on the flow was received. Flow end-condition EDRs may not be generated immediately after receiving the last packet. For example, in case of session-end or timeout EDRs, last packet time and EDR generation time may be different.</p> <p><b>sn-flow-start-time</b> gives the time of the first packet of the flow (irrespective of whether intermediate EDRs were generated), and <b>sn-flow-end-time</b> gives the time when EDRs are generated at hagr, session-end, timeout or normal-end-signaling conditions. The values of these fields will be populated in EDRs only for hagr, session-end, timeout and normal-end-signaling EDRs.</p>

Attributes	Description
<b>sn-flow-id</b>	This attribute reports the flow-id assigned internally by the ECS module to each flow.
<b>sn-flow-start-time</b>	This attribute reports the time of the first packet of the flow (irrespective of whether intermediate EDRs were generated).  Also see <b>sn-flow-end-time</b> .
<b>sn-format-name</b>	This attribute reports the name of the EDR/UDR format used.
<b>sn-group-id</b>	This attribute reports the sequence group ID of the record.
<b>sn-ha-ip-address</b>	This attribute reports IP address of the Home Agent (HA).
<b>sn-ip-pool-name</b>	This attribute reports the IP pool name corresponding to the current flow in EDR.
<b>sn-ip-protocol-name</b>	This attribute reports the IP protocol name for the flow. For IANA registered IP Protocol (Layer 4 Protocol) name, like TCP, UDP, AH, ESP, ICMP, etc.
<b>sn-nat-binding-timer</b>	For Network Address Translation (NAT) in-line service, this attribute reports the port chunk hold timer.
<b>sn-nat-gmt-offset</b>	For NAT in-line service, this attribute reports the GMT offset of the node generating NAT bind record.
<b>sn-nat-ip</b>	For NAT in-line service, this attribute reports the NAT IP address of the port chunk.
<b>sn-nat-last-activity-time-gmt</b>	For NAT in-line service, this attribute reports the time when the last flow in a specific NAT set of flows was seen.
<b>sn-nat-no-port-packet-dropped</b>	For NAT in-line service, this attribute reports the number of packets dropped because of no NAT IP/port.
<b>sn-nat-port-block-end</b>	For NAT in-line service, this attribute reports the last port number of the port chunk.
<b>sn-nat-port-block-start</b>	For NAT in-line service, this attribute reports the starting port number of the port chunk.
<b>sn-nat-port-chunk-alloc-dealloc-flag</b>	For NAT in-line service, this attribute reports whether the port chunk is allocated or released.

Attributes	Description
<b>sn-nat-port-chunk-alloc-time-gmt</b>	For NAT in-line service, this attribute reports when the port chunk was allocated.
<b>sn-nat-port-chunk-dealloc-time-gmt</b>	For NAT in-line service, this attribute reports when the port chunk was released.
<b>sn-nat-realm-name</b>	For NAT in-line service, this attribute reports the name of the NAT realm.
<b>sn-nat-subscribers-per-ip-address</b>	For NAT in-line service, this attribute reports the subscriber(s) per NAT IP address.
<b>sn-nemo-vrf-name</b>	This attribute indicates the VRF name associated with UE behind the Network Mobility Services (NEMO) Mobile Router (MR).  <b>Important</b> This is a customer-specific attribute, and is available only with NEMO license.
<b>sn-ocs-server-reachable</b>	This attribute indicates the state of the OCS server. This attribute supports the following values: <ul style="list-style-type: none"> <li>• OCS_SERVER_NOT_APPLICABLE = 0</li> <li>• OCS_SERVER_UNREACHABLE = 0 + 1</li> <li>• OCS_SERVER_REACHABLE = 0 + 2</li> </ul>
<b>sn-parent-protocol</b>	This attribute reports the parent protocol of the flow. An integer value like in <b>sn-app-protocol</b> ; for RTCP/RTP flows, the parent protocol may be RTSP or SIP; for GRE flows, the parent protocol will be PPTP, and so on.
<b>sn-port-service-name</b>	This attribute reports the registered name for the server port. For IANA registered/Well Known Transport Port name mapping for the Server Port like SSL, HTTP, DNS, FTP, TELNET, SSH, Diablo, Rainbow six, Unreal_UT etc. This port service name mapping is done based on the Server port, which means if the flow is "FromMobile", the sn-server-port is mapped as the service name port. If the flow is "ToMobile", the sn-subscriber-port is mapped as the service name.
<b>sn-rulebase</b>	This attribute reports the name of the ECS rulebase applied.
<b>sn-ruledef-name</b>	This attribute reports the ruledef name corresponding to the last charging action matched.  <b>Important</b> This is a customer-specific attribute.

Attributes	Description
<b>sn-rating-group</b>	This attribute reports the rating group corresponding to last charging action matched.  <b>Important</b> This attribute configuration currently supports only static and predefined rules and ruledefs. It will NOT be supported for dynamic rules installed by PCRF.
<b>sn-sequence-no</b>	This attribute reports the unique sequence number (per <b>sn-sequence-group</b> and <b>radius-nas-ip-address</b> ) of EDR identifier and linearly increasing in EDR file.
<b>sn-server-port</b>	This attribute reports the TCP/UDP port number of the server in a subscriber's data flow.
<b>sn-service-id</b>	This attribute reports the Service ID corresponding to last charging action matched.  <b>Important</b> This attribute configuration currently supports only static and predefined rules and ruledefs. It will NOT be supported for dynamic rules installed by PCRF.
<b>sn-st16-ip-addr</b>	This attribute reports the IP address of the chassis handling this flow.  <b>Important</b> Note that this attribute is interchangeable with <b>radius-nas-ip-address</b> for other systems.
<b>sn-start-time</b> [ <b>format</b> <i>format</i> ] <b>localtime</b>	This attribute reports the timestamp for last packet of flow in UTC.
<b>sn-subscriber-imsi</b>	This attribute reports the IMSI number of the subscriber.
<b>sn-subscriber-nat-flow-ip</b>	For NAT in-line service, this attribute reports the NAT IP address of NAT-enabled subscriber.
<b>sn-subscriber-nat-flow-port</b>	For NAT in-line service, this attribute reports the NAT port number of NAT-enabled subscriber.
<b>sn-subscriber-port</b>	This attribute reports the TCP/UDP port number of the Mobile handling subscriber data flow.
<b>sn-volume-amt</b> { <b>ip</b>   <b>tcp</b> } { <b>bytes</b>   <b>pkts</b> } { <b>uplink</b>   <b>downlink</b> }	This attribute reports IP/TCP protocol-specific volume amount of downlink/uplink bytes/packets during a flow. This includes all the bytes/packets received by ECS, including the bytes/packets dropped and retransmitted by ECS.

Attributes	Description
<b>sn-volume-dropped-amt</b> { ip   tcp } { bytes   packets } { downlink   uplink }	For Stateful Firewall in-line service, this attribute reports IP/TCP protocol-specific volume amount of downlink/uplink bytes/packets dropped by Stateful Firewall during a flow.
<b>sn-volume-ip-with-rtsp-or-rtp</b> bytes { downlink   priority   uplink }	This attribute reports the IP volume amount of downlink/uplink bytes of an RTSP flow and the RTP flows controlled by it, or Comma Separated Value (CSV) position priority of this field. If <b>uplink</b> or <b>downlink</b> is not specified it shows the total of both.
<b>sn-vrf-name</b>	This attribute indicates the VRF name associated with the base session of NEMO. <b>Important</b> This is a customer-specific attribute.
<b>subscriber-ipv4-address</b>	For NAT in-line service, this attribute generates the subscriber IPv4 address in the NBR.
<b>subscriber-ipv6-address</b>	For NAT in-line service, this attribute generates the subscriber IPv6 prefix in the NBR.
<b>transaction-charge-downlink-bytes</b>	This attribute reports the total charge downlink bytes for the transaction. Excludes the dropped/retransmitted bytes from the total transaction downlink bytes.
<b>transaction-charge-downlink-packets</b>	This attribute reports the total charge downlink packets for the transaction. Excludes the dropped/retransmitted packets from the total transaction downlink packets.
<b>transaction-charge-uplink-bytes</b>	This attribute reports the total charge uplink bytes for the transaction. Excludes the dropped/retransmitted bytes from the total transaction uplink bytes.
<b>transaction-charge-uplink-packets</b>	This attribute reports the total charge uplink packets for the transaction. Excludes the dropped/retransmitted packets from the total transaction uplink packets.
<b>transaction-downlink-bytes</b>	This attribute reports the total downlink bytes for the transaction.
<b>transaction-downlink-packets</b>	This attribute reports the total downlink packets for the transaction.
<b>transaction-uplink-bytes</b>	This attribute reports the total uplink bytes for the transaction.
<b>transaction-uplink-packets</b>	This attribute reports the total uplink packets for the transaction.

**format { MM/DD/YY-HH:MM:SS | MM/DD/YY-HH:MM:SS:sss | MM/DD/YYYY-HH:MM:SS | MM/DD/YYYY-HH:MM:SS:sss | YYYY/MM/DD-HH:MM:SS | MM/DD/YYYY-HH:MM:SS:sss | YYYYMMDDHHMMSS | YYYYMMDDHHMMSSsss | seconds**

Specifies the timestamp format.

In releases prior to 18.0, the current timestamps available in the EDR format configuration allow recording of time information only up to seconds level. In 18.0 and later releases, new timestamp formats are added to allow recording of time information up to milliseconds granularity.

This feature enables to record timestamps of the events at finer granularity. The timestamps will be populated according to the selected timestamp format whenever any of the predefined events/event triggers for generating EDRs is encountered.

### localtime

Specifies timestamps with the local time. By default, timestamps are displayed in GMT/UTC.

**{ ip | tcp } { bytes | pkts } { downlink | uplink }**

Specifies bytes/packets sent/received from/by mobile.

### priority *priority*

Specifies the position priority of the value within the EDR record. Lower numbered priorities (across all attribute, event-label, and rule-variable) occur first.

*priority* must be an integer from 1 through 65535. Up to 50 position priorities (across all attribute, event-label, and rule-variable) can be configured.

### Usage Guidelines

Use this command to set the attributes and priority for EDR file format.

A particular field in EDR format can be entered multiple times at different priorities. While removing the EDR field using the **no attribute** command either you can remove all occurrences of a particular field by specifying the field name or a single occurrence by additionally specifying the optional **priority** keyword.

In 21.1 and later releases, a maximum of 75 EDR attribute fields can be configured in an EDR record. The limit is expanded from 50 fields up to 75 fields.

### Example

The following is an example of this command:

```
attribute radius-user-name priority 12
```

## delimiter

This command allows you to configure a comma or a tab as a delimiter character for EDRs.

### Product

All

### Privilege

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > EDR Format Configuration

**active-charging service** *service\_name* > **edr-format** *format\_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acs-edr)#
```

**Syntax Description**

**delimiter** { **comma** | **tab** }  
**no delimiter**

**no**

This **no** variant reverts back to the default configuration. By default, comma is used as the delimiter for EDRs.

**comma**

This keyword allows you to specify comma as an EDRdelimiter. Comma is the default configuration.

**tab**

This keyword allows you to specify tab as an EDR delimiter.

**Usage Guidelines**

Use this command to configure either comma or tab as the delimiter between EDR fields.

The comma character is currently used as the delimiter between EDR fields. But comma is a valid character for URLs. Thus when a EDR URL contains a comma, the downstream parser encounters issues.

Hence, this feature has been developed to allow TAB as an additional character to be used as the delimiter in the EDR file. For backward compatibility reasons, this CLI configuration is introduced to choose the delimiter character between both comma and TAB.

**Example**

The following example specifies tab as the delimiter configuration for EDRs:

```
delimiter tab
```

**end**

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

**end**

**Usage Guidelines**

Use this command to return to the Exec mode.

# event-label

This command allows you to specify an optional event label/identifier to be used as an attribute in the EDRs.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > ACS Configuration > EDR Format Configuration

**active-charging service** *service\_name* > **edr-format** *format\_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acs-edr)#
```

---

**Syntax Description**

**event-label** *event\_label* **priority** *priority*  
**no event-label**

**no**

If previously configured, removes the event label configuration.

***event\_label***

Specifies the event label/identifier to be used as EDR attribute.

*event\_label* must be an alphanumeric string of 1 through 63 characters.

***priority priority***

Specifies the Comma Separated Value (CSV) position of the attribute (label/identifier) in the EDR.

*priority* must be an integer from 1 through 65535.

---

**Usage Guidelines**

Use this command to configure an optional event label/identifier as an attribute in the EDR and its position in the EDR.

**Example**

The following is an example of this command:

```
event-label radius_csv1 priority 23
```

# exit

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

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator



**Syntax Description** `exit`

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

## rule-variable

This command allows you to specify fields and their order in EDRs.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > ACS Configuration > EDR Format Configuration

**active-charging service** *service\_name* > **edr-format** *format\_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acs-edr)#
```

**Syntax Description** **rule-variable** *rule\_variable* **priority** *priority* [ **in-quotes** ]  
**no rule-variable** *rule\_variable* [ **priority** *priority* ]

**no**

If previously configured, removes the specified rule variable configuration.

### **rule\_variable**

Specifies the rule variable for the EDR format.

*rule\_variable* must be one of the following options:

- **bearer 3gpp**: 3GPP bearer-related fields:
  - **charging-id**: Charging ID of the bearer flow
  - **imei**: IMEI or IMEISV (depending on the case) associated with the bearer flow. Only available in StarOS 8.1 and later releases.
  - **imsi**: Specific Mobile Station Identification number.
  - **pcrf-correlation-id**: PCRF correlation ID of the bearer flow sent by Gx interface.
  - **rat-type**: RAT type associated with the bearer flow. Only available in StarOS 8.1 and later releases.
  - **sgsn-address**: SGSN associated with the bearer flow. Only available in StarOS 8.1 and later releases. For MIPv6 calls, sgsn-address field is populated with HSGW address.
  - **user-location-information**: User location information associated with the bearer flow. Only available in StarOS 8.1 and later releases.
- **bearer 3gpp2**: 3GPP2 bearer-related fields:
  - **always-on**: 3GPP2 always on indicator

- **bsid**: 3GPP2 BSID
- **esn**: 3GPP2 ESN
- **ip-qos**: 3GPP2 IP QoS
- **ip-technology**: 3GPP2 IP technology
- **release-indicator**: 3GPP2 release indicator
- **service-option**: 3GPP2 service option
- **session-begin**: 3GPP2 session begin indicator
- **session-continue**: 3GPP2 session continue indicator
  
- **bearer ggsn-address**: GGSN IP address field. For MIPv6 calls, ggsn-address field in EDR will be populated with PGW address.
- **bearer qci**: QCI of the bearer corresponding to the flow for which the EDR is getting generated.
- **dns**: Domain Name System (DNS) related fields:
  - **answer-ip-list**: DNS Host IP list. A maximum of 4 IP addresses will be part of an EDR.
  - **answer-name**: DNS answer name. This depends upon query type.
  - **previous-state**: DNS previous state information
  - **query-name**: DNS query name
  - **query-type**: DNS query type. Numeric value as per the DNS specifications.
  - **return-code**: DNS query response code
  - **state**: DNS current state information
  - **tid**: DNS Transaction Identifier
  
- **file-transfer**: File Transfer related fields:
  - **chunk-number**: Number of chunks
  - **current-chunk-length**: Length of current chunk
  - **declared-chunk-length**: Declared size of the chunk
  - **declared-file-size**: Declared size of the file
  - **filename**: Name of the file being transferred
  - **previous-state**: Previous state of session
  - **state**: Current state of session
  - **transferred-file-size**: Transferred size of the file
  
- **flow**: Flow related fields:
  - **ip-control-param**: First 8 bytes of IPv6 header is inserted in EDRs.

- **tethered**: Tethering detected on flow. Enables/disables tethering detection result field in EDRs sent to MUR.
- **tethered-application**: Application based tethering detected on flow.
- **tethered-dns**: DNS-based tethering detected on flow. Either 0 or 1.
- **tethered-ip-ttl**: IP-TTL based tethering detected on flow.
- **ttl**: Time To Live/Max hops value received in the first packet of the flow.
- **ftp**: File Transfer Protocol (FTP) related fields:
  - **client-ip-address**:
  - **client-port**
  - **command name**: Command sent
  - **connection-type**
  - **filename**: File name being transferred in any of the FTP-related FTP command
  - **pdu-length**: FTP PDU length
  - **pdu-type**
  - **previous-state**: Previous state of FTP session
  - **reply code**
  - **server-ip-address**
  - **server-port**
  - **session-length**: Total length of FTP session
  - **state**: Current state of FTP session
  - **url**: URL of file
  - **user**: User identifier
- **http**: Hypertext Transport Protocol (HTTP) related fields:
  - **accept**: Content types that are acceptable for the response
  - **attribute-in-data**: Dynamic header field in application payload
  - **attribute-in-url**: Dynamic header field in URL
  - **content disposition**
  - **content length**
  - **content type**
  - **cookie**: HTTP cookie header
  - **domain**
  - **dnt**

- **header-length**: HTTP header length
- **host**
- **payload-length**: Payload length
- **pdu-length**
- **previous-state**: Previous state of session
- **referer**
- **reply code**: HTTP response
- **request method**: HTTP request method
- **session-length**: Total length of HTTP session
- **state**: Current state of session
- **transaction-length**: Total length of HTTP transaction
- **transfer-encoding**: Transfer encoding
- **uri**: Uniform Resource Identifier
- **url**: Uniform Resource Locator
  - **length size**: This optional filter allows the user to configure the HTTP URL length from 1 to 4095. The EDR rule-variable "HTPP URL" supports the maximum length of 4095. That is, any URL greater than the maximum length is truncated and then written to EDR.
 

In 17.0 and later releases: The length of HTTP URL is from 1 to 4095.

In 15.0 and 16.0 releases: The length of HTTP URL is from 1 to 255.

In releases prior to 15.0: The length of HTTP URL is from 1 to 127.
- **user-agent**
  - **length size**: This optional filter allows the user to configure the HTTP User-Agent length from 1 to 255. In releases prior to 15.0, the EDR rule-variable "HTPP User-Agent" supports the maximum length of 127. That is, any user-agent greater than 127 is truncated and then written to EDR.
- **version**
- **x-header**: extension header
- **ad-delivered, ad-replaced, compression-bytes-in, compression-bytes-out, dns-resolution-locally, dns-resolution-remotely, tpo-enabled**




---

**tpot** The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

---

- **icmp**: Internet Control Message Protocol (ICMP) related fields:

- **code**: ICMP code
- **type**: ICMP type
- **icmpv6**: Internet Control Message Protocol Version 6 (ICMPv6) related fields:
  - **code**: ICMPv6 code
  - **type**: ICMPv6 type
- **imap**: Internet Message Access Protocol (IMAP) related fields:
  - **cc**: IMAP e-mail CC field
  - **command**: IMAP command
  - **content**
  - **date**: IMAP e-mail Date field
  - **final-reply**: IMAP final reply
  - **from**: IMAP e-mail From field
  - **mail-size**: IMAP size of e-mail in RFC822 format
  - **mailbox-size**: IMAP number of e-mails in the mailbox
  - **message-type**: IMAP message type
  - **previous-state**: IMAP session previous state
  - **session-length**: IMAP session length
  - **session-previous-state**: IMAP session previous state
  - **session-state**: IMAP session state
  - **state**: IMAP state
  - **subject**: IMAP e-mail Subject field
  - **to**: IMAP e-mail To field
- **ip**: Internet Protocol (IP) related fields:
  - **dst-address**: destination IP address
  - **protocol**: Protocol being transported by IP packet
  - **server-ip-address**: IP address of server. This field in EDR contains either the IPv4 or IPv6 address of the server for a particular flow (flow level). The maximum length of this field is 48 characters. For an IPv6 address, the maximum length is 45 characters; for an IPv4 address, the maximum length is 15 characters.
  - **src-address**: Source IP address
  - **subscriber-ip-address**: IP address of subscriber. This field in EDR contains either the IPv4 or IPv6 address of the client/subscriber for a particular call (subscriber level). The value of this field does not change for a particular call. The maximum length of this field is 48 characters. For an IPv6

address, the maximum length is 45 characters. For an IPv4 address, the maximum length is 15 characters.

- **total-length**: Total length of packet, including payload
- **version**: IP version
- **mms**: Multimedia Message Service (MMS) related fields:
  - **bcc**
  - **cc**
  - **content location**
  - **content type**
  - **date** [ **format** { **MM/DD/YYYY-HH:MM:SS** | **YYYY/MM/DD-HH:MM:SS** } ]
  - **from**
  - **message-size**
  - **previous-state**
  - **response status**
  - **state**
  - **subject**
  - **tid**
  - **to**
- **p2p**: Peer-to-peer protocol related fields:
  - **app-identifier** { **quic-sni** | **tls-cname** | **tls-sni** }: P2P application-identifiers - QUIC-SNI, TLS-common name, or TLS-SNI
  - **tls-version**: The TLS version variable is displayed from the P2P dynamic library. The following values of SSL version that is used by UE for the TLS connection on the flow are considered:
    - 0 – Invalid
    - 1 – TLS1.0
    - 2 – TLS1.1
    - 3 – TLS1.2
    - 4 – TLS1.3
  - **bailout-pkt-num** : Number of packets taken by plugin to detect the application in the flow before flow was offload to VPP. This variable is supported only in CUPS.
  - **duration**: P2P protocol duration
  - **protocol**: P2P protocol
  - **protocol-group**: Associated protocol group of the specific P2P protocol/application

- **ssl-params**: Specifies the SSL flow parameters.
  - **cert-issuer-cname**: Specifies the SSL Certificate Issuer CName.
  - **cert-subject-cname**: Specifies the SSL Certificate Subject Organization Name.
  - **cert-issuer-oname**: Specifies the SSL Certificate Issuer Organization Name.
  - **cert-validity**: Specifies the validity of SSL Certificate.
  - **ssl-decode-failure**: Specifies the reason for SSL Decode failure.
  
- **pop3**: Post Office Protocol version 3 (POP3) related fields:
  - **command name**: Command of POP3 session
  - **mail-size**: Mail size
  - **pdu-length**: Length of POP3 PDU
  - **pdu-type**: Type of packet
  - **previous-state**: Previous state of POP3 session
  - **reply status**: Reply for the POP3 command
  - **session-length**: Total length of POP3 session
  - **state**: Current state of POP3 session
  - **user-name**: User of POP3 session
  
- **rtcp**: RTP Control Protocol (RTCP) related fields:
  - **control-session-flow-id**: Flow ID of the controlling RTSP/SIP session
  - **jitter**: RTCP interarrival jitter
  - **rtsp-id**: RTSP ID of the RTCP flow
  - **uri**: URI of the control protocol related to the RTCP flow
  
- **rtp**: Real-time Transfer Protocol (RTP) related fields:
  - **control-session-flow-id**: Flow ID of the controlling RTSP/SIP session
  - **pdu-length**: Length of RTP PDU
  - **rtsp-id**: RTSP ID of the flow
  - **session-length**: Total length of RTP session
  - **uri**: URI of the control protocol related to the RTP flow
  
- **rtsp**: Real Time Streaming Protocol (RTSP) related fields:
  - **command-id**: RTSP command ID
  - **content type**
  - **date**: RTSP Date field

- **previous-state**: RTSP previous state
- **reply code**
- **request method 1**: play method
- **request method 2**: setup method
- **request method 3**: pause method
- **request method 4**: record method
- **request method 5**: options method
- **request method 6**: redirect method
- **request method 7**: describe method
- **request method 8**: announce method
- **request method 9**: teardown method
- **request method 10**: get-parameter method
- **request method 11**: set-parameter method
- **request packet**
- **rtp-uri**: RTSP RTP-Info stream-uri field
- **session-id**: RTSP session-id field
- **session-length**: Total number of bytes passed through the RTSP data session
- **state**: RTSP state
- **uri**: RTSP uri field
- **uri sub-part**
- **user-agent**: RTSP user-agent field
- **sdp**: Session Description Protocol (SDP) related fields:
  - **connection-ip-address**: IP address in SDP connection field
  - **media-audio-port**: Port used for audio media
  - **media-video-port**: Port used for video media
- **secure-http**: HTTPS related field.
- **sip**: Session Initiation Protocol (SIP) related fields:
  - **call-id**: SIP call-id field
  - **content type**
  - **from**: SIP From field
  - **previous-state**: SIP previous state



- **reply code**
- **request method**
- **request packet**
- **state**: SIP state
- **to**: SIP To field
- **uri**: SIP URI field
- **uri sub-part**
  
- **smtp**: Simple Mail Transfer Protocol (SMTP) related fields:
  - **command name**: Command of SMTP session
  - **mail-size**: Size of given mail
  - **pdu-length**: Length of SMTP PDU
  - **previous-state**: Previous state of SMTP session
  - **recipient**: SMTP e-mail Recipient field
  - **reply status**: Response for the SMTP command
  - **sender**: SMTP e-mail Sender field
  - **session-length**: Total length of SMTP session
  - **state**: Current state of SMTP session
  
- **tcp**: Transmission Control Protocol (TCP) related fields:
  - **dst-port**: TCP destination port
  - **duplicate**: TCP retransmitted/duplicate packet
  - **flag**: Current packet TCP flag
  - **os-signature**: OS signature string for IPv4 TCP flow. Enables/disables OS Signature field in EDRs sent to MUR.
  - **out-of-order**: TCP out of order packet analyzed
  - **payload-length**: TCP payload length
  - **previous-state**: Previous state of MS
  - **sn-tcp-accl**: TCP Acceleration enabled on flow. Either 0 or 1.
  - **sn-tcp-accl-reject-reason**: Reason for not accelerating the TCP flow.
  - **sn-tcp-min-rtt**: Specifies minimum RTT observed for accelerated TCP flow.
  - **sn-tcp-rtt**: Specifies smoothed RTT for accelerated TCP flow.
  - **src-port**: TCP source port
  - **state**: Current state of MS

- **tpo-enabled**




---

**important** The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

---

- **syn-control-params**: 8 bytes following the TCP Acknowledgement in the TCP SYN packet displayed as hexadecimal string of characters.
- **syn-options**: All TCP options received in the TCP SYN packet displayed as hexadecimal string of characters.
- **syn-seq**: The absolute 4 byte value of the sequence number received in the TCP SYN packet displayed as decimal value.
- **v6-os-signature**: OS signature string for IPv6 TCP flow. Enables/disables OS Signature field in EDRs sent to MUR.
- **tls sni**: TLS/SSL SNI field (SNI rule variable configured for TLS/SSL flows in EDR).
- **traffic-type**: Traffic type of flow (voice or non-voice depending upon flow type).
- **udp**: User Datagram Protocol (UDP) related fields:
  - **dst-port**: UDP destination port
  - **src-port**: UDP source port
- **voip-duration**: Duration of voice call, in seconds. For a flow in which voice call end is detected, output will be a non-zero value. For other flows it will be zero.  
This is no longer supported for P2P in 14.0 and later releases.
- **wsp**: Wireless Session Protocol (WSP) related fields:
  - **content type**
  - **domain**: WSP domain name
  - **host**: WSP host name
  - **pdu-length**: WSP PDU length
  - **pdu-type**: WSP PDU type
  - **reply code**
  - **session-length**: WSP total packet length
  - **tid**: WSP transaction identifier
  - **total-length**: WSP total packet length
  - **url**: WSP URL
  - **user-agent**: WSP user agent
- **wtp**: Wireless Transaction Protocol (WTP) related fields:

- **gtr**: Group Transmission Flag
- **pdu-length**: PDU length of the WTP packet
- **pdu-type**: WTP protocol data unit information
- **previous-state**: WTP previous state information
- **state**: WTP current state information
- **tid**: WTP transaction identifier
- **transaction class**: WTP transaction class
- **ttr**: WTP Trailer Transmission flag

**Important**

For more information on protocol-based rules, see the *ACS Ruledef Configuration Mode Commands* chapter.

**priority priority**

Specifies the CSV position of the field (protocol rule) in the EDR.

*priority* must be an integer from 1 through 65535.

**in-quotes**

Specifies placing double quotes (" ") around the specified field in the EDR.

**Important**

In this release, this keyword is only valid for the MMS protocol **to** and **subject** fields. **rule-variable mms to priority priority [in-quotes] rule-variable mms subject priority priority [in-quotes]**

**Usage Guidelines**

Use this command to specify what field appears in which order in the EDR.

A particular field in an EDR format can be entered multiple times with different priorities. While removing the EDR field using the **no rule-variable** command you can remove all occurrences of a particular field by specifying the field name or a single occurrence by additionally specifying the optional **priority** keyword.

**Example**

The following is an example of this command:

```
rule-variable tcp dst-port priority 36
```

rule-variable



## CHAPTER 5

# EDR Module Configuration Mode Commands

The EDR Module Configuration Mode allows you to configure Event Data Record (EDR) file transfer parameters.

### Command Modes

Exec > Global Configuration > Context Configuration > EDR Module Configuration

**configure > context** *context\_name* > **edr-module active-charging-service**

Entering the above command sequence results in the following prompt:

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



### Important

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

- [cdr, on page 39](#)
- [end, on page 44](#)
- [exit, on page 44](#)
- [file, on page 44](#)

## cdr

This command allows you to configure EDR/UDR file transfer parameters.

### Product

All

### Privilege

Security Administrator, Administrator

### Command Modes

Exec > Global Configuration > Context Configuration > EDR Module Configuration

**configure > context** *context\_name* > **edr-module active-charging-service**

Entering the above command sequence results in the following prompt:

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

### Syntax Description

```
cdr { purge { storage-limit storage_limit | time-limit time_limit } [ max-files max_records_to_purge ] | push-interval push_interval | push-trigger trigger_percentage | remove-file-after-transfer |
```

```
transfer-mode { pull [ module-only ] | push primary { encrypted-url
encrypted_url | url url } [ [ max-files max_records ] [ max-tasks task_num ] [
module-only ] [ secondary { encrypted-secondary-url encrypted_secondary_url |
secondary-url secondary_url } ] [ source-address ip_address ] [ via
local-context ] + ] | use-harddisk } | push-count push_count
default cdr [ purge | push-interval | push-trigger space-usage-percent |
remove-file-after-transfer | transfer-mode [ module-only | push via ] |
use-harddisk ] + | push-count
no cdr [ purge | remove-file-after-transfer | use-harddisk ] +
```

### default

Configures the default setting for the specified keyword(s):

- **purge**: Disabled
- **push-interval**: 300 seconds
- **push-trigger**: 80 percent
- **remove-file-after-transfer**: Disabled
- **transfer mode**: Pull
- **push via**: LC is used for push
- **use-harddisk**: Disabled



### Important

The **use-harddisk** keyword is available only on the ASR 5500 chassis.

### no

If previously configured, disables the specified configuration:

- **purge**: Disables purging of records.
- **remove-file-after-transfer**: Retains a copy of the file even after it has been pushed or pulled to another server.
- **use-harddisk**: Disables data storage on the ASR 5500 hard disk array.



**Important** The **use-harddisk** keyword is available only on the ASR 5500 chassis.

- **push-count** *push\_count*: Specifies the number of EDR/CDR/UDR files transferred in each EDR/UDR push SFTP session. Default value is "1". *push\_count* is configured as an integer value between 1 and 32, inclusive.

**purge** { **storage-limit** *storage\_limit* | **time-limit** *time\_limit* } [ **max-files** *max\_records\_to\_purge* ]

Specifies to purge/delete the EDR records based on "time" or "volume" limit.

When the configured threshold limit is reached on the hard disk drive, the records that are created dynamically in the `/mnt/hd-raid/data/records/` directory are automatically deleted. Files that are manually created should be deleted manually.

- **storage-limit** *storage\_limit*: Specifies to start deleting files when the specified megabytes of space is used for storage. The *storage\_limit* specifies the volume limit for the record files, in megabytes, and must be an integer from 10 through 143360.
- **time-limit** *time\_limit*: Specifies to start deleting files older than the specified time limit. The *time\_limit* specifies the time limit for the record files, and must be an integer from 600 through 2592000.
- **max-files** *max\_records\_to\_purge*: Specifies the maximum number of records to purge.

The *max\_records\_to\_purge* can be 0, or an integer from 1000 through 10000. If the value is set to 0, during each cycle, the records will be deleted until the purge condition is satisfied. If the value is set between 1000 and 10000, during each cycle, the records will be deleted until either the purge condition is satisfied or the number of records deleted equals the configured **max-files** value.

Default: 0

#### **push-interval** *push\_interval*

Specifies the transfer interval (in seconds) to push EDR and UDR files to an external file server.

The *push\_interval* must be an integer from 60 through 3600.

Default: 300

#### **push-trigger space-usage-percent** *trigger\_percentage*

Specifies the EDR/UDR disk space utilization percentage, upon reaching which an automatic push is triggered and files are transferred to the configured external server.

The *trigger\_percentage* specifies the EDR/UDR disk utilization percentage for triggering push, and must be an integer from 10 through 80.

Default: 80

#### **remove-file-after-transfer**

Specifies that the system must delete EDR/UDR files after they are transferred to the external file server.

Default: Disabled

**transfer-mode** { **pull** [ **module-only** ] | **push** **primary** { **encrypted-url** *encrypted\_url* | **url** *url* } [ [ **max-files** *max\_records* ] [ **max-tasks** *task\_num* ] [ **module-only** ] [ **secondary** { **encrypted-secondary-url** *encrypted\_secondary\_url* | **secondary-url** *secondary\_url* } ] [ **source-address** *ip\_address* ] [ **via local-context** ] + ]

Specifies the EDR/UDR file transfer mode—how the EDR and UDR files are transferred to the external file server.

- **pull**: Specifies that the external server is to pull the EDR files.
- **push**: Specifies that the system is to push EDR files to the external server for ASR 5500.
- **max-files** *max\_records*: Specifies the maximum number of files sent per iteration based on configured file size.

Default: 4000

- **max-tasks** *task\_num*: Specifies the maximum number of tasks (child processes) that will be spawned to push the files to the remote server. The *task\_num* must be an integer from 4 through 8.

Default: 4




---

**Important** Note that increasing the number of child processes will improve the record transfer rate. However, spawning more child will consume additional resource. So, this option needs to be used with proper resource analysis.

---

- **module-only**: Specifies that the transfer-mode is only applicable to the EDR module; if not configured it is applicable to both EDR and UDR modules. This enables to support individual record transfer-mode configuration for each module.

- **primary encrypted-url** *encrypted\_url*: Specifies the primary URL location in encrypted format to which the system pushes the EDR files.

The *encrypted\_url* must be the location in an encrypted format, and must be an alphanumeric string of 1 through 1024 characters.

- **primary url** *url*: Specifies the primary URL location to which the system pushes the EDR files.

The *url* must be the location, and must be an alphanumeric string of 1 through 1024 characters in the "*//user:password@host:[port]/directory*" format.

- **secondary encrypted-secondary-url** *encrypted\_secondary\_url*: Specifies the secondary URL location in encrypted format to which the system pushes the EDR files when the primary location is unreachable or fails.

The *encrypted\_secondary\_url* must be the secondary location in an encrypted format, and must be an alphanumeric string of 1 through 1024 characters in the "*//user:password@host:[port]/directory*" format.

- **secondary secondary-url** *secondary\_url*: Specifies the secondary location to which the system pushes the EDR files when the primary location is unreachable or fails.

The *secondary\_url* must be the secondary location, and must be an alphanumeric string of 1 through 1024 characters in the "*//user:password@host:[port]/directory*" format.

- **source-address** *ip\_address*: Configures the source IP address to be used to establish the connection for the SFTP/SSH file-transfer operation.

- **via local-context**: Configuration to select LC/SPIO for transfer of EDRs. The system pushes the EDR files via SPIO in the local context.

## use-harddisk



### Important

---

The **use-harddisk** keyword is available only on the ASR 5500 chassis.

---



Specifies that on the ASR 5500 chassis the hard disk the FSC hard disk array be used to store EDR/UDR files. On configuring to use the hard disk for EDR/UDR storage, EDR/UDR files are transferred from DPCs to the hard disk array. Default: Disabled

+

Indicates that multiple keywords can be specified in a single command entry. When the "+" appears in the syntax, any of the keywords that appear prior to the "+" can be entered in any order.

#### **push-count** *push\_count*

Specifies the number of EDR/CDR/UDR files transferred in each EDR/UDR push SFTP session. Default value is "1". *push\_count* is configured as an integer value between 1 and 32,inclusive.



**Note** When *push\_count* is set to "1", file transfer operation is functionally identical to legacy behavior.

#### **Usage Guidelines**

Use this command to configure how the EDRs are moved and stored.

On the ASR 5500 chassis, you must run this command only from the local context. If you run this command in any other context it will fail and result in an error message.

If PUSH transfer mode is configured, the external server URL to which the EDR files need to be transferred to must be specified. The configuration allows a primary and a secondary server to be configured. Configuring the secondary server is optional. Whenever a file transfer to the primary server fails for four consecutive times, the files will be transferred to the secondary server. The transfer will switch back to the original primary server when:

- Four consecutive transfer failures to the secondary server occur.
- After switching from the primary server, 30 minutes elapses.

When changing the transfer mode from pull to push, disable the PULL from the external server. Make sure that the push server URL configured is accessible from the local context. Also, make sure that the base directory that is mentioned contains *udr* directory created within it.

After changing the transfer mode from push to pull, enable external server for ASR 5500. Any of the ongoing PUSH activity will continue till all the scheduled file transfers are completed. If there is no PUSH activity going on at the time of this configuration change, all the PUSH related configuration is nullified immediately.

The ***cdr use-harddisk*** command is available only on the ASR 5500 chassis. This command can be run only in a context where CDRMOD is running. Configuring in any other context will result in failure with the message "*Failure: Please Check if CDRMOD is running in this context or not.*"

The ***cdr use-harddisk*** command can be configured either in the EDR or UDR module, but will be applicable to both record types. Configuring in one of the modules will prevent the configuration to be applied in the other module. Any change to this configuration must be done in the module in which it was configured, the change will be applied to both record types.

The VPNMgr can send a maximum of 4000 files to the remote server per iteration. However if the individual file size is big (say when compression is not enabled), then while transferring 4000 files SFTP operation takes a lot of time. To prevent this, the ***cdr transfer-mode push*** command can be configured with the keyword ***max-files***, which allows operators to configure the maximum number of files sent per iteration based on configured file size.

**end****Example**

The following command retains a copy of the data file after it has been transferred to the storage location:

```
no cdr remove-file-after-transfer
```

## end

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

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Syntax Description</b>	<b>end</b>
<b>Usage Guidelines</b>	Use this command to return to the Exec mode.

## exit

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

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Syntax Description</b>	<b>exit</b>
<b>Usage Guidelines</b>	Use this command to return to the parent configuration mode.

## file

This command allows you to configure EDR file parameters.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > Global Configuration > Context Configuration > EDR Module Configuration <b>configure &gt; context <i>context_name</i> &gt; edr-module active-charging-service</b>
	Entering the above command sequence results in the following prompt: <pre>[<i>context_name</i>]host_name(config-edr)#</pre>

**Syntax Description**

```
file [ charging-service-name { include | omit } ] [ compression { gzip |
  none } ] [ current-prefix string ] [ delete-timeout seconds ] [ directory
  directory_name ] [ edr-format-name ] [ exclude-checksum-record ] [
  field-separator { hyphen | omit | underscore } ] [ file-sequence-number
  rulebase-seq-num ] [ headers ] [ name file_name ] [ reset-indicator ] [
  rotation [ num-records number | tariff-time minute minute_value hour hour_value
  | time seconds | volume bytes ] ] [ sequence-number { length length | omit
  | padded | padded-six-length | unpadded } ] [ storage-limit limit ] [
  single-edr-format ] [ time-stamp { expanded-format | rotated-format |
  unix-format } ] [ trailing-text string ] [ trap-on-file-delete ] [
  unique-seq-num ] [ xor-final-record ] +
default file [ charging-service-name ] [ compression ] [ current-prefix
] [ delete-timeout ] [ directory ] [ edr-format-name ] [ field-separator
] [ file-sequence-number ] [ headers ] [ name ] [ reset-indicator ] [
rotation { num-records | tariff-time | time | volume } ] [ sequence-number
] [ storage-limit ] [ time-stamp ] [ trailing-text ] [ unique-seq-num ]
+
```

**default**

Configures the default setting for the specified keyword(s).

**charging-service-name { include | omit }**

Specifies to include/exclude name of the charging service in the file name.

- **include**: Include name of the charging service in the EDR file name.
- **omit**: Exclude name of the charging service in EDR file name.

**compression { gzip | none }**

Specifies compression of EDR files.

- **gzip**: Enables GNU zip compression of the EDR file at approximately 10:1 ratio.
- **none**: Disables Gzip compression.

**current-prefix *string***

Specifies a string to add to the beginning of the EDR file that is currently being used to store EDR records.

*string* must be an alphanumeric string of 1 through 31 characters.

Default: **curr**

**delete-timeout *seconds***

Specifies a timeout period (in seconds) when completed EDR files are deleted. By default, files are never deleted.

*seconds* must be an integer from 3600 through 31536000.

Default: Disabled

**directory *directory\_name***

Specifies a subdirectory in the default directory in which to store EDR files.

*directory\_name* must be an alphanumeric string of 1 through 191 characters.

Default: **/records/edr**

**edr-format-name**

Specifies creation of separate files for EDRs that have different formats. Name of the EDR format is included in the file name.

**exclude-checksum-record**

When entered, this keyword excludes the final record containing #CHECKSUM followed by the 32-bit Cyclic redundancy check (CRC) of all preceding records from the EDR file.

Default: Disabled (inserts checksum record into the EDR file header)

**field-separator [ hyphen | omit | underscore ]**

Specifies the field inclusion/exclusion type of separators between two fields of EDR file name:

- **hyphen**: Specifies to use "-" (hyphen) as the field separator.
- **omit**: Excludes the field separator.
- **underscore**: Specifies to use "\_" (underscore) as the field separator.

**file-sequence-number rulebase-seq-num**

Specifies that the file name sequence numbers must be unique per rulebase and EDR format name combination.

**headers**

Includes a file header summarizing the record layout.

**name *file\_name***

Specifies a string to be used as the base file name for EDR files.

Default: **edr**

*file\_name* must be an alphanumeric string of 1 through 31 characters. The file name format is as follows:

*base\_rulebase\_format\_sequencenum\_timestamp*

- *base*: Specifies the type of record in file or contains the operator-specified string.

Default: **edr**

- *rulebase*: Specifies the name of the ACS rulebase. EDRs from different rulebases go into different EDR files.

- *format*: Specifies the name of the EDR format if **single-edr-format** is specified, else the format field (and the trailing underscore) is omitted from the file name.

- *sequencenum*: This is a 5-digit sequence number to detect the missing file sequence. It is unique among all EDR files on the system.
- *timestamp*: Contains a timestamp based on file creation time in UTC time in MMDDYYYYHHMMSS format.

EDR files that have not been closed have a string added to the beginning of their filenames.

Filename for an EDR file in CSV format that contains information for rulebase named *rulebase1* and an EDR schema named *edr\_schema1* appears as follows:

```
edr_rulebase1_edr_schema1_00005_01302006143409
```

If the file name is not configured the system will create files for EDRs/UDRs/FDRs (xDRs) using the following template with limits to 256 characters:

```
basename_ChargSvcName_timestamp_SeqNumResetIndicator_FileSeqNumber
```

- *basename*: A global-based configurable text string that is unique per system that uniquely identifies the global location of the system running ACS.
- *ChargSvcName*: A system context-based configurable text string that uniquely identifies a specific context-based charging service
- *timestamp*: Date and time at the instance of file creation. Date and time in the form of "MMDDYYYYHHmmSS" where HH is a 24-hour value from 00-23
- *SeqNumResetIndicator*: A one-byte counter used to discern the potential for duplicated FileSeqNumber with a range of 0 to 255, which is incremented by a value of 1 for the following conditions:
  - Failure of an ACS software process on an individual PAC/PSC.
  - Failure of the system such that a second system takes over. For example, a backup or standby system put in place according to Interchassis Session Recovery.
  - File Sequence Number (FileSeqNumber) rollover from 999999999 to 0
- *FileSeqNumber*: Unique file sequence number for the file with 9 digit integer having range from 000000000 to 999999999. It is unique on each system.

File name for a closed xDR file in CSV format that contains information for ACS system *xyz\_city1* and charging service name *prepaid2* with timestamp *12311969190000*, and file sequence number counter reset indicator to *002* for file sequence number *034939002* appears as follows:

```
xyz_city1_prepaid2_12311969190000_002_034939002
```

File name for a running xDR file, not closed, in CSV format that contains information for the same parameters for file sequence number *034939003* prefixed with *curr\_* and appears as follows:

```
curr_xyz_city1_prepaid2_12311969190000_002_034939002
```



### Important

When the "rulebase name" and "edr-format-name" options are enabled through this **file** command, if the "field-separator" value is "underscore" (default value) then, in the filename, the fields Rulebase name and EDR format name will be separated by "hyphen". If the "field-separator" value is "hyphen" then, in the filename, the fields Rulebase name and EDR format name will be separated by "underscore". This will ensure that the number of the fields in the filename is not increased and does not affect the backend billing system.

**reset-indicator**

Specifies inclusion of the reset indicator counter value, from 0 through 255, in the EDR file name, and is incremented (by one) whenever any of the following conditions occur:

- An ACSMgr/SessMgr process fails.
- A peer chassis has taken over in compliance with our Interchassis Session Recovery feature.
- The sequence number, see the **sequence-number** keyword, has rolled over to zero.

**rotation { num-records *number* | tariff-time minute *minute\_value* hour *hour\_value* | time *seconds* | volume *bytes* }**

Specifies when to close an EDR file and create a new one.

- **num-records *number***: Specifies the number of records that should be added to the file. When the number of records in the file reaches the specified value, the file is complete.

*number* must be an integer from 100 through 10240.

Default: 1024

- **time *seconds***: Specifies the period of time (in seconds) to wait before closing the EDR file and creating a new one.

*seconds* must be an integer from 30 through 86400.

Default: 3600

- **tariff-time minute *minute\_value* hour *hour\_value***: Specifies the time of day (hour and minute) at which the files are rotated once per day.

*minute\_value* is an integer value from "0" up to "59".

*hour\_value* is an integer value from "0" up to "23".




---

**important** The options **time** and **tariff-time** are mutually exclusive and only any one of them can be configured. Other file rotation options can be used with either of them.

---

- **volume *bytes***: Specifies the maximum size (in bytes) of the EDR file before closing it and creating a new one.

*bytes* must be an integer from 51200 through 62914560.

Note that a higher setting may improve the compression ratio when the compression keyword is set to *gzip*.

**sequence-number { length *length* | omit | padded | padded-six-length | unpadded }**

Specifies including/excluding sequence number in the file name.

- **length *length***: Includes the sequence number with the specified length.

*length* must be the length of the file sequence number, with preceding zeroes, in the file name, and must be an integer from 1 through 9.




---

**important** The **length** keyword is applicable in both EDR and UDR modules. When applied in both modules without the **file udr-seq-num** configuration, the minimum among the two values will come into effect for both the modules. With the **file udr-seq-num** keyword, each module will use its own value of length.

---

- **omit**: Excludes the sequence number from the file name.
- **padded**: Includes the padded sequence number with preceding zeros in the file name. This is the default setting.
- **padded-six-length**: Includes the padded sequence number with six preceding zeros in the file name.
- **unpadded**: Includes the unpadded sequence number in the file name.

### single-edr-format

Creates separate files for EDRs having different formats.

Default: Disabled

### storage-limit *limit*

Specifies deleting files when the specified amount of space (in bytes) is used up for EDR/UDR file storage RAM on packet processing cards.

The *limit* must be an integer from 10485760 through 536870912. Default: 33554432



### Important

---

The total storage limit is 536870912 bytes (512 MB). This limit is for both UDR and EDR files combined.

---

### time-stamp { **expanded-format** | **rotated-format** | **unix-format** }

Specifies the timestamp of when the file was created be included in the file name.

- **expanded-format**: Specifies the UTC MMDDYYYYHHMMSS format.
- **rotated-format**: Specifies the time stamp format to YYYYMMDDHHMMSS format.
- **unix-format**: Specifies the UNIX format of *x.y*, where *x* is the number of seconds since 1/1/1970 and *y* is the fractional portion of the current second that has elapsed.

### trailing-text *string*

Specifies the inclusion of an arbitrary text string in the file name.

*string* must be an alphanumeric string of 1 through 30 characters.

### trap-on-file-delete

Instructs the system to send an SNMP notification (starCDRFileRemoved) when an EDR/UDR file is deleted due to lack of space.

Default: Disabled

**unique-seq-num**

Specifies that the file sequence numbers that are part of the EDR file names be independently generated. If disabled, a single set of sequence numbers are shared by both UDR and EDR files.

Default: Disabled

**xor-final-record**

Specifies inserting an XOR checksum (in place of the CRC checksum) into the EDR file header if the **exclude-checksum-record** is left at its default setting.

Default: Disabled

+

Indicates that multiple keywords can be specified in a single command entry. When the "+" appears in the syntax, any of the keywords that appear prior to the "+" can be entered in any order.

---

**Usage Guidelines**

Use this command to configure EDR file characteristics.

**Example**

The following command sets the prefix of the current active EDR file to *Current*:

```
file current-prefix Current
```

The following command sets the base file name to *EDRfile*:

```
file name EDRfile
```





## CHAPTER 6

# eGTP Service Configuration Mode Commands

The eGTP Service Configuration Mode is used to create and manage Evolved GPRS Tunneling Protocol (eGTP) interface types and associated parameters.

### Command Modes

Exec > Global Configuration > Context Configuration > eGTP Service Configuration

**configure > context** *context\_name* > **egtp-service** *service\_name*

Entering the above command sequence results in the following prompt:

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



### Important

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



### Important

The commands should be added or removed in the startup config only and not when the node is live.

- [associate](#), on page 51
- [allow-lte-m-rat](#), on page 53
- [collision-handling](#), on page 53
- [cups-enabled](#), on page 54
- [end](#), on page 55
- [exit](#), on page 56
- [gtpc](#), on page 56
- [interface-type](#), on page 63
- [pool](#), on page 65
- [ran-nas decode proto-type-spare cause-value-length](#), on page 67
- [validation-mode](#), on page 67

## associate

Configures an association with a GTP-U service where parameters are applied to the GTP-U data flow. For an SGSN being configured for S4 functionality, this command associates a configured GTP-U service that will enable communication with the SGW over the S4 interface.

---

**Product**

- ePDG
- P-GW
- SAEGW
- SGSN
- SaMOG



**Important** For StarOS releases prior to 16, the ePDG and SGSN are only supported on the ASR 5500 platform.

---



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

---



---

**Privilege** Administrator

---

**Command Modes** Exec > Global Configuration > Context Configuration > eGTP Service Configuration  
**configure > context** *context\_name* > **egtp-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description** **associate gtpu-service** *name*  
**no associate gtpu-service**

**no**

Removes the association to the configured GTP-U service from this service.

**gtpu-service** *name*

Associates a GTP-U service with this eGTP service. *name* must be an alphanumeric string of 1 through 63 characters.

---

**Usage Guidelines** Use this command to associate a GTP-U service with this eGTP service.



**Important** If you modify this command, the parent service (service within which the eGTP/GTP-U service is configured) will automatically restart. Service restart results in dropping of active calls associated with the parent service.

---

### Example

The following command associates this eGTP service with a GTP-U service named *gtpu3*:

```
associate gtpu-service gtpu3
```

# allow-lte-m-rat

Enables **lte-m-rat** as a new RAT type.

## Product

ePDG  
P-GW  
SAEGW



## Important

For StarOS releases prior to 16, the ePDG and SGSN are only supported on the ASR 5500 platform.

## Privilege

Administrator

## Command Modes

Exec > Global Configuration > Context Configuration > eGTP Service Configuration

**configure** > **context** *context\_name* > **egtp-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

## Syntax Description

**allow-lte-m-rat**  
[ **no** ] **gtpc node-feature lte-m**

**no**

Disables the LTE-M configuration.

**gtpc node-feature lte-m**

The **gtpc node-feature lte-m** CLI command is disabled by default.

## Usage Guidelines

Use this command to enable LTE-M as new RAT type.

# collision-handling

Enables operators to configure the behavior of the P-GW for collision handling of the Delete Bearer command (DBcmd) message when the Modify Bearer Request (MBreq) message for the default bearer is pending at the P-GW or S-GW.

## Product

P-GW  
S-GW

## Privilege

Administrator, Security Administrator

## Command Modes

Exec > Global Configuration > Context Configuration > eGTP Service Configuration

**configure** > **context** *context\_name* > **egtp-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description**

```
collision-handling dbcmd-over-mbreq { drop | queue }
[ default | no ] collision-handling dbcmd-over-mbreq
```

**default**

Returns the collision handling for the DBcmd over MBReq transaction to the default behavior. The default behavior is to use pre-StarOS 19.0 behavior: abort the MBReq message and handle the DBcmd message.

**no**

Disables collision handling for the **dbcmd-over-mbreq** transaction.

**collision-handling**

Enables collision handling for the **dbcmd-over-mbreq** transaction.

**drop**

Configures the P-GW to drop the DBcmd message when the MBReq message is pending.

**queue**

Configures the P-GW to queue the DBcmd message when the MBReq is message is pending.

---

**Usage Guidelines**

Use this command when you want more flexibility in configuring the behavior of the P-GW for collision handling of the Delete Bearer command (DBcmd) message when the Modify Bearer Request (MBReq) message for the default bearer is pending at the P-GW.

An EGTP service must be configured in EGTP Service Configuration Mode in order to use this command.

**Example**

This command configures the P-GW to queue the DBcmd message when the MBReq is message is pending.

```
collision-handling dbcmd-over-mbreq queue
```

## cups-enabled




---

**Important**

This command is available in this release only for testing purposes. For more information, contact your Cisco Account representative.

---

Configures eGTPC service with CUPS mode that is applicable only for SAEGW service.

---

**Product**

SAEGW

**Privilege**

Administrator

**Command Modes**

Exec &gt; Global Configuration &gt; Context Configuration &gt; eGTP Service Configuration

**configure > context** *context\_name* > **egtp-service** *service\_name*

Entering the above command sequence results in the following prompt:

*[context\_name]*host\_name(config-egtp-service)#**Syntax Description****[ no ] cups-enabled***name***no**

Removes the association to the configured GTP-U service from this service.

**Usage Guidelines**

The following services should be in STARTED state, and associated under SAEGW service for SAEGW service to move to STARTED state:

1. All eGTPC services should be configured with cups-enabled CLI.
  - S-GW Ingress Service (which is configured as part of SAEGW S-GW Service)
  - S-GW Egress Service (which is configured as part of SAEGW S-GW Service)
  - P-GW Ingress Service (which is configured as part of SAEGW P-GW Service)
2. Other dependent Services like:
  - Sx Service
  - GTP-U Service

There is no requirement to configure GTP-U service under eGTPC service, in case **cups-enabled** CLI is enabled. If GTP-U service is configured along with cups-enabled CLI, then it will not have any affect.

There is no change in non-CUPS behavior.

Any variation in the above mentioned configuration of SAEGW service will not get the Service in STARTED state. The same would be displayed in **show configuration errors** CLI command.

The **show egtp-service all** for eGTPC and **show saegw-service all** for SAEGW will display if the services are CUPS enabled.

The **cups-enabled** CLI command must not be used for standalone P-GW and S-GW service.

**end**

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

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description****end**

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

## exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** **exit**

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

## gtpc

Configure the GPRS Tunneling Protocol Control (GTP-C) plane settings for this service.

**Product** ePDG

MME

P-GW

S-GW

SAEGW

SaMOG

SGSN

**Privilege** Administrator

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

**configure** > **context** *context\_name* > **egtp-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description** **gtpc** { **allow-on-congestion** { **apn-name** *apn\_name* | **arp** *priority\_level* } | **bind** { **ipv4-address** *ipv4\_address* [ **ipv6-address** *ipv6\_address* ] | **ipv6-address** *ipv6\_address* [ **ipv4-address** *ipv4\_address* ] } | **command-messages** { **dual-ip-stack-support** } | **disable** **cause-source** | **echo-interval** *seconds* [ **dynamic** [ **smooth-factor** *multiplier* ] ] | **echo-max-retransmissions** *number* | **echo-retransmission-timeout** *seconds* | **error-response-handling** | **peer-salvation** | **ip** **qos-dscp** { *forwarding\_type* | **max-remote-restart-counter-change** *integer* } | **max-retransmissions** *num* | **node-feature** { **cellular-iot** **network-triggered-service-restoration** | **pgw-restart-notification** } | **path-failure** **detection-policy** { **echo** | **control-restart-counter-change** | **echo-restart-counter-change** } |

```

private-extension overcharge-protection | reject s2b-ho-no-context |
retransmission-timeout seconds | retransmission-timeout-ms milliseconds }
no gtpc { allow-on-congestion { apn-name apn_name | arp priority_level } |
bind { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address
ipv6_address [ ipv4-address ipv4_address] } | command-messages {
dual-ip-stack-support } | disable cause-source | echo-interval |
error-response-handling | node-feature {
cellular-iotnetwork-triggered-service-restoration |
pgw-restart-notification } | path-failure detection-policy |
private-extension overcharge-protection | reject s2b-ho-no-context }
default gtpc disable cause-source |{ echo-interval |
echo-max-retransmissions | echo-retransmission-timeout disable cause-source|
ip qos-dscp | max-retransmissions | node-feature { cellular-iot
network-triggered-service-restoration | pgw-restart-notification } |
path-failure detection-policy | retransmission-timeout |
retransmission-timeout-ms }

```

**no**

Disables or removes the configured GTP-C setting.

**default**

Resets the specified parameter to its default value.

**allow-on-congestion { apn-name *apn\_name* | arp *priority\_level* }**



**Important**

*P-GW, SAEGW, and S-GW only.* This functionality requires that a valid VoLTE license key be installed. Contact your Cisco account representative for information on how to obtain a license.

Enables the prioritized handling for calls under congestion conditions for the specified APN/ARP(s).

- If prioritized APN/ARP handling is enabled, and if the APN/ARP received in a CSReq at the EGTP demux matches any of the configured prioritized APN/ARP values, any valid CSReq will not be rejected at EGTP demux because of congestion control.
- This feature impacts only CSReq handling for new incoming calls.
- P-GW initiated dedicated bearer creation/updating is not changed due to this configuration.

**apn-name** *apn\_name*: Configures the gateway to allow calls for this Access Point Name (APN), even under congestion. *apn\_name* is an alphanumeric string of 1 through 64 characters. A maximum of 3 APNs can be configured.

**arp** *priority\_level*: Configures the gateway to allow calls for this ARP, even under congestion. *priority\_level* sets the priority value as an integer from 1 to 15. A maximum of 8 ARP values can be configured.



**Important**

There is no APN-to-ARP mapping.

**bind** { **ipv4-address** *ipv4\_address* [ **ipv6-address** *ipv6\_address* ] | **ipv6-address** *ipv6\_address* [ **ipv4-address** *iv4p\_address* ] }

Binds the service to an interface with IPv4 address, IPv6 address, or both.

**ipv4-address** *ipv4\_address* [ **ipv6-address** *ipv6\_address* ]: Binds this service to the IPv4 address of a configured interface. Optionally, bind the service to a configured interface with an IPv6 address.

*ipv4\_address* must be entered using IPv4 dotted-decimal notation.

*ipv6\_address* must be entered using IPv6 colon-separated hexadecimal notation.

**ipv6-address** *ipv6\_address* [ **ipv4-address** *ipv4\_address* ]: Binds this service to the IPv6 address of a configured interface. Optionally, bind the service to a configured interface with an IPv4 address.

*ipv6\_address* must be entered using IPv6 colon-separated hexadecimal notation.

*ipv4\_address* must be entered using IPv4 dotted-decimal notation.



#### Important

For binding GTP-C service on S2b interface, either IPv6 or IPv4 bind address shall be used. Binding both IPv4 and IPv6 address is not supported on ePDG.

The **ipv6-address** *ipv6\_address* [ **ipv4-address** *ipv4\_address* ] option is not currently supported on the SGSN.

#### cellular-iot

Enables the Cellular IoT features supported for eGTP Service.

#### command-messages dual-ip-stack-support

**command-messages**: Configuration related to MBC/DBC/BRC messages on S-GW and P-GW.

**dual-ip-stack-support**: Enables to handle command messages on both IPv4/IPv6 transport if supported. By default feature is enabled.

#### disable cause-source

**disable**: Disables functionality at eGTPC level.

**cause-source**: Disables cause source Bit in Cause IE.

#### echo-interval *seconds* [ **dynamic** [ **smooth-factor** *multiplier* ] ]

Configures the duration (in seconds) between the sending of echo request messages. *seconds* is an integer from 60 to 3600.

Default: 60

**dynamic**: Enables the dynamic echo timer for the eGTP service. The dynamic echo timer uses a calculated round trip timer (RTT) to support variances in different paths to peer nodes.

**smooth-factor** *multiplier*: Introduces a multiplier into the dynamic echo timer. *multiplier* is an integer from 1 to 5.

Default: 2



**max-remote-restart-counter-change *integer***

Specifies the counter change after which the P-GW will detect a peer restart. Note that a peer restart will be detected only if the absolute difference between the new and old restart counters is less than the value configured. For example, if the **max-remote-restart-counter-change** is 10 and the current peer restart counter is 251, then eGTP will detect a peer restart only if the new restart counter is 252 through 255 or 0 through 5. Similarly, if the stored restart counter is 1, eGTP will detect a peer restart only if the new restart counter is 2 through 11.

Valid settings are from 1 to 255.

The recommended setting is 32.

The default setting is 255.

**echo-max-retransmissions *number***

Configures the maximum retries for GTP Echo requests. *number* is an integer from 0 to 15. If **echo-max-retransmissions** option is not configured, then the **max-retransmissions** configuration will be used for maximum number of echo retries.

Default: 4

**echo-retransmission-timeout *seconds***

Configures the echo retransmission timeout, in seconds, for the eGTP service. *seconds* is an integer ranging from 1 to 20.

If dynamic echo is enabled (**gtpc echo-interval dynamic**) the value set in this command serves as the dynamic minimum (if the RTT multiplied by the smooth factor is less than the value set in this command, the service uses this value).

Default: 3

**error-response-handling**

Enables error-response-handling on the S-GW. If this command is enabled in the eGTP service, then on receiving a bad response from the peer instead of dropping the message while doing validation eGTP-C informs the S-GW about the bad response received. The S-GW uses this notification from eGTP-C that a bad response is received to send a proper response to the other peer.

**peer-salvation**

Enables peer salvation for inactive GTPv2 peers for EGTP services in this context. When enabled, this functionality is enabled at the specific egtp-service level.

This functionality should be enabled at the context level if it is enabled at the egtp-service level. The configuration sequence is not dependent on enabling this functionality.

The parameter configured at the context level is used when peer-salvation is enabled. Ensure that peer-salvation is configured at all the configured services of a product. For example, sgw-services (egtp-service).

**Note**

- The parameter configured at the context level is used when peer-salvation is enabled. Ensure that peer-salvation is configured at all the configured services of a product. For example, sgw-services (egtp-service).
- All the information (peer statistics/recovery counter and so on) of the particular peer is lost after it is salvaged.
- The context level configuration is applied to egtpinmgr and egtpegmgr separately.

**ip qos-dscp { forwarding\_type }**

Specifies the IP QoS DSCP per-hop behavior (PHB) to be marked on the outer header of signalling packets originating from the LTE component. This is a standards-based feature (RFC 2597 and RFC 2474).

Note that CS (class selector) mode options below are provided to support backward compatibility with the IP precedence field used by some network devices. CS maps one-to-one to IP precedence, where CS1 is IP precedence value 1. If a packet is received from a non-DSCP aware router that used IP precedence markings, then the DSCP router can still understand the encoding as a Class Selector code point.

The following forwarding types are supported:

- **af11**: Designates the use of Assured Forwarding 11 PHB.  
This is the default setting.
- **af12**: Designates the use of Assured Forwarding 12 PHB.
- **af13**: Designates the use of Assured Forwarding 13 PHB.
- **af21**: Designates the use of Assured Forwarding 21 PHB.
- **af22**: Designates the use of Assured Forwarding 22 PHB.
- **af23**: Designates the use of Assured Forwarding 23 PHB.
- **af31**: Designates the use of Assured Forwarding 31 PHB.
- **af32**: Designates the use of Assured Forwarding 32 PHB.
- **af33**: Designates the use of Assured Forwarding 33 PHB.
- **af41**: Designates the use of Assured Forwarding 41 PHB.
- **af42**: Designates the use of Assured Forwarding 42 PHB.
- **af43**: Designates the use of Assured Forwarding 43 PHB.
- **be**: Designates the use of Best Effort forwarding PHB.
- **cs1**: Designates the use of Class Selector code point "CS1".
- **cs2**: Designates the use of Class Selector code point "CS2".
- **cs3**: Designates the use of Class Selector code point "CS3".
- **cs4**: Designates the use of Class Selector code point "CS4".

- **cs5**: Designates the use of Class Selector code point "CS5".
- **cs6**: Designates the use of Class Selector code point "CS6".
- **cs7**: Designates the use of Class Selector code point "CS7".
- **ef**: Designates the use of Expedited Forwarding PHB typically dedicated to low-loss, low-latency traffic.

The assured forwarding behavior groups are listed in the table below.

	<b>Class 1</b>	<b>Class 2</b>	<b>Class 3</b>	<b>Class 4</b>
<b>Low Drop</b>	AF11	AF21	AF31	AF41
<b>Medium Drop</b>	AF12	AF22	AF32	AF42
<b>High Drop</b>	AF13	AF23	AF33	AF43

Traffic marked with a higher class is given priority during congestion periods. If congestion occurs to traffic with the same class, the packets with the higher AF value are dropped first.

#### **max-retransmissions num**

Configures the maximum number of retries for packets as an integer from 0 through 15.

After maximum retransmissions is reached, the path is considered to be failed.

Default: 4

#### **node-feature pgw-restart-notification**

Enables P-GW Restart Notification functionality. Node will start announcement of new supported features to peer nodes in echo as soon as configuration is added.

From release 17.0 onwards, the S4-SGSN and MME support receiving/advertising the P-GW Restart Notification (PRN). This command option must be configured in order to inform S-GW that S4-SGSN and/or MME supports receiving/advertising the PRN in eGTPC echo request/response messages.

Default: Disabled

#### **node-feature network-triggered-service-restoration**

This keyword applies to MME and S-GW only.

Enables Network Triggered Service Restoration (NTSR) functionality as per 3GPP TS 23.007 Release 11 for this eGTP service.

Upon receipt of a Downlink Data Notification (DDN) message including an IMSI, the MME will accept the request and initiate paging including the IMSI in order to force the UE to re-attach. IMSI-based DDN requests contain a zero TEID. Since the UE is not attached, the UE will be paged over the whole MME coverage area.

A different MME may be selected by the eNodeB to service the attach request. Since the MME that serviced the DDN will not be aware that the UE has responded with the attach request, it will stop paging upon a timeout.

#### **path-failure detection-policy echo**

Enables session cleanup upon path failure detected via ECHO timeout toward a peer.

Default: Enabled

If disabled, there is no session cleanup upon path failure detected via ECHO timeout toward a peer; however, SNMP trap/logs will continue to indicate path failure.

#### **path-failure detection-policy control-restart-counter-change**

Enables path failure detection policy when the restart counter in Echo Request/Echo Response messages changes. Used in conjunction with the **max-remote-restart-counter-change** command.

#### **path-failure detection-policy echo-restart-counter-change**

Enables path failure detection policy when the restart counter in Control Request/Control Response messages changes. Used in conjunction with the **max-remote-restart-counter-change** command.

#### **private-extension overcharge-protection**



#### **Important**

From StarOS 19.0 and later releases, this command is obsolete.



#### **Important**

Use of Overcharging Protection requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

Controls whether the PDU will contain overcharge-protection related data in the Indication information element or in the private extension.

- If this keyword is enabled in the eGTP service, then eGTP-C will encode/decode overcharge-protection related data in/from the private extension instead of the Indication IE.
- If this option is disabled in the eGTP service, then the eGTP-C layer will encode/decode overcharge-protection related data in the Indication IE.
- By default, this option is disabled.

#### **reject s2b-ho-no-context**

Allows handoff call on S2b interface, even when eGTP-C does not have a UE context.

#### **retransmission-timeout *seconds***



#### **Important**

In 17.3 and later releases, this option has been deprecated. Use the **retransmission-timeout-ms** option.

Configures GTPv2 control packets (non-echo) retransmission timeout (in seconds) as an integer from 1 to 20.

Default: 5

**retransmission-timeout-ms** *milliseconds*

Configures the control packet retransmission timeout in GTP, in milliseconds <in steps of 100>, ranging from 1000 to 20000.

Default: 5000

**Usage Guidelines**

Use this command to configure GTP-C settings for the current service.

This interface assumes the characteristics of an S11 reference point on the S-GW or MME.

For communication between the S4-SGSN and LTE S-GW, the interface assumes the characteristics of an S4 reference point on the S4-SGSN. Before using the **gtpc** command on the S4-SGSN, a new or existing service must be created or entered using the **egtp-service** command in the *Context Configuration Mode*. Once the eGTP service is configured, the service must be associated with the configured 2G and/or 3G services on the S4-SGSN using the **associate** command in the *SGSN Service Configuration Mode* and/or *GPRS Service Configuration Mode*.

**Important**

If you modify this command, the parent service (service within which the eGTP/GTP-U service is configured) will automatically restart. Service restart results in dropping of active calls associated with the parent service.

**Important**

For ePDG, IPv6 bind address must be used as ePDG supports IPv6 as transport on the S2b interface.

**Example**

The following command binds the service to a GTP-C interface with an IPv4 address of *112.104.215.177*:

```
gtpc bind ipv4-address 112.104.215.177
```

## interface-type

Configures the interface type used by this service.

**Product**

ePDG  
MME  
P-GW  
SAEGW  
S-GW  
SaMOG  
SGSN

**Important**

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

**Privilege**

Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > eGTP Service Configuration

**configure** > **context** *context\_name* > **egtp-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
interface-type { interface-cgw-egress | interface-epdg-egress |
interface-mme | interface-pgw-ingress [ s2a ] [ s2b ] | interface-sgsn |
interface-sgw-egress | interface-sgw-ingress }
```

**interface-cgw-egress**

Specifies the SaMOG Gateway's EGTP interface for egress.

**interface-epdg-egress**

Specifies that the interface has the characteristics of an ePDG's egress EGTP interface.

**interface-mbms-egress**

This keyword is for future development.

**interface-mme**

Specifies that the interface has the characteristics of an eGTP MME S11 reference point to/from an S-GW or an eGTP MME Sv reference point to/from a Mobile Switching Center (MSC).

**interface-pgw-ingress [ s2a ] [ s2b ]**

Specifies that the interface has the characteristics of an eGTP P-GW S5/S8 reference point from an S-GW. The interface assumes the characteristics of either a GTP-C (control Plane) or GTP-U (user plane) reference point.

- **s2a**: P-GW supports the S2a interface. SAEGW does not support the S2a interface at this time.
- **s2b**: P-GW supports the S2b interface. S2b interface support is available on the SAEGW in 18.2 and later releases.

**Note**

The **S2a** and **S2b** keywords will be available only if a valid license is installed. For more information, contact your Cisco account or support representative.

**interface-sgsn**

Specifies that the interface has the characteristics of an eGTP S-GW S4 reference point to/from an SGSN. On an S4-SGSN, this option specifies that the eGTP service is used for an S4-SGSN and gives the service the characteristics required for messaging towards an S-GW (S4) / MME (S3) / S4-SGSN (S16).

**interface-sgw-egress**

Specifies that the interface has the characteristics of an eGTP S-GW S5/S8 reference point to an eGTP P-GW. The interface assumes the characteristics of either a GTP-C (control Plane) or GTP-U (user plane) reference point.

**interface-sgw-ingress**

Specifies that the interface has the characteristics of:

- An eGTP-C S-GW S11 reference point from the MME.
- An eGTP-U S-GW S1-U reference point from the eNodeB.

**Usage Guidelines**

Use this command to specify the type of interface that this service uses. By configuring this command, the interface takes on the characteristics of the selected type.

Disable specific interface support for P-GW by entering the following command:

```
interface-type interface-pgw-ingress
```

**Important**

If you modify this command, the parent service (service within which the eGTP/GTP-U service is configured) will automatically restart. Service restart results in dropping of active calls associated with the parent service.

**Example**

The following command configures the interface bound to this service to maintain the characteristics of an eGTP-C S-GW S11 reference point from an MME:

```
interface-type interface-sgw-ingress
```

The following command accepts or rejects Create Session Request (CSR) on GTP based S2a interface:

```
interface-type interface-pgw-ingress s2a
```

# pool

This command enables the default S4-SGSN functionality for (flex) pooling and enables inclusion of the configured pool hop-counter count in new SGSN context/identity request messages. This command supports S4-SGSN pooling across the S16 interface. The S16 interface provides a GTPv2 path to a peer S4-SGSN.

Support for the S16 interface is provided as part of the S4 interface license. This command sets the S4-SGSN as the default SGSN within a pool. If the default S4-SGSN receives an inbound SGSN context request, it forwards it to the right SGSN in the pool based on the NRI bits of the P-TMSI.

---

**Product** SGSN



---

**Important**

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

---



---

**Privilege** Security Administrator, Administrator

---

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

**configure** > **context** *context\_name* > **egtp-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description**

```
pool { default-sgsn | hop-counter count }
no pool default-sgsn
```

**no**

Disables the default SGSN pooling functionality or removes the SGSN pool hop-counter IE from the GTP Identity/context requests.

**default-sgsn**

Enables the default SGSN pooling functionality.

**hop-counter** *count*

Enables and configures the SGSN pool hop-counter to set the number of hops and to include the configured count in the **new** SGSN Context Requests or the **new** SGSN Identity Requests. *count* is an integer from 1 to 255.

If **default-sgsn** is enabled, then any messages relayed will have the default value of 4 for the counter if the message does not include this hop-counter ID.

Default: 4

---

**Usage Guidelines**

Use this command to enable the default flex functionality without exposing the pool (flex) structure. This functionality provides a means for SGSNs outside of the pool to reach a pooled SGSN on the basis of its NRI.

Once the pooling has been enabled, repeat the command using the **hop-counter** keyword to enable inclusion of the hop-counter IE in SGSN context/identity request messages and to configure the count for the pooling hop-counter. If the SGSN is behaving as the 'default SGSN', this SGSN will forward (relay) requests with the hop-count included to the target SGSN.

**Example**

The following command enables the default pooling functionality which allows an outside SGSN to reach a pooled SGSN:

```
pool default-sgsn
```



The following command sets 25 hops to be included in messages:

```
pool hop-count 25
```

## ran-nas decode proto-type-spare cause-value-length

Configures the spare protocol types for the RAN/NAS IE. The cause value and length for the spare protocol type IE can also be configured.



### Note

- This CLI configuration is supported only for the S2b interface.
- Spare protocol types are supported only for Failed Create Bearer Response/Failed Update Bearer Response messages.

### Product

P-GW

### Privilege

Administrator

### Command Modes

Exec > Global Configuration > Context Configuration > eGTP Service Configuration

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

Entering the above command sequence results in the following prompt:

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

### Syntax Description

```
ran-nas decode proto-type-spare cause-value-length <1 | 2>
```

#### cause-value-length

Specifies the length of cause value to be decoded.

<1 | 2>

The cause length value can be 1 octet or octets. The default value is 2 octets.

### Usage Guidelines

Use this command to specify the spare protocol types for the RAN/NAS IE. If there is a mismatch between length of cause value IE and configured CLI value, the IE is ignored.

#### Example

The following command sets the length of the cause value to be decoded.

```
ran-nas decode proto-type-spare cause-value-length 2
```

## validation-mode

Configures the type of validation to be performed on messages received by this service.

<b>Product</b>	ePDG P-GW SAEGW SGSN
<b>Privilege</b>	Administrator
<b>Command Modes</b>	Exec > Global Configuration > Context Configuration > eGTP Service Configuration <b>configure</b> > <b>context</b> <i>context_name</i> > <b>egtp-service</b> <i>service_name</i> Entering the above command sequence results in the following prompt: <pre>[context_name]host_name(config-egtp-service)#</pre>
<b>Syntax Description</b>	<b>validation-mode { custom1   standard }</b> <b>default validation-mode</b>  <b>default</b> Returns the command to the default setting. Default: <b>standard</b>  <b>{ custom1   standard }</b> <b>custom1</b> : Specifies that the message should be validated based on a vendor-specific set of mandatory elements. <b>standard</b> : Specifies that the message should be validated based on the set of mandatory elements as defined in 3GPP 29.274. This is the default option on an S4-SGSN.
<b>Usage Guidelines</b>	Use this command to specify the type of validation performed on messages received by this service. The information elements contained in messages have mandatory elements and conditional elements. The standard set of elements, as defined by 3GPP 29.274 is checked if this command is set to <b>standard</b> . The <b>custom1</b> setting is for a vendor-specific set of mandatory elements.  <b>Example</b> The following command sets the validation mode for incoming messages to <i>standard</i> : <b>validation-mode standard</b>



## CHAPTER 7

# EDNS Configuration Mode Commands

The EDNS Configuration Mode enables configuring of EDNS fields and format.

### Command Modes

Exec > ACS Configuration > EDNS Configuration

**active-charging service** *service\_name* > **edns**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acs-edns) #
```



### Important

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



### Important

Commands under this mode are license controlled. Contact your Cisco account representative for detailed information on specific licensing requirements.

- [end](#), on page 69
- [exit](#), on page 70
- [fields](#), on page 70
- [format](#), on page 71
- [security-profile](#), on page 72

## end

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

### Product

All

### Privilege

Security Administrator, Administrator

### Syntax Description

**end**

### Usage Guidelines

Use this command to return to the Exec mode.

## exit

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

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator

---

**Syntax Description**

**exit**

---

**Usage Guidelines**

Use this command to return to the parent configuration mode.

## fields

This command allows you to enable or disable EDNS Fields Configuration Mode.

---

**Product**

P-GW  
SAEGW

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > ACS Configuration > EDNS Configuration

**active-charging service** *service\_name* > **edns**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acs-edns)#
```

---

**Syntax Description**

**fields** *fields\_name*  
**no edns-fields**

**no**

If previously configured, deletes the specified EDNS Fields mode from the EDNS mode.

**edns-fields**

Defines EDNS fields tag value and enters the edns-fields mode.

---

**Usage Guidelines**

Use this command to configure EDNS fields.

On entering this command, the CLI prompt changes to:

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

Also see the *EDNS Fields Configuration Mode Commands* chapter.

---

**Example**

The following command enables EDNS Fields Configuration Mode:

**edns-fields**

The following command disables EDNS Fields Configuration Mode:

```
no edns-fields
```

## format

This command allows you to enable or disable EDNS Format Configuration Mode.

---

**Product**

P-GW  
SAEGW

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > ACS Configuration > EDNS Configuration

**active-charging service** *service\_name* > **edns**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acs-edns)#
```

---

**Syntax Description**

**format** *format\_name*  
**no format** *format\_name*

**no**

If previously configured, deletes the specified EDNS Format mode from the EDNS mode.

**edns-format**

Enables EDNS format configuration.

**format\_name**

Defines the name of EDNS field or EDNS format.

---

**Usage Guidelines**

Use this command to configure EDNS fields.

On entering this command, the CLI prompt changes to:

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

Also see the *EDNS Format Configuration Mode Commands* chapter.

**Example**

The following command enables EDNS Format Configuration Mode:

```
edns-format f1
```

The following command disables EDNS Format Configuration Mode:

```
no edns-format f1
```

# security-profile

This CLI command allows you to configure the security profile in EDNS to add mapping with the device-id.

---

## Product

P-GW  
SAEGW

---

## Privilege

Security Administrator, Administrator

---

## Command Modes

Exec > ACS Configuration > EDNS Configuration

**active-charging service** *service\_name* > **edns**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acs-edns)#
```

---

## Syntax Description

**security-profile** *security\_profile\_name*  
**no security-profile** *security\_profile\_name*

**no**

If added previously, removes the security-profile configuration.

**security-profile**

Defines the security profile configuration in the EDNS to add mapping with the device-id.

***security\_profile\_name***

Defines the name of the security profile. This is a string of size 1 to 50.

**device-id**

Defines the device-id to map to an EDNS profile.

***device\_id\_name***

Defines the device id name. This is a string of size 1 to 50.

---

## Usage Guidelines

Use this CLI command to configure the security profile in EDNS to add mapping with the device-id.

### Example

The following is an example of this command:

```
security-profile s1
```



## CHAPTER 8

# EDNS Fields Configuration Mode Commands

The EDNS Fields Configuration Mode enables configuring EDNS Fields tag value.

### Command Modes

Exec > ACS Configuration > EDNS > EDNS Fields Configuration

**active-charging service** *service\_name* > **edns** > **fields** *fields\_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acs-edns-fields)#
```



### Important

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



### Important

Commands under this mode are license controlled. Contact your Cisco account representative for detailed information on specific licensing requirements.

- [end, on page 73](#)
- [exit, on page 74](#)
- [tag, on page 74](#)

## end

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

### Product

All

### Privilege

Security Administrator, Administrator

### Syntax Description

**end**

### Usage Guidelines

Use this command to return to the Exec mode.

## exit

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

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator

---

**Syntax Description**

**exit**

---

**Usage Guidelines**

Use this command to return to the parent configuration mode.

## tag

This command allows you to configure a comma or a tab as a delimiter character for EDRs.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > ACS Configuration > EDNS > EDNS Fields Configuration

**active-charging service** *service\_name* > **edns** > **edns-fields** *fields\_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acs-edns)#
```

---

**Syntax Description**

```
tag { val { imsi | msisdn | pgw-address | apn-name } { encrypt } } |
default device-id }
no tag
```

---

**no**

Removes the tag value for EDNS fields.

---

**tag**

Defines tag value for EDNS fields

---

**val**

Defines tag value for EDNS fields. This is an integer value between 1 and 65535. Tag value will be of 2 bytes.

---

**imsi**

Defines the imsi of the subscriber.

---

**msisdn**

Defines the msisdn of the subscriber.



**pgw-address**

Defines the address of the node.

**default**

Defines the standard opt-code value.

**apn-name**

Defines the access point name of the subscriber connected to.

**device-id**

Defines device-id learned during registration.

**encrypt**

Encrypts the subscriber traffic. This option is available for imsi and msisdn only.



---

**Important**

If encoding of any of the fields fails, EDNs insert will not happen.

---

---

**Usage Guidelines**

Use this command to configure tag values of EDNS Fields.

**Example**

The following example defines tag value:

```
tag val imsi encrypt default device-id
```





## CHAPTER 9

# EDNS Format Configuration Mode Commands

The EDR Format Configuration Mode enables configuring EDNS formats and associating fields with formats.

### Command Modes

Exec > ACS Configuration > EDNS > EDNS Format Configuration

**active-charging service** *service\_name* **edns> edns-format** *format\_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acs-edns-format) #
```



### Important

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



### Important

Commands under this mode are license controlled. Contact your Cisco account representative for detailed information on specific licensing requirements.

- [end, on page 77](#)
- [exit, on page 78](#)
- [fields, on page 78](#)

## end

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

### Product

All

### Privilege

Security Administrator, Administrator

### Syntax Description

**end**

### Usage Guidelines

Use this command to return to the Exec mode.

## exit

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

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator

---

**Syntax Description**

**exit**

---

**Usage Guidelines**

Use this command to return to the parent configuration mode.

## fields

This command allows you to configure EDNS Format mode commands.

---

**Product**

P-GW  
SAEGW

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > ACS Configuration > EDNS > EDNS Format Configuration  
**active-charging service** *service\_name* **edns** > **edns-format** *format\_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acs-edns-format)#
```

---

**Syntax Description**

**fields** *fields\_name* **encode**  
**no fields**

**no**

Removes the fields values.

**fields**

Inserts EDNS fields.

**fields\_name**

Specifies fields name.

**encode**

Defines fields to be used for encoding EDNS message.

---

**Usage Guidelines**

Use this command to configure fields value.

**Example**

The following example specifies fields in EDNS format mode:

```
fields f1 encode
```





## CHAPTER 10

# EIR Profile Configuration Mode Commands

The EIR is used for authentication and authorization of a subscriber's equipment during an Attach. The EIR database includes information about the subscriber's equipment (UE), such as the International Mobile Equipment Identity (IMEI) and the UE manufacturer's software version number (SV) which is usually paired with the IMEI. The IMEI(SV) can be in one of three lists in the EIR:

- white list - the subscriber equipment is permitted access
- black list - the subscriber equipment is not permitted access
- grey list - the subscriber equipment is being tracked for evaluation or other purposes

To view the configured values of the EIR profile, use the Exec mode **show sgsn-mode** command.

To associate the EIR profile with call control profile, see the call control profile mode's **eir-profile** command.

### Command Modes

The EIR Profile configuration mode provides the commands to define Equipment Identify Register (EIR) parameters that can be used by the SGSN on a global level. The SGSN supports a total of 16 instances of the EIR profile.

Exec > Global Configuration > SGSN Global Configuration > EIR Profile Configuration

**configure > sgsn-global > eir-profile** *eir\_profile\_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-eir-profile-eir_profile_name)#
```



### Important

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

- [check-imei-every-n-events](#), on page 82
- [end](#), on page 82
- [eir-address](#), on page 83
- [exit](#), on page 84
- [include-imsi](#), on page 84
- [map-include-imsi](#), on page 84

## check-imei-every-n-events

This command performs IMEI check for every N events.

---

**Product**

SGSN

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration > EIR Profile Configuration

**configure** > **sgsn-global** > **eir-profile** *eir\_profile\_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-eir-profile-eir_profile_name)#
```

---

**Syntax Description**

**check-imei-every-n-events** *check\_frequency*  
**no check-imei-every-n-events**

**no**

Removes the IMEI check definition from the EIR profile configuration.

***check\_frequency***

The frequency must be an integer from 1 to 15.

When a value is configured, the SGSN skips sending the 'check IMEI' message for the first N-1 event where IMDI/IMEISV is received.

---

**Usage Guidelines**

Use this command to perform IMEI check for every N events. If a value is not defined, then by default, the SGSN sends a 'check IMEI' message for every event.

**Example**

The following command removes the check frequency configuration from the EIR profile:

```
no check-imei-every-n-events
```

## end

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

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator

---

**Syntax Description**

**end**

---

**Usage Guidelines**

Use this command to return to the Exec mode.



# eir-address

This command configures the address of the equipment identify register (EIR).

---

**Product**

SGSN

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > Global Configuration > SGSN Global Configuration > EIR Profile Configuration

**configure** > **sgsn-global** > **eir-profile** *eir\_profile\_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-eir-profile-eir_profile_name)#
```

---

**Syntax Description**

```
eir-address { isdn isdn_address | point-code point_code } [ source-ssn source_ssn ]
no eir-address
```

**no**

Removes the EIR address from this EIR profile.

**isdn** *isdn\_address*

Configures a standard ISDN E.164 address to identify the EIR. *isdn\_address* is an integer from 0 to 9.

**point-code** *point\_code*

Configures a standard SS7 formatted point-code address to identify the EIR. *point\_code* must be in dotted-decimal or decimal format. Format options include:

- 0.0.1 to 7.255.7 for point-code in the ITU range.
- 0.0.1 to 255.255.255 for point-code in the ANSI range.
- 0.0.1 to 15.31.255 for point-code in the TTC Range.
- A string of 1 to 11 digits in dotted-decimal to represent a point-code in a different range.

**source-ssn** *source\_ssn*

Configures the source SSN value to be used, to define the subsystem number of the element being identified. *source\_ssn* is an integer from 1 to 255. The default value is 149 (SGSN).

---

**Usage Guidelines**

Use this command to define a single EIR address to be used for multiple EIRs when this EIR profile is associated with a call control profile.

**Example**

The following command configures the point-code 255.255.255 with source SSN value 250 for the EIR address :

```
eir-address point-code 255.255.255 source-ssn 250
```

## exit

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

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Syntax Description</b>	<b>exit</b>
<b>Usage Guidelines</b>	Use this command to return to the parent configuration mode.

## include-imsi

This command enables inclusion of IMSI in the TCAP message.

<b>Product</b>	SGSN
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > Global Configuration > SGSN Global Configuration > EIR Profile Configuration <b>configure &gt; sgsn-global &gt; eir-profile</b> <i>eir_profile_name</i> Entering the above command sequence results in the following prompt: <code>[context_name]host_name(config-eir-profile-eir_profile_name)#</code>
<b>Syntax Description</b>	<b>[ no ] include-imsi</b>  <b>no</b> Disables inclusion of IMSI in the TCAP message.
<b>Usage Guidelines</b>	Use this command to enable or disable the inclusion of IMSI in the TCAP message for IMSI checking during the IMEI check operation. By default, IMSI checking is not included.

## map-include-imsi

This command enables adding IMSI in the MAP message.

<b>Product</b>	SGSN
<b>Privilege</b>	privilege
<b>Command Modes</b>	Exec > Global Configuration > SGSN Global Configuration > EIR Profile Configuration <b>configure &gt; sgsn-global &gt; eir-profile</b> <i>eir_profile_name</i> Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-eir-profile-eir_profile_name)#
```

---

**Syntax Description**

[ no ] **map-include-imsi**

**no**

Disables inclusion of IMSI in the MAP message.

---

**Usage Guidelines**

Use this command to enable or disable inclusion of IMSI checking during the check IMEI procedure. By default, IMSI checking is not part of the IMEI check procedure.

map-include-imsi



# CHAPTER 11

## eNB Group Configuration Mode Commands

---

### Command Modes

Creates Global eNB and enters eNB Group configuration mode.

Exec > Global Configuration > LTE Policy > eNB Group Service Configuration

**configure** > **lte-policy** > **enb-group** *enb\_group\_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(enb-group) #
```

- [end, on page 87](#)
- [exit, on page 87](#)
- [global-enb-id, on page 88](#)
- [relative-mme-capacity, on page 88](#)

## end

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

---

### Product

All

---

### Privilege

Security Administrator, Administrator

---

### Syntax Description

**end**

---

### Usage Guidelines

Use this command to return to the Exec mode.

## exit

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

---

### Product

All

---

### Privilege

Security Administrator, Administrator

---

### Syntax Description

**exit**

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

## global-enb-id

Global eNB ID.

**Product** MME

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > LTE Policy Configuration > eNB Group  
**configure > lte-policy > enb-group**

Entering the above command sequence results in the following prompt:

```
[local]host_name(enb-group)#
```

**Syntax Description** **global-enb-id enbid-list** *enbid\_list\_name* | **prefix** *network\_identifier\_name* **bits**  
*bits*

**global-enb-id prefix** *network\_identifier\_name* **bits** *bits*

Global eNB ID prefix contains bit string which should be matched with Hexadecimal value.  
*network\_identifier\_name* Must Hexadecimal number between 0x0 and 0xFFFFFFFF

**enbid-list** *enbid\_list\_name*

Specifies eNB ID list with discrete eNB IDs. *enbid\_list\_name* must be a string of size string of size 1 to 64.

**Usage Guidelines** Use this command to create group of eNBs based on eNB ID "prefix" to match with 'bits' of eNBs.

### Example

The following command to create group of eNBs based on eNB ID "prefix" to match with 'bits' of eNBs.

```
global-enb-id prefix network_identifier_name bits bits
```

## relative-mme-capacity

Relative MME Capacity which should be sent to eNB group.

.

**Product** MME

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > LTE Policy Configuration > eNB Group

**configure > lte-policy > enb-group**

Entering the above command sequence results in the following prompt:

```
[local]host_name(enb-group)#
```

---

**Syntax Description**

**relative-mme-capacity** *relative\_mme\_capacity*

**relative-mme-capacity** *relative\_mme\_capacity*

Relative MME capacity in S1 setup response for eNB which matches grouping criteria.

*relative\_mme\_capacity* Must be an Integer from 1 to 255.

---

**Usage Guidelines**

Use this command to configure relative MME Capacity which be sent to eNB group.

**Example**

The following command to configure relative MME Capacity which be sent to eNB group.

**relative-mme-capacity** *relative\_mme\_capacity*







## CHAPTER 12

# eNBID List Configuration Mode Commands

---

### Command Modes

Creates Global eNB and enters eNB Group configuration mode.

Exec > Global Configuration > LTE Policy > eNB Group Service Configuration

**configure > lte-policy > enbid-list** *enbid\_list\_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(enbid-list)#
```

- [end, on page 91](#)
- [exit, on page 91](#)
- [enbid, on page 92](#)
- [enb-id-range, on page 92](#)

## end

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

---

### Product

All

---

### Privilege

Security Administrator, Administrator

---

### Syntax Description

**end**

---

### Usage Guidelines

Use this command to return to the Exec mode.

## exit

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

---

### Product

All

---

### Privilege

Security Administrator, Administrator

---

### Syntax Description

**exit**

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

## enbid

the discrete eNB IDs

.

**Product** MME

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > LTE Policy Configuration > eNBID List  
**configure > lte-policy > enbid-list**

Entering the above command sequence results in the following prompt:

```
[local]host_name(enbid-list)#
```

**Syntax Description** [ **no** ] **enb-id** *discrete\_eNB\_id*

**no**

Disables the configuration of discrete eNB IDs.

**enb-id** *discrete\_eNB\_id*

Specifies the discrete eNB IDs. *discrete\_eNB\_id* must be a Hexadecimal number between 0x1 and 0xFFFFFFFF.

## enb-id-range

Range of discrete eNB IDs.

.

**Product** MME

**Privilege** Administrator

**Command Modes** Exec > Global Configuration > LTE Policy Configuration > eNBID List  
**configure > lte-policy > enbid-list**

Entering the above command sequence results in the following prompt:

```
[local]host_name(enbid-list)#
```

**Syntax Description** [ **no** ] **enb-id-range from** *starting\_eNB\_id* **to** *ending\_eNB\_id*

**no**

Disables the configuration of discrete eNB IDs.

**enb-id-range**

Specifies the range of discrete eNB IDs.

**from *starting\_eNB\_id***

Specifies the starting eNB ID in the range in Hexadecimal. *starting\_eNB\_id* must be a Hexadecimal number between 0x1 and 0xFFFFFFFF.

**to *ending\_eNB\_id***

Specifies the last eNB ID in the range in Hexadecimal. *ending\_eNB\_id* must be a Hexadecimal number between 0x1 and 0xFFFFFFFF.

enb-id-range



# CHAPTER 13

## EPDG Service Configuration Mode Commands

### Command Modes

Creates Evolved Packet Data GateWay service and enters EPDG service configuration mode.

Exec > Global Configuration > Context > EPDG Service Configuration

**configure** > **context** *context\_name* > **epdg service** *service\_name*

Entering the above command sequence results in the following prompt:

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

- [aaa](#), on page 96
- [allow](#), on page 96
- [associate](#), on page 97
- [bind](#), on page 98
- [data-buffering](#), on page 99
- [dns-pgw](#), on page 99
- [end](#), on page 100
- [exit](#), on page 101
- [fqdn](#), on page 101
- [interworking-5g](#), on page 102
- [ip](#), on page 102
- [max-sessions](#), on page 103
- [mobile-access-gateway](#), on page 104
- [newcall](#), on page 105
- [pdn-type](#), on page 106
- [pgw-selection](#), on page 106
- [plmn](#), on page 108
- [reporting-action](#), on page 109
- [setup-timeout](#), on page 109
- [subscriber](#), on page 110
- [threshold](#), on page 111
- [timeout idle](#), on page 112
- [username](#), on page 113
- [vendor-specific-attr](#), on page 114

## aaa

This command configures AAA parameters for ePDG service.

---

**Product**

ePDG

---

**Privilege**

Security Administrator, Administrator

---

**Syntax Description**

```
aaa send framed-mtu value
aaa send framed-mtu
```

**no**

Disables AAA parameters for ePDG service.

**send**

Configures AVP to be send to AAA server.

**framed-mtu *value***

This is the framed-MTU AVP value to be sent in DER, which is an integer from 64 through 1500.

---

**Usage Guidelines**

Use this command to configure AAA parameters for ePDG service.

**Example**

The following command configures framed-MTU AVP value 100 to be send to AAA server for ePDG service.

```
aaa send framed-mtu 100
```

## allow

This command allows duplicate precedence in a TFT for a S2b ePDG session.

---

**Product**

ePDG

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > Global Configuration > Context > EPDG Service Configuration

```
configure > context context_name > epdg service service_name
```

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description**

```
[ no ] allow { custom-swm-swu-error-mapping | duplicate-prec-in-tft }
```

**no**

Disables allowing exception.

**custom-swm-swu-error-mapping**

Customises mapping of SWm errors with SWu Notify Error Type.

**duplicate-prec-in-tft**

The duplicate precedence is allowed in a tft for a S2b ePDG session.

**Usage Guidelines**

Use this command to allow exception with Spec or RFC.

**Example**

The following command is used to allow duplicate precedence in a tft for a S2b ePDG session.

```
allow duplicate-prec-in-tft
```

# associate

This command associates configuration of ePDG service to qci-qos mapping and EGTP service.

**Product**

ePDG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context > EPDG Service Configuration

```
configure > context context_name > epdg service service_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
associate { egtp-service egtp_service_name | gtpc-load-control-profile
gtpc_load_control_profile_name | gtpc-overload-control-profile
gtpc_overload_control_profile_name | qci-qos-mapping qci_qos_mapping |
subscriber-map subscriber_map_name }
no associate { egtp-service | gtpc-load-control-profile
gtpc_load_control_profile_name | gtpc-overload-control-profile
gtpc_overload_control_profile_name | qci-qos-mapping | subscriber-map }
```

**no**

Disables association.

**egtp-service egtp\_service\_name**

The eGTP service should be configured before associating the same with ePDG service.

*egtp\_service\_name* is a string and the value must be between 1 and 63.

**gtpc-load-control-profile** *gtpc\_load\_control\_profile\_name*

Associates GTPC-load-control-profile for the epdg service.

*1* and *64*.

**gtpc-overload-control-profile** *gtpc\_overload\_control\_profile\_name*

Associates GTPC-overload-control-profile for the ePDG service.

*1* and *64*.

**qci-qos-mapping** *qci\_qos\_mapping*

The associated qci-qos mapping table should be configured prior to associating the same with ePDG service.

*qci-qos\_mapping* is a string and the value must be between *1* and *63*.

**subscriber-map** *subscriber\_map\_name*

Configures subscriber map association to get PGW address locally.

*subscriber\_map\_name* is a string and the size must be between *1* and *64*.

**Usage Guidelines**

Use this command to associate the ePDG service to egtp service or QCI to QoS mapping.

**Example**

The following command removes the association of epdg service to egtp service.

```
no associate egtp-service
```

# bind

This command binds the services.

**Product**

ePDG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context > EPDG Service Configuration

```
configure > context context_name > epdg service service_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
bind address bind_address crypto-template crypto_template_service_name
no bind address
```

**no**

Disables binding.



**address *bind\_address***

Specifies the address of the EPDG service. This must be followed by an IPv4 address, using dotted-decimal notation or an IPv6 address, using xx::yy::zz format.

**crypto-template *crypto\_template\_service\_name***

Specifies the crypto template to use, this is a string of size between 0 and 127.

**Usage Guidelines**

Use this command to bind the ePDG service.

**Example**

The following command binds the ePDG Service to the IPv4 address 12.32.44.56.

```
bind address 12.32.44.56
```

## data-buffering

This command allows to downlink packets to be buffered, while session is in connecting state. By default it is enabled.

**Product**

ePDG

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
[ no | default ] data-buffering
```

**no**

Disables data buffering.

**default**

Sets / restores the data buffering to its default value. By default, the data buffering is enabled.

**Usage Guidelines**

Use this command to allow to downlink packets to be buffered, while session is in connecting state.

**Example**

The following command allows to set the default value of the data-buffering.

```
default data-buffering
```

## dns-pgw

Configures context of dns-client.

**Product**

ePDG

end

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec &gt; Global Configuration &gt; Context &gt; EPDG Service Configuration

**configure > context** *context\_name* > **epdg service** *service\_name*

Entering the above command sequence results in the following prompt:

*[context\_name]*host\_name(config-epdg-service)#**Syntax Description**

```
dns-pgw { context dns_client_context_name | selection { topology [ weight ] | weight } }
{ no | default } dns-pgw { context | selection { topology [ weight ] | weight } }
```

**default**

Configures context of dns-client to its default value.

**no**

Disables dns-client's context.

**context** *dns\_client\_context\_name*

Specifies the dns-client's context name, which is a string and should be between 1 and 79.

**selection** { **topology** [ **weight** ] | **weight** }

Specifies the pgw dns selection criteria.

**topology**: Enables topology selection.**topology weight**: Enables topology with weight.**weight**: Enables selection with weight-only, disables topology selection.**Usage Guidelines**

Enable/disable PGW Selection based on topology and load-balancing of PGWs on weight's from DNS.

Use this command to configure the source in which dns-client is configured, dns-pgw selection topology/weight will be used to enable/disable PGW Selection based on topology and load-balancing of PGWs.

**Example**

Use the following command to configure dns-client context.

**dns-pgw context** 21**end**

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

**Product**

All

<b>Privilege</b>	Security Administrator, Administrator
<b>Syntax Description</b>	<b>end</b>
<b>Usage Guidelines</b>	Use this command to return to the Exec mode.

## exit

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

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Syntax Description</b>	<b>exit</b>
<b>Usage Guidelines</b>	Use this command to return to the parent configuration mode.

## fqdn

Designates ePDG fully qualified domain name.

<b>Product</b>	ePDG
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > Global Configuration > Context > ePDG Service Configuration <b>configure &gt; context</b> <i>context_name</i> > <b>epdg service</b> <i>service_name</i> Entering the above command sequence results in the following prompt: <i>[context_name]host_name(config-epdg-service)#</i>

<b>Syntax Description</b>	<b>fqdn</b> <i>epdg_fqdn</i> <b>{ no   default } fqdn</b>
---------------------------	--

### default

Resets the ePDG fully qualified domain name to its default setting.

### no

Disables ePDG FQDN.

### fqdn *epdg\_fqdn*

Designates ePDG with fully qualified domain name, name is a string between 1 and 256 alphanumeric characters.

**Usage Guidelines**

Use this command to configure ePDG FQDN under ePDG service which will be used for longest suffix match during dynamic allocation.

**Example**

Use the following command to disable ePDG FQDN:

```
no fqdn
```

## interworking-5g

Configures the 5G interworking on ePDG service.

**Product**

ePDG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context > EPDG Service Configuration

```
configure > context context_name > epdg service service_name
```

Entering the previous command sequence results in the following prompt:

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

**Syntax**

```
[ no ] interworking-5g
```

**no**

If disabled, all calls are treated as 4G for the ePDG service.

**interworking-5g**

Enabling the **interworking-5g** enables the 5G interworking for the ePDG service.

**Usage Guidelines**

The 5G Interworking configuration is available only if the ePDG 5G license is configured. If the ePDG license is not present, or the interworking-5g configuration is not enabled, by default the ePDG selects the P-GW as per the legacy behavior.

**Example**

Use the following configuration to enable or disable the 5G interworking on ePDG:

```
[ no ] interworking-5g
```

## ip

This command configures Internet Protocol (IP) parameters.

---

**Product** ePDG

---

**Privilege** Security Administrator, Administrator

---

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

**configure > context** *context\_name* > **epdg service** *service\_name*

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description**

```
ip fragment-chain { max-ooo-fragment fragments | timeout secs }
default ip fragment-chain { max-ooo-fragment | timeout }
```

**default**

Resets the ePDG Internet Protocol(IP) parameters to default values.

**fragment-chain**

This option configures ip fragment chain settings during TFT handling.

**max-ooo-fragment** *fragments*

This is the number of fragments to buffer per fragment chain for out-of-order reception before receiving first fragment(for L4 packet filtering).

*fragments* is an integer value from 0 through 300.

The default value is 45.

0 represents no buffering is done for out-of-order fragments, correct bearer will be selected with first fragment.

**timeout** *secs*

This is the time to hold an ip fragment chain.

*secs* is an integer value from 1 through 10.

The default value is 5.

---

**Usage Guidelines**

Use this command to configure ePDG Internet Protocol (IP) parameters.

**Example**

Use the following command to configure ePDG IP parameter timeout to 6 seconds:

```
ip fragment-chain timeout 6
```

## max-sessions

This command configures the approximate maximum number of sessions ePDG service can support, ranging from 0 to 1000000. Default is 1000000.

---

**Product** ePDG

---

**Privilege** Security Administrator, Administrator

---

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

**configure > context** *context\_name* > **epdg service** *service\_name*

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description** **max-sessions** *value*  
**default max-sessions**

#### **default**

Resets the approximate maximum number of sessions that ePDG service can support to default value (1000000).

#### **value**

This is the approximate maximum number of sessions that ePDG service can support, ranging from 0 to 1000000.

The default value is 1000000.

---

**Usage Guidelines** Use this command to configure the approximate maximum number of sessions that ePDG service can support.

#### **Example**

Use the following command to configure the approximate maximum number of sessions that ePDG service can support to 10.

```
max-sessions 10
```

## mobile-access-gateway

Configures MAG context within epdg service.

---

**Product** ePDG

---

**Privilege** Security Administrator, Administrator

---

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

**configure > context** *context\_name* > **epdg service** *service\_name*

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description** **mobile-access-gateway context** *context\_name* [ **mag-service** *mag\_service\_name* ]  
**no mobile-access-gateway context**

**no**

Disables MAG context.

**mobile-access-gateway context *context\_name* [ mag-service *mag\_service\_name* ]**

**context** designates the name of the context in which the MAG service is configured. This must be followed by *context\_name* of MAG service of size 1 to 79 characters.

**mag-service** designates the name of the MAG service. This must be followed by *mag\_service\_name* of size 1 to 63 characters.

**Usage Guidelines**

Use this command to specify where MIPv6 sessions are routed through this service.

**Example**

Use the following command to configure MAG context with context name fg.

```
mobile-access-gateway context fg
```

# newcall

Configures new call related behavior.

**Product**

ePDG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context > EPDG Service Configuration

```
configure > context context_name > epdg service service_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no | default ] newcall duplicate-session notify-delete name
```

**no**

Disables new call related behavior.

**default**

Sets the default value for the new call related behavior. 'notify-delete' is enabled by default.

**duplicate-session**

Configures action regarding duplicate session.

**notify-delete**

Initiate delete session request to PGW during reattach if another PGW is selected. Enabled by default.

**Usage Guidelines** Use this command to configure new call related behavior.

### Example

The following example configures new call related behavior:

```
newcall duplicate-session notify-delete
```

## pdn-type

This command configures pdn-type related parameters for ePDG service.

**Product** ePDG

**Privilege** Security Administrator, Administrator

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

```
configure > context context_name > epdg service service_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description** [ no ] **pdn-type ipv6 path-mtu**

**no**

Disables pdn-type related parameters for ePDG service.

**Usage Guidelines** Use this command to configure pdn-type related parameters for ePDG service.

### Example

Use the following command to disable pdn-type related parameters for ePDG service.

```
no pdn-type ipv6 path-mtu
```

## pgw-selection

Configures pgw-selection related parameters for the ePDG service.

**Product** ePDG

**Privilege** Security Administrator, Administrator

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

```
configure > context context_name > epdg service service_name
```

Entering the above command sequence results in the following prompt:



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

---

**Syntax Description**

```
[ no ] pgw-selection select pgw 4gonly-ue no-5gs-interworking
smf-not-configured { agent-info error-terminate |
local-configuration-preferred | prefer aaa-pgw-id }
```

**no**

Disables pgw-selection related parameters for the ePDG service.

**4gonly-ue**

If the P-GW is enabled for 4G only UE, ePDG selects the P-GW by overriding the default SMF selection.

**no-5gs-interworking**

If the P-GW is enabled for 5Gs interworking not subscribed cases, ePDG selects the P-GW and overrides the default SMF+PGW-IWK selection.

**smf-not-configured**

Enabling the **pgw smf-not-configured** option overrides the **4gonly-ue** and **no-5gs-interworking** options.

**pgw-selection agent-info error-terminate**

**agent-info** specifies the action to be taken when MIP6-agent-info is expected but not received from AAA/HSS.

**error-terminate** terminates the pgw-selection and rejects the call.

**local-configuration-preferred**

Configures local PGW selection as the preferred mechanism. Applicable for initial attach. Default is AAA/DNS based selection.

**prefer aaa-pgw-id**

Configures AAA provided PGW ID(IP address/FQDN) selection as the preferred mechanism for initial attach.

---

**Usage Guidelines**

Use this command to terminate the pgw-selection and reject the call when MIP6-agent-info is expected but not received from AAA/HSS.

The ePDG selects SMF+PGW-IWK as per the default behavior. This default behavior is customized using one of the previous configuration commands under ePDG-service mode to choose P-GW.

All the previous three commands are configurable only when ePDG 5G license is present and **interworking-5g** is enabled.

**Example**

Use the following command to terminate pgw-selection and reject the call.

```
pgw-selection agent-info error-terminate
```

**Example**

Use the following configurations to enable or disable P-GW selection for 4G-only UE, SMF+PGW-IWK, or ignore the SMF selection to select the P-GW:

```
pgw-selection select pgw no-5gs-interworking 4gonly-ue smf-not-configured
```

# plmn

Configures PLMN related parameters for the EPDG service.

**Product**

ePDG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context > EPDG Service Configuration

```
configure > context context_name > epdg service service_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
plmn id mcc mcc_plmn_id mnc mnc_plmn_id  
no plmn id
```

**no**

Disables PLMN related parameters for the EPDG service.

```
plmn id mcc mcc_plmn_id mnc mnc_plmn_id
```

**plmn id mcc** *mcc\_plmn\_id* configures MCC part of PLMN ID for the EPDG service and prompts as " Enter a number, ranging from 200...999 - string of size 3 to 3" . *mcc\_plmn\_id* is a string of three characters, entered as number between 200 and 999.

**mnc** *mnc\_plmn\_id* configures MNC part of PLMN ID for the EPDG service and prompts as " Enter a number, ranging from 00...999 - string of size 2 to 3" . *mnc\_plmn\_id* is a string of two to three characters, entered as number between 00 and 999.

**Usage Guidelines**

Use this command to configure PLMN identifier (MCC and MNC Values) for ePDG Service.

**Example**

Use the following command to configure PLMN identifier MCC 456 and MNC 64 for ePDG service.

```
plmn id mcc 456 mnc 64
```

## reporting-action

Configures reporting of events.

---

**Product** ePDG

---

**Privilege** Security Administrator, Administrator

---

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

**configure** > **context** *context\_name* > **epdg-service** *epdg\_service\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-epdg-service)#
```

---

**Syntax Description** [ no ] **reporting-action event-record**

**no**

Disables RTT record generation for this ePDG service.

**event-record**

Configures event records.

---

**Syntax Description** Use this command to configure the reporting of events for the ePDG service.

### Example

The following command configures the reporting of event records:

```
reporting-action event-record
```

## setup-timeout

Maximum time allowed for session setup in seconds.

---

**Product** ePDG

---

**Privilege** Security Administrator, Administrator

---

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

**configure** > **context** *context\_name* > **epdg service** *service\_name*

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description** **setup-timeout** *time*  
**default setup-timeout**

**default**

Sets up the maximum time allowed for a session to default value (as 60 seconds).

**setup-timeout *time***

*time* is an integer value between 2 and 300.

**Usage Guidelines**

Use this command to configure maximum time allowed for session setup in seconds.

**Example**

Use the following command to configure maximum session time as *120* seconds:

```
setup-timeout 120
```

# subscriber

Configures a subscriber with a given name.

**Product**

ePDG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context > EPDG Service Configuration

```
configure > context context_name > epdg service service_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ default ] subscriber name
no subscriber
```

**default**

Configures a subscriber with a given default name.

**no**

Cancels the subscriber configuration.

**subscriber *name***

Configures a subscriber with a given name, which is a string of size between 1 and 127.

**Usage Guidelines**

Use this command to configure the subscriber with a given name.

**Example**

Use the following command to configure the subscriber as *sss*.

**subscriber** *sss*

## threshold

This command is used to configure threshold values to set and clear the alarms for each monitoring parameters separately.

---

### Product

ePDG

---

### Privilege

Security Administrator, Administrator

---

### Command Modes

Exec > Global Configuration > Context > EPDG Service Configuration

**configure** > **context** *context\_name* > **epdg service** *service\_name*

Entering the above command sequence results in the following prompt:

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

---

### Syntax Description

```
threshold { epdg-ikev2-authentication-failures | epdg-ikev2-setup-attempts
| epdg-ikev2-setup-failure | epdg-ikev2-setup-failure-rate |
epdg-ikev2-setup-success } threshold_value [ clear clear_value ]
no threshold { epdg-ikev2-authentication-failures |
epdg-ikev2-setup-attempts | epdg-ikev2-setup-failure |
epdg-ikev2-setup-failure-rate | epdg-ikev2-setup-success }
```

**no**

Disables the configuration of a specific threshold for ePDG service.

**epdg-ikev2-authentication-failures** *threshold\_value*

Configures the threshold value for IKEv2 Authentication Failures.

*threshold\_value* is the threshold value for IKEv2 Authentication Failures, which is an integer between 0 and 1000000.

**epdg-ikev2-setup-attempts** *threshold\_value*

Configures the threshold value for IKEv2 Setup Attempts.

*threshold\_value* is the threshold value for IKEv2 Setup Attempts, which is an integer between 0 and 10000000.

**epdg-ikev2-setup-failure** *threshold\_value*

Configures the threshold value for IKEv2 Setup Failure.

*threshold\_value* is the threshold value for IKEv2 Setup Failure, which is an integer between 0 and 1000000.

**epdg-ikev2-setup-failure-rate** *threshold\_value*

Configures the threshold value for IKEv2 Setup Failure Rate.

*threshold\_value* is the percentage of IKEv2 Setup Failure Rate, which is an integer between 0 and 100.

**epdg-ikev2-setup-success *threshold\_value***

Configures the threshold value for IKEv2 Setup Success.

*threshold\_value* is the threshold value for IKEv2 Setup Success, which is an integer between 0 and 10000000.

**clear *clear\_value***

Configures the alarm clear threshold for the following.

- IKEv2 Authentication Failures. *clear\_value* is the number of IKEv2 Authentication Failures, which is an integer between 0 and 1000000.
- IKEv2 Setup Attempts. *clear\_value* is the number of IKEv2 Setup Attempts, which is an integer between 0 and 10000000.
- IKEv2 Setup Failure. *clear\_value* is the number of IKEv2 Setup Failure, which is an integer between 0 and 1000000.
- IKEv2 Setup Failure Rate. *clear\_value* is the percentage of IKEv2 Setup Failure Rate, which is an integer between 0 and 100.
- IKEv2 Setup Success. *clear\_value* is the number of IKEv2 Setup Success, which is an integer between 0 and 10000000.

**Usage Guidelines**

Use this command to configure a specific threshold for ePDG service.

**Example**

The following command configures ePDG IKEV2 Authentication Failures threshold as 50 for a specific ePDG Service.

```
threshold epdg-ikev2-authentication-failures 50
```

## timeout idle

Configures the subscriber's time-to-live (TTL) settings for the EPDG service.

**Product**

ePDG

**Privilege**

System Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > ePDG Service Configuration

```
configure > context context_name > epdg-service epdg_service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name (config-epdg-service)#
```

**Syntax Description**

```
timeout idle sec { micro-checkpoint-deemed-idle [ dur ] |
micro-checkpoint-periodicity dur }
```

```
no timeout idle
```

```
default timeout idle
```

**no**

Disables idle timeout configuration along with the idle seconds micro-checkpoint duration or deemed idle duration configuration.

**default**

Configures the default value for subscriber's time out settings. The idle timeout default value is 0. The default value of micro-checkpoint-deemed-idle would be 0 seconds and that for micro-checkpoint-periodicity is 10 seconds.

**idlesec**

Designates the maximum duration a session can remain idle, in seconds, before system automatically terminates the session. Must be followed by number of seconds between 0 and 2147483647. Zero indicates function is disabled.

**micro-checkpoint-deemed-idle***dur*

Configures micro-checkpoint duration when UE is deemed idle for this Subscriber. Default is "0" (disabled). *dur* is an integer between 10 and 1000.

**micro-checkpoint-periodicity***dur*

Configures the micro-checkpoint-periodicity for this Subscriber. Default is "10". *dur* is the an integer between 10 and 10000.

**Syntax Description**

Use this command to configure the subscriber's time-to-live (TTL) settings for the EPDG service.

**Example**

The following command configures the idle timeout to *10* and micro-checkpoint-periodicity to *50* for the subscriber:

```
timeout idle 10 micro-checkpoint-periodicity 50
```

## username

Sets the options related to username received from mobile.

**Product**

ePDG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context > EPDG Service Configuration

```
configure > context context_name > epdg service service_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
username { check-mac-address [ failure-handling { continue | terminate
} ] | mac-address-delimiter { NAI-label | colon | colon-or-NAI-label } |
mac-address-stripping }
no username { check-mac-address | mac-address-stripping }
```

**no**

Cancels the options related to username received from mobile.

```
username { check-mac-address [ failure-handling { continue | terminate } ] | mac-address-delimiter { NAI-label
| colon | colon-or-NAI-label } | mac-address-stripping }
```

**check-mac-address** validates Mac address. By default, Mac address is not validated.

**failure-handling { continue | terminate }** : MAC Address validation failure handling configuration.

**continue** ignores failure and continues.

**terminate** terminates session on request failure.

**mac-address-delimiter** is the second delimiter to be used to extract the MAC address from username when first delimiter is '@'.

**NAI-label** NAI-label(.nai) to be used to extract the MAC Address from username as a second delimiter when first delimiter is '@'.

**colon** Colon(:) to be used to extract the MAC Address from username as a second delimiter when first delimiter is '@'.

**colon-or-NAI-label** Either colon(:) or NAI-Label(.nai) to be used to extract the MAC address from username as a second delimiter when first delimiter is '@'. This is the default option.

**mac-address-stripping** strips Mac Address from the username. By default, it is disabled.

**Usage Guidelines**

Use this command to set the options (Validate Mac address / mac-address-delimiter / mac-address-stripping) related to username received from mobile.

**Example**

Use the following command to set the options related to username received from mobile.

```
username check-mac-address failure-handling terminate
```

## vendor-specific-attr

Configures the vendor-specific-attributes values on PMIP based S2b interface.

**Product**

ePDG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context > EPDG Service Configuration

```
configure > context context_name > epdg service service_name
```



Entering the above command sequence results in the following prompt:

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

---

### Syntax Description

```
vendor-specific-attr { dns-server-req { apco | pco } | pcscf-server-req
  { apco | private-extn } }
default vendor-specific-attr { dns-server-req | pcscf-server-req }
```

#### default

Configures vendor-specific-attributes to default the value. Default setting is to use APCO IE for DNS Server Address and PrivateExtension IE for PCSCF Server Address.

#### dns-server-req

Configures the DNS Server Address to be present in PCO/APCO IE.

#### apco

Configures to use APCO IE to carry information over PMIP based S2b.

#### pco

Configures to use PCO IE to carry information over PMIP based S2b.

#### pcscf-server-req

Configures the PCSCF Server Address to be present in APCO/PrivateExtn IE.

#### apco

Configures to use APCO IE to carry information over GTP based S2b.

#### private-extn

Configures to use PrivateExtension IE to carry information over GTP based S2b.

---

### Usage Guidelines

Use this command to configure the vendor-specific-attributes values on PMIP based S2b interface.

#### Example

Use the following command to configure the vendor-specific-attributes values on PMIP based S2b interface to pco.

```
vendor-specific-attr dns-server-req pco
```

■ vendor-specific-attr



## CHAPTER 14

# Ethernet Interface Configuration Mode Commands

### Command Modes

The Ethernet Interface Configuration Mode is used to create and manage Ethernet IP interface parameters within a specified context.

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

**configure** > **context** *context\_name* > **interface** *interface\_name* **broadcast**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth) #
```



### Important

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

- [bfd](#), on page 118
- [crypto-map](#), on page 119
- [description](#), on page 120
- [end](#), on page 121
- [exit](#), on page 121
- [ip access-group](#), on page 121
- [ip address](#), on page 122
- [ip igmp profile](#), on page 123
- [ip mtu](#), on page 123
- [ip ospf authentication-key](#), on page 125
- [ip ospf authentication-type](#), on page 125
- [ip ospf bfd](#), on page 126
- [ip ospf cost](#), on page 127
- [ip ospf dead-interval](#), on page 127
- [ip ospf hello-interval](#), on page 128
- [ip ospf message-digest-key](#), on page 129
- [ip ospf network](#), on page 129
- [ip ospf priority](#), on page 130
- [ip ospf retransmit-interval](#), on page 131

- [ip ospf transmit-delay](#), on page 132
- [ipv6 access-group](#), on page 132
- [ipv6 address](#), on page 133
- [ipv6 ospf](#), on page 134
- [ipv6 router advertisement](#), on page 136
- [logical-port-statistics](#), on page 136
- [mpls ip](#), on page 137
- [policy-forward](#), on page 138
- [pool-share-protocol](#), on page 139
- [port-switch-on-L3-fail](#), on page 140
- [vlan-map](#), on page 141

## bfd

Configures Bidirectional Forwarding Detection (BFD) interface parameters.

---

### Product

All

---

### Privilege

Security Administrator, Administrator

---

### Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

**configure** > **context** *context\_name* > **interface** *interface\_name* **broadcast**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

---

### Syntax Description

```
[no] bfd { echo [echo-interval interval_num] | interval interval_num }
      min_rx milliseconds multiplier value
```

#### no

Disables the specified option on this interface.

#### echo

Enables BFD echo mode.

BFD echo mode works with asynchronous BFD. Echo packets are sent by the forwarding engine and forwarded back along the same path in order to perform detection—the BFD session at the other end does not participate in the actual forwarding of the echo packets. The echo function and the forwarding engine are responsible for the detection process, therefore the number of BFD control packets that are sent out between two BFD neighbors is reduced.

Since the forwarding engine is testing the forwarding path on the remote (neighbor) system without involving the remote system, there is an opportunity to improve the interpacket delay variance, thereby achieving quicker failure detection times than when using BFD Version 0 with BFD control packets for the BFD session.

**echo-interval *interval\_num***

Specifies the transmit interval between BFD echo packets. The default interval is 150 ms. The range is from 0 to 999 ms. (VPC only)

**interval *interval\_num***

Specifies the transmit interval (in milliseconds) between BFD packets.

- For releases prior to 17.0, *interval\_num* is an integer from 50 through 999. (Default 50)
- For release 17.0 onwards, *interval\_num* is an integer from 50 through 10000. (Default 50)

**min\_rx *milliseconds***

Specifies the receive interval in milliseconds for control packets.

- For releases prior to 17.0, *milliseconds* is an integer from 50 through 999. (Default 50)
- For release 17.0 onwards, *milliseconds* is an integer from 50 through 10000. (Default 50)

**multiplier *value***

Specifies the value used to compute the hold-down time as a number from 3 to 50.

**Usage Guidelines**

Specify BFD parameters including echo mode and the transmit interval between BFD packets.

**Example**

To apply enable echo mode on this interface, use the following command:

```
bfd echo
```

The following command sets BFD interval parameters:

```
bfd interval 3000 min_rx 300 multiplier 3
```

## crypto-map

Applies the specified IPsec crypto-map to this interface.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
crypto-map map_name [ secondary-address sec_ip_addr ]  
no crypto-map map_name
```

**no**

Deletes the application of the crypto map on this interface.

## description

**map\_name**

Specifies the name of the crypto map being applied as an alphanumeric string of 1 through 127 characters that is case sensitive.

**secondary-address sec\_ip\_addr**

Applies the crypto map to the secondary address for this interface. *sec\_ip\_addr* must be specified using the IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Usage Guidelines**

In order for ISAKMP and/or manual crypto maps to work, they must be applied to a specific interface using this command. Dynamic crypto maps should **not** be applied to interfaces.

The crypto map must be configured in the same context as the interface.

**Example**

To apply the IPsec crypto map named cmap1 to this interface, use the following command:

```
crypto-map cmap1
```

## description

Sets the descriptive text for the current interface.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
description text
no description
```

**no**

Clears the description for the interface.

**text**

Specifies the descriptive text as an alphanumeric string of 0 through 79 characters.

**Usage Guidelines**

Set the description to provide useful information on the interface's primary function, services, end users, etc. Any information useful may be provided.

**Example**

```
description sampleInterfaceDescriptiveText
```

# end

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

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Syntax Description</b>	<b>end</b>
<b>Usage Guidelines</b>	Use this command to return to the Exec mode.

# exit

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

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Syntax Description</b>	<b>exit</b>
<b>Usage Guidelines</b>	Use this command to return to the parent configuration mode.

# ip access-group

Specifies the name of the Access Control List (ACL) group to assign to the interface.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Syntax Description</b>	<b>[ no ] ip access-group</b> <i>group_name</i> { <b>in</b>   <b>out</b> } <i>priority</i>

**no**

Removes the ACL group from this interface.

***group\_name***

Specifies the name of an existing ACL group as an alphanumeric string of 1 through 47 characters.

**Important**

Up to eight ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 128-rule limit for the interface.

**{ in | out }**

Specifies whether the ACL group will apply to inbound or outbound traffic.

**priority**

If more than one ACL group is applied, *priority-value* specifies the priority in which they will be compared against the packet. If not specified, the priority is set to 0. *priority-value* must be an integer from 0 through 4294967295. If access groups in the list have the same priority, the last one entered is used first.

**Usage Guidelines**

Specify the name of the Access Control List (ACL) group to assign to the interface along with its directionality and priority.

**Example**

```
ip access-group acl-101 in 56
```

## ip address

Specifies the primary and optional secondary IPv4 addresses and subnets for this interface.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
ip address ip_address { mask | /mask } [ secondary ip_address ] [ srp-activate ]
no ip address ip_address
```

**no**

Removes the IPv4 address from this interface.

**ip\_address{ mask | /mask }**

Configures the IPv4 address and mask for the interface. *ip\_address* must be entered using IPv4 dotted-decimal notation. IPv4 dotted-decimal or CIDR notation is accepted for the mask.

**Important**

For IPv4 addresses, 31-bit subnet masks are supported per RFC 3021.

**secondary ip\_address**

Configures a secondary IPv4 address on the interface.

**Important**

You must configure the primary IPv4 address before you will be allowed to configure a secondary address.



**srp-activate**

Activates the IP address for Interchassis Session Recovery (ICSR). Enable this IPv4 address when the Service Redundancy Protocol (SRP) determines that this chassis is ACTIVE. Requires an ICSR license on the chassis to activate.

**Usage Guidelines**

The following command specifies the primary IP address and subnets for this interface.

**Example**

The following example configures an IPv4 address for this interface:

```
ip address 192.154.3.5/24
```

## ip igmp profile

Associates an Internet Group Management Protocol (IGMP) profile with this interface.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
[ no ] ip igmp profile profile_name
```

**no**

Removes the IGMP profile from this interface.

***profile\_name***

Specifies the name of an existing IGMP profile as an alphanumeric string of 1 through 63 characters.

If the name is not for an existing profile, you are prompted to create a new profile. You are then moved to the IGMP Profile Configuration mode.

**Usage Guidelines**

Associates an Internet Group Management Protocol (IGMP) profile with this interface.

**Example**

```
ip igmp profile default
```

## ip mtu

Configures the Maximum Transmission Unit (MTU) for this interface.

**Product**

All

**Privilege**

Security Administrator, Administrator

---

**Syntax Description**    `ip mtu mtu_size [ mru mr_u_size ]`

**no**

Removes the MTU value.

***mtu\_size***

Specifies the MTU in bytes as an integer from 576 though 2048.

***mr\_u\_size***

Specifies the MRU in bytes as an integer from 576 though 2048.

---

**Usage Guidelines**

For MTU,

IP MTU is supported for a normal interface and point-to-point interface (OLC ports).

The maximum MTU size allowed with an OLC port is 1600.

The maximum MTU size allowed with an Ethernet port is 2048. The default MTU size is 1500.

The maximum sizes for ethernet MTUs are:

- **Untagged traffic** (non-VLAN) – **ip MPU *mtu-size*** + ethernet header (20 bytes)
- **VLAN traffic** – **ip MPU *mtu-size*** + ethernet header (20 bytes) + vlan header (4 bytes)

**Example**

The following command sets the MTU value to *2048*.

```
ip mtu 2048
```

Usage Guidelines for MRU:

1. MRU attribute is optional and when it is not configured, MRU is set to the same value as MTU.
2. MRU optional attribute is not visible to users on VPC-DI and VPC-SI platforms. This is only visible on ASR 5500.
3. On nonlegacy ASR 5500 variants such as CUPS or ICUPS, the following error is shown to you when you try to configure MRU on an interface.

```
Failure: Configure MRU Feature is not supported when ICUPS/CUPS is
enabled!
```

**Example**

The following command sets the MTU value to *2048*.

```
ip mtu 2048
```

The following command sets the MTU value to *1600* and MRU value to *1900*.

```
ip mtu 2048 mr_u 1900
```

## ip ospf authentication-key

Configures the password for authentication with neighboring Open Shortest Path First (OSPF) routers.

---

**Product**

PDSN  
HA  
GGSN

---

**Privilege**

Security Administrator, Administrator

---

**Syntax Description**

```
ip ospf authentication-key [ encrypted ] password auth_key
no ip ospf authentication-key
```

**no**

Deletes the authentication key.

**encrypted**

Use this keyword if you are pasting a previously encrypted authentication key into the CLI command.

**password *auth\_key***

Specifies the password to use for authentication as an alphanumeric string of 1 through 16 characters entered in clear text format.

---

**Usage Guidelines**

Use this command to set the authentication key used when authenticating with neighboring routers.

**Example**

To set the authentication key to 123abc, use the following command;

```
ip ospf authentication-key password 123abc
```

Use the following command to delete the authentication key;

```
no ip ospf authentication-key
```

## ip ospf authentication-type

Configures the OSPF authentication method to be used with OSPF neighbors over the logical interface.

---

**Product**

PDSN  
HA  
GGSN

---

**Privilege**

Security Administrator, Administrator

---

**Syntax Description**    `ip ospf authentication-type { message-digest | null | text }`  
`no ip ospf authentication-type { message-digest | null | text }`

**no**

Disable this function.

**message-digest**

Uses the message digest (MD) authentication method.

**null**

Uses no authentication, thus disabling either MD or clear text methods.

**text**

Uses the clear text authentication method.

---

**Usage Guidelines**    Use this command to set the type of authentication to use when authenticating with neighboring routers.

**Example**

To set the authentication type to use clear text, enter the following command;

```
ip ospf authentication-type text
```

## ip ospf bfd

Enables or disables OSPF Bidirectional Forwarding Detection (BFD) on this interface.

---

**Product**    PDSN  
               HA  
               GGSN

---

**Privilege**    Security Administrator, Administrator

---

**Syntax Description**    `ip ospf bfd [ disable ]`  
`no ip ospf cost`

**no**

Disable this function.

**disable**

Disables OSPF BFD on this interface.

---

**Usage Guidelines**    Enable or disable OSPF Bidirectional Forwarding Detection (BFD) on this interface.

**Example**

Use the following command to enable OSPF BFD;

```
ip ospf bfd
```

## ip ospf cost

Configures the cost associated with sending a packet over the OSPF logical interface.

**Product**

PDSN

HA

GGSN

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
ip ospf cost value
```

```
no ip ospf cost
```

**no**

Disable this function.

**value**

Specifies the cost to assign to OSPF packets as an integer from 1 through 65535. Default: 10

**Usage Guidelines**

Use this command to set the cost associated with routes from the interface.

**Example**

Use the following command to set the cost to 20;

```
ip ospf cost 20
```

Use the following command to disable the cost setting;

```
no ip ospf cost
```

## ip ospf dead-interval

Configures the interval that the router should wait, during which time no packets are received and after which the router considers a neighboring router to be off-line.

**Product**

PDSN

HA

GGSN

---

**Privilege** Security Administrator, Administrator

---

**Syntax Description** `[ no ] ip ospf dead-interval seconds`

**no**

Returns the value to its default of 40 seconds.

**seconds**

Specifies the interval (in seconds) as an integer from 1 through 65535. This number is typical four times the hello-interval. Default: 40

---

**Usage Guidelines** Use this command to set the dead intervals for OSPF communications.

**Example**

To set the dead-interval to *100*, use the following command;

```
ip ospf dead-interval 100
```

## ip ospf hello-interval

Configures the interval (in seconds) between sending OSPF hello packets.

---

**Product** PDSN  
HA  
GGSN

---

**Privilege** Security Administrator, Administrator

---

**Syntax Description** `ip ospf hello-interval seconds`  
`no ip ospf hello-interval`

**no**

Returns the value to its default of 10 seconds.

**seconds**

Specifies the number of seconds between sending hello packets as an integer from 1 through 65535. Default: 10

---

**Usage Guidelines** Specify the interval (in seconds) between sending OSPF hello packets.

**Example**

To set the hello-interval to *25*, use the following command;

```
ip ospf hello-interval 25
```

## ip ospf message-digest-key

Enables or disables the use of MD5-based OSPF authentication.

---

**Product**

PDSN  
HA  
GGSN

---

**Privilege**

Security Administrator, Administrator

---

**Syntax Description**

```
ip ospf message-digest-key key_id md5 [ encrypted ] password authentication_key  
no ip ospf message-digest-key key_id
```

**no**

Deletes the key.

**message-digest-key *key\_id***

Specifies the key identifier number as an integer from 1 through 255.

**encrypted**

Use this if you are pasting a previously encrypted authentication key into the CLI command.

**password *authentication\_key***

Specifies the password to use for authentication as an alphanumeric string of 1 through 16 characters entered in clear text format.

---

**Usage Guidelines**

Use this command to create an authentication key that uses MD5-based OSPF authentication.

**Example**

To create a key with the ID of 25 and a password of *123abc*, use the following command;

```
ip ospf message-digest-key 25 md5 password 123abc
```

To delete the same key, enter the following command;

```
no ip ospf message-digest-key 25
```

## ip ospf network

Configures the Open Shortest path First (OSPF) network type.

---

**Product**

PDSN  
HA

GGSN

---

**Privilege**

Security Administrator, Administrator

---

**Syntax Description**

```
ip ospf network { broadcast | non-broadcast | point-to-multipoint |
point-to-point }
no ip ospf network
```

**no**

Disable this function.

**broadcast**

Sets the network type to broadcast.

**non-broadcast**

Sets the network type to non-broadcast multi access (NBMA).

**point-to-multipoint**

Sets the network type to point-to-multipoint.

**point-to-point**

Sets the network type to point-to-point.

---

**Usage Guidelines**

Use this command to specify the OSPF network type.

**Example**

To set the OSPF network type to *broadcast*, enter the following command;

```
ip ospf network broadcast
```

To disable the OSPF network type, enter the following command;

```
no ip ospf network
```

## ip ospf priority

Designates the OSPF router priority.

---

**Product**

PDSN

HA

GGSN

---

**Privilege**

Security Administrator, Administrator



**Syntax Description**

```
ip ospf priority value
no ip ospf priority value
```

**no**

Disable this function.

***value***

Sets the priority value as an integer from 0 through 255.

**Usage Guidelines**

Use this command to set the OSPF router priority.

**Example**

To set the priority to 25, enter the following command:

```
ip ospf priority 25
```

To disable the priority, enter the following command:

```
no ip ospf priority
```

## ip ospf retransmit-interval

Configures the interval in (seconds) between LSA (Link State Advertisement) retransmissions.

**Product**

PDSN

HA

GGSN

**Privilege**

Security Administrator, Administrator

**Syntax Description**

```
ip ospf retransmit-interval seconds
no ip ospf retransmit-interval
```

**no**

Returns the value to its default of 5 seconds.

***seconds***

Specifies the number of seconds between LSA (Link State Advertisement) retransmissions as an integer from 1 through 65535. Default: 5

**Usage Guidelines**

Configure the interval in (seconds) between LSA (Link State Advertisement) retransmissions.

**Example**

To set the retransmit-interval to 10, use the following command;

```
ip ospf retransmit-interval 10
```

## ip ospf transmit-delay

Configures the interval (in seconds) that the router should wait before transmitting an OSPF packet.

---

### Product

PDSN  
HA  
GGSN

---

### Privilege

Security Administrator, Administrator

---

### Syntax Description

```
ip ospf transmit-delay seconds
no ip ospf transmit-delay
```

**no**

Returns the value to its default of 1 second.

### **seconds**

Specifies the number of seconds that the router should wait before transmitting a packet as an integer from 1 through 65535. Default: 1

---

### Usage Guidelines

Configure the interval (in seconds) that the router should wait before transmitting an OSPF packet.

### Example

To set the transmit-delay to 5, use the following command;

```
ip ospf transmit-delay 5
```

## ipv6 access-group

Specifies the name of the access control list (ACL) group to assign to this interface. You can filter for either inbound or outbound traffic.

---

### Product

PDSN  
HA

---

### Privilege

Security Administrator, Administrator

---

### Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

```
configure > context context_name > interface interface_name broadcast
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth) #
```

---

**Syntax Description**

```
[ no ] ipv6 access-group group_name { in | out } { priority-value priority_value }
}
```

**no**

Removes a previously configured access group association.

**group\_name**

Specifies the name of the access group as an alphanumeric string of 1 to 79 characters.

**in**

Applies the filter to the inbound traffic.

**out**

Applies the filter to the outbound traffic.

**priority-value**

Specifies the priority of the access group as an integer from 0 to 4294967295. 0 is the highest priority. If priority-value is not specified, the priority is set to 0.

If access groups in the list have the same priority, the last one entered is used first.

---

**Usage Guidelines**

Use this command to specify the ACL group to assign the interface to. Specify an ACL group name with this command.




---

**Important**

Up to eight ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 128-rule limit for the interface.

---

**Example**

Use the following command to associate the *group\_1* access group with the current IPv6 profile for inbound access:

```
ipv6 access-group group_1 in 1
```

## ipv6 address

Specifies an IPv6 address and subnet mask.

---

**Product**

PDSN

HA

---

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

**configure > context** *context\_name* > **interface** *interface\_name* **broadcast**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

**Syntax Description**

[ **no** ] **ipv6 address** *ipv6\_address/mask*

**no**

Removes the IPv6 address from this interface.

***ipv6\_address/mask***

Specifies an individual host IP address to add to this host pool in IPv6 colon-separated hexadecimal CIDR notation.

**Important**

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

**Usage Guidelines**

Configures the IPv6 address and subnet mask for a specific interface.

**Example**

The following example configures an IPv6 address for this interface:

```
ipv6 address 2002:0:0:0:0:0:c014:101/128
```

# ipv6 ospf

Enables Open Shortest Path First Version 3 (OSPFv3) functionality on this IPv6 interface.

**Product**

PDSN

HA

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

**configure > context** *context\_name* > **interface** *interface\_name* **broadcast**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

**Syntax Description**

```
[ no ] ipv6 ospf [ area { integer | ipv4-address } | cost cost-value |
dead-interval dead-intrv | hello-interval hello-intrvl | priority p-value |
retransmit-interval retx-interval | transmit-delay td-interval ]
```

**no**

Removes a previously configured access group association.

**area { integer | ipv4-address }**

Specifies an OSPFv3 area.

*decimal\_value*: Specifies the identification number of the area as an integer from 0 through 4294967295.

*ipv4-address*: Specifies the IP address of the area in IPv4 dotted-decimal notation.

**cost cost-value**

Specifies a link cost as an integer from 1 through 65535. The link cost is carried in the LSA updates for each link. The cost is an arbitrary number.

**dead-interval dead-intrv**

Specifies the interval (in seconds) after which a neighbor is declared dead when no hello packets as an integer from 1 through 65535.

**hello-interval hello-intrvl**

Specifies the interval (in seconds) between hello packets that OSPFv3 sends on an interface as an integer from 1 through 65535.

**priority p-value**

Specifies the priority of the interface as an integer from 0 through 255.

**retransmit-interval retx-interval**

Specifies the time (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPFv3 interface as an integer from 1 through 65535.

**transmit-delay td-interval**

Specifies the estimated time (in seconds) required to send a link-state update packet on the interface as an integer from 1 through 65535.

**Usage Guidelines**

Configure an OSPFv3 interface in this context.

**Example**

```
ipv6 ospf area 334 cost 555 dead-interval 40 hello-interval 10 priority
10 retransmit-interval 5 transmit-delay 10
```

## ipv6 router advertisement

Enables or disables the system to send IPv6 router advertisements.

---

### Product

PDSN

HA

---

### Privilege

Security Administrator, Administrator

---

### Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

**configure > context** *context\_name* > **interface** *interface\_name* **broadcast**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

---

### Syntax Description

[ no ] **ipv6 router advertisement**

---

### Usage Guidelines

Enables sending of router advertisements on the interface. All of the pool prefixes in the context (belonging to the interface) will be advertised in the router advertisement.

The router-lifetime in the advertisement is sent as 0 to indicate to the receiver that the sender cannot be a default-router. For all the prefixes (pools), the valid and preferred lifetime are sent as default. The router-advertisement is sent every 600 seconds.

If the pool-prefix is deleted, then router-advertisement is sent for that particular prefix with the valid and preferred time set to 0.

## logical-port-statistics

Enables or disables the collection of logical port (VLAN and NPU) bulk statistics for the first 32 configured Ethernet or PVC interface types.

---

### Product

All

---

### Privilege

Security Administrator, Administrator

---

### Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

**configure > context** *context\_name* > **interface** *interface\_name* **broadcast**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

---

### Syntax Description

[ no ] **logical-port-statistics**

**no**

Stops the collection of logical port statistics on this interface.

**Usage Guidelines**

Starts or stops the collection of logical port bulkstats. Default: This feature is not enabled.

Statistics are collected for up to 32 logical ports. The system collects statistics on a per minute basis and maintains samples for the last 5-minute and 15-minute intervals when this feature is enabled.

**Example**

To start collection of logical port statistics on this interface, enter the following command:

```
logical-port-statistics
```

## **mpls ip**

Enables or disables dynamic Multiprotocol Label Switching (MPLS) distribution and forwarding of IP packets on this interface.

**Product**

GGSN  
HA  
P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

**configure** > **context** *context\_name* > **interface** *interface\_name* **broadcast**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth) #
```

**Syntax Description**

[ **no** ] **mpls ip**

**no**

Stops dynamic label distribution and forwarding on this interface.

**Usage Guidelines**

Starts label distribution and forwarding over an interface for a context that has MPLS enabled. For additional information, refer to the *Context Configuration Mode Commands* chapter. Default: This feature is not enabled.

**Example**

To start dynamic MPLS distribution and forwarding on this interface, enter the following command:

```
mpls ip
```

# policy-forward

This command supports downlink IPv4 data packets received from the SGi that are forwarded/redirected to a configured next-hop address if the subscriber session does not exist in the P-GW.

---

**Product**

PDSN  
P-GW

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

**configure > context *context\_name* > interface *interface\_name* broadcast**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

---

**Syntax Description**

**policy-forward { icmp unreachable next-hop *ip\_address* | unconnected-address next-system *ip\_address* }**  
**no policy-forward unconnected-address**

**no**

Deletes the policy forwarding configuration for unconnected address for the current interface.

**icmp unreachable next-hop *ip\_address***

Specifies routing of Internet Control Message Protocol (ICMP) unreachable is required in overlapping pool configuration. *ip\_address* must be expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**unconnected-address next-system *ip\_address***

Specifies the IP address of the next system P-GW to handle processing during P-GW upgrade. *ip\_address* must be an IP address expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.




---

**Important**

The **unconnected-address next-system *ip\_address*** keyword enables IPv4 downlink data packet forwarding/redirection.

---



---

**Usage Guidelines**

Use this command to set the redirecting policy for IP packets from an existing P-GW to a new P-GW during upgrade. To configure this command both keywords will be in separate interface.




---

**Important**

This is a customer specific command.

---



**Example**

To configure existing P-GW system for redirecting the P-GW packets to new P-GW during existing P-GW upgrade enter the following commands:

```
policy-forward unconnected-address next-system ip_address
policy-forward icmp unreachable next-hop ip_address
```

## pool-share-protocol

Configures the primary or secondary system for the IP pool sharing protocol and enter IPSP configuration mode.

**Product**

PDSN  
HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

**configure** > **context** *context\_name* > **interface** *interface\_name* **broadcast**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth) #
```

**Syntax Description**

```
pool-share-protocol { primary ip_address | secondary ip_address } [ mode {
active | inactive | check-config } ]
no pool-share-protocol
```

**no**

Deletes the IP pool sharing protocol information from the current interface.

**primary address**

On the secondary system, defines the IP address of an interface on the primary system that has identical IP pools configured for use with the IP pool sharing protocol. *ip\_address* must be expressed in IP v4 dotted-decimal notation.

**secondary ip\_address**

On the primary system, define the IP address of an interface on the secondary system that has identical IP pools configured for use with the IP pool sharing protocol. *ip\_address* must be expressed in IP v4 dotted-decimal notation.

**mode { active | inactive | check-config }**

This is an optional command to manage the mode for IP pool sharing protocol for primary or secondary HA.

**active:** Activates the IP pool sharing protocol mode.

**inactive:** Inactivates the IP pool sharing protocol mode.

**check-config:** Verifies the IP pool sharing protocol configuration.

### Usage Guidelines

Use this command to set the IP address of the primary or secondary system for use with the IP pool sharing protocol and enter ipsp configuration mode. This command must be configured for an interface in each context that has IP pools configured. Refer to the *System Administration Guide* for information on configuring and using the IP pool sharing protocol.



#### Important

Both the primary and secondary systems must be in the same subnet.



#### Important

For information on configuring and using IP Pool Sharing Protocol (IPSP), refer to the *PDSN Administration Guide*.



#### Important

Reserve free addresses on the primary HA for this command via the **reserved-free-percentage** command as described in the *IPSP Configuration Mode Commands* chapter of this guide.

### Example

To configure a secondary system with an IP address of *192.168.100.10* for use with the IP pool sharing protocol, enter the following command:

```
pool-share-protocol secondary 192.168.100.10
```

To inactivate a secondary system with an IP address of *192.168.100.10* for use with the IP pool sharing protocol, enter the following command:

```
pool-share-protocol secondary 192.168.100.10 mode inactive
```

## port-switch-on-L3-fail

Causes the ASR 5500 MIO port to which the current interface is bound to switch over to the port on the redundant line card or MIO when connectivity to the specified IP address is lost.

### Product

All

### Privilege

Security Administrator, Administrator

### Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

```
configure > context context_name > interface interface_name broadcast
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth) #
```

**Syntax Description**

```
port-switch-on-L3-fail address { ip_address | ipv6_address } [
minimum-switchover-period switch_time ] [ interval int_time ] [ timeout time_out
] [ num-retry number ]
no port-switch-on-L3-fail
```

**no**

Disable port switchover on failure.

**ip\_address**

The IP address to monitor for connectivity, entered in IPv4 dotted-decimal or IPv6 colon-separated hexadecimal notation.

**minimum-switchover-period switch\_time**

After a switchover occurs, another switchover cannot occur until the specified amount of time (in seconds) has elapsed. The *switch\_time* must be an integer from 1 through 3600. Default: 120

**interval int\_time**

Specifies how often (in seconds) monitoring packets are sent to the IP address being monitored. The *int\_time* must be an integer from 1 through 3600. Default: 60

**timeout time\_out**

Specifies how long to wait (in seconds) without a reply before resending monitoring packets to the IP address being monitored. The *time\_out* must be an integer from 1 through 10. Default: 3

**num-retry number**

Specifies how many times to retry sending monitor packets to the IP address being monitored before performing the switchover. The *number* must be an integer from 1 through 100. Default: 5

**Usage Guidelines**

Use this command to monitor a destination in your network to test for L3 connectivity. The destination being monitored should be reachable from both the active and standby line cards.

**Example**

The following command enables port switchover on connectivity failure to the IP address *192.168.10.100* using default values:

```
port-switch-on-L3-fail address 192.168.10.100
```

The following command disables port switchover on connectivity failure:

```
no port-switch-on-L3-fail
```

## vlan-map

Sets a single next-hop IP address so that multiple VLANs can use a single next-hop gateway. The *vlan-map* is associated with a specific interface (ASR 5000 only).

<b>Product</b>	PDSN HA SGSN
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration <b>configure &gt; context <i>context_name</i> &gt; interface <i>interface_name</i> broadcast</b> Entering the above command sequence results in the following prompt: <pre>[<i>context_name</i>]host_name(config-if-eth)#</pre>
<b>Syntax Description</b>	<b>vlan-map next-hop <i>ip_address</i></b>  <b>next-hop <i>ip_address</i></b> Specifies the IP address for the next-hop gateway in IPv4 dotted-decimal notation.
<b>Usage Guidelines</b>	Use this command to combine multiple VLAN links to go through a single IP address. This feature is used in conjunction with nexthop forwarding and overlapping IP pools.  After configuring the vlan-map, move to the Ethernet Port Configuration mode to attach the vlan-map to a specific VLAN.  <b>Example</b> The following command sets an IPv4 address for a next-hop gateway. <b>vlan-map next-hop 123.123.123.1</b>



## CHAPTER 15

# Ethernet Port Configuration Mode Commands

### Command Modes

The Ethernet Port Configuration Mode is used to create and manage Ethernet ports and their bindings between contexts.

Exec > Global Configuration > Ethernet Port Configuration

**configure > port ethernet slot\_number/port\_number**

Entering the above command sequence results in the following prompt:

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



### Important

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

- [bind interface](#), on page 144
- [breakout-cable](#), on page 144
- [boxertap](#), on page 146
- [description](#), on page 146
- [do show](#), on page 147
- [end](#), on page 147
- [exit](#), on page 148
- [fault-unidirect-mode](#), on page 148
- [flow-control](#), on page 149
- [ingress-mode](#), on page 150
- [link-aggregation](#), on page 150
- [media](#), on page 154
- [medium](#), on page 155
- [preferred slot](#), on page 156
- [shutdown](#), on page 157
- [snmp trap link-status](#), on page 158
- [srp virtual-mac-address](#), on page 158
- [threshold high-activity](#), on page 159
- [threshold monitoring](#), on page 160
- [threshold rx-utilization](#), on page 161
- [threshold tx-utilization](#), on page 163

- [vlan, on page 164](#)

## bind interface

Configures an association (binds) between a virtual IP interface, an SS7 or Frame Relay link to a specific context.

---

### Product

All

---

### Privilege

Security Administrator, Administrator

---

### Command Modes

Exec > Global Configuration > Ethernet Port Configuration

**configure > port ethernet** *slot\_number/port\_number*

Entering the above command sequence results in the following prompt:

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

---

### Syntax Description

[ **no** ] **bind interface** *interface\_name context\_name*

#### **no**

Indicates the virtual interface specified is to be unbound from the context.

#### ***interface\_name***

Specifies the name of an existing virtual interface to be bound to the context as an alphanumeric string of 1 through 79 characters. The interface must be previously defined using the Context Configuration mode **interface** command.

#### ***context\_name***

Specifies the name of the context to be bound to the virtual port. *context\_name* must refer to a previously configured context.

---

### Usage Guidelines

Bind an interface to a context to allow the context to provide service.

#### **Example**

The following command binds the *ethernet10* interface with the *allstar4* context:

```
bind interface ethernet10 allstar4
```

## breakout-cable

Configures port breakout-cable usage for 100GBASE to 10x10GBASE SR or LR interfaces on MIO2 cards.



**Important** This command cannot be executed on ports equipped with CPAK 100GBASE-LR4 modules because they do not support use of breakout cables.

**Product**

All products running on an ASR 5500 equipped with MIO2 cards and CPAK modules

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Ethernet Port Configuration

**configure** > **port ethernet slot\_number/port\_number**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

[ no ] **breakout-cable**

**no**

Disables breakout cable support for the 100GBASE interface on an MIO2 card.

**Usage Guidelines**

Use this command to enable or disable the splitting of the 100GB interface on MIO2 cards into ten 10GBASE-SR or 10GBASE-LR ports using an MPO24-to-multiple LC breakout cable. This command can be executed for one or both CPAK modules (port 10 and/or 20) on the MIO2. The use of breakout cables is supported for CPAK-100G-SR10 and CPAK 10x10G-LR modules.

If you enable **breakout-cable** for CPAK ports 5/10 and/or 5/20, after synchronization the configuration will also be valid on CPAK ports 6/10 and/or 6/20.

After enabling or disabling the **breakout-cable** command, you must run the Exec mode **file synchronize** command to assure that the standby MIO2 has the same port configuration as the active MIO2. If a reboot causes the standby MIO2 to become active without synchronization, the breakout port configuration will not be valid on the newly active MIO2.

If you enable or disable cable splitting you must also reboot the system by issuing the Exec mode **reload** command.



**Note** After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.



**Caution** Issuing the **reload** command causes the system to become unavailable for session processing until the reboot process is complete.

For additional information, refer to the *MIO2 Cabling* chapter of the *ASR 5500 Installation Guide*.

**Example**

The following command enables support for a 100Gb interface to ten 10Gb interfaces breakout cable:

```
breakout-cable
```

# boxertap

Binds a physical port to a named interface for debugging purposes.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Ethernet Port Configuration

```
configure > port ethernet slot_number/port_number
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no ] boxertap interface_name
```

**no**

Unbinds the physical port to the interface.

***interface\_name***

Specifies the name of the virtual interface to be bound to the physical port as an alphanumeric string of 1 through 79 characters.

**Usage Guidelines**

Bind a physical port to a named interface for debugging purposes.

**Example**

The following command binds the *ggsn01* interface to the boxertap port.

```
boxertap ggsn01
```

# description

Allows you to enter descriptive text for this configuration.

**Product**

All

**Privilege**

Security Administrator, Administrator



---

**Syntax Description**    **description** *text*  
**no description**

**no**

Clears the description for this configuration.

**text**

Enter descriptive text as an alphanumeric string of 1 to 100 characters.

If you include spaces between words in the description, you must enclose the text within double quotation marks (" "), for example, "AAA BBBB".

---

**Usage Guidelines**    The description should provide useful information about this configuration.

## do show

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

---

**Product**    All

---

**Privilege**    Security Administrator, Administrator

---

**Syntax Description**    **do show**

---

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

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




---

**Caution**

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

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

---

## end

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

---

**Product**    All

---

**Privilege**    Security Administrator, Administrator

---

**Syntax Description**    **end**

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

## exit

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

**Product** All

**Privilege** Security Administrator, Administrator

**Syntax Description** `exit`

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

## fault-unidirect-mode

Configures the unidirectional mode that generates fault messages for the connection's peer when local faults are detected and remote faults are received.

**Product** All

**Privilege** Security Administrator, Administrator

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

**configure** > **port ethernet** *slot\_number/port\_number*

Entering the above command sequence results in the following prompt:

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

**Syntax Description** `[ no ] fault-unidirect-mode ( clause-46 | clause-66 )`

**no fault-unidirect-mode**

Disables fault message generation.

**( clause-46 | clause-66 )**

**clause-46:** On local fault reception, continuous remote faults are sent. On remote fault reception, continuous idles are sent. [IEEE 802.3, Clause 46, Reconciliation Sublayer (RS) and 10 Gigabit Media Independent Interface (XGMII)]

**clause-66:** On local fault reception, frame transmit is continued, remote fault indication is sent during Inter-Frame Gap (IFG). On remote fault reception, frame transmit is continued. [IEEE 802.3, Clause 66, Extensions of the 10 Gb/s Reconciliation Sublayer (RS), 100BASE-X PHY, and 1000BASE-X PHY for unidirectional transport]

**Usage Guidelines** Configure the unidirectional mode that generates fault messages for the connection's peer when local faults are detected and remote faults are received.

**Example**

After flow control has been disabled, use the following command to enable flow control:

```
fault-unidirect-mode clause-46
```

# flow-control

Enables and disables flow control on the ASR 5000 Quad Gig-E line card (QGLC) and 10-Gig-E line card (XGLC).

**Product**

PDSN  
SGSN  
GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Ethernet Port Configuration

```
configure > port ethernet slot_number/port_number
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no ] flow-control
```

**no**

Disables flow control on the specified port.

**Usage Guidelines**

Flow control is enabled by default on the QGLC and can be disabled using the **no** command on a per-port basis. This command does not work on the Fast Ethernet Line Card (FELC) and Gigabit Ethernet Line Card (GELC/GLC2) which do not support flow control.

**Important**

Flow control must be enabled on all XGLCs in the chassis. To prevent XGLC shutdowns, you should also enable flow control at 6Gbps on the peer ports of all routers in your network that connect with the ASR 5000.

**Example**

After flow control has been disabled, use the following command to enable flow control:

```
flow-control
```

# ingress-mode

Labels this port as an ingress port (incoming traffic).

---

**Product**

IPSG  
SaMOG

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > Global Configuration > Ethernet Port Configuration

**configure** > **port ethernet** *slot\_number/port\_number*

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description**

[ **no** ] **ingress-mode**

**no**

Disables ingress port tag.

---

**Usage Guidelines**

Use this command to label this port in order for the session manager to recognize the interface from which IP data packets are being received. This command should be used in single context configurations. In single context configurations, the ingress port can only be identified if labeled.




---

**Important**

For IPSG context and service rules, regardless of number of contexts in the configuration, **ingress-mode** CLI command must be configured for ASR5500 and VPC-SI or VPC-DI platforms. This is done to give precedence to the two matching flows. For example, cases when IPv4SA or IPv4DA both are matched for the ingress packet, then if the incoming interface is designated as ingress, the lookup will be performed in the order of IPv4SA first and then IPv4DA. But if the **ingress-mode** is not set, priority is given to the IPv4DA flow. This is true only for ASR5500 and later platforms such as VPC-SI and VPC-DI.




---

**Important**

It is recommended to enable the **ingress-mode** configuration for IPv6 traffic to avoid packet drops.




---

**Important**

Do not enable this command for downlink interfaces. This command should only be applied to uplink interfaces.

## link-aggregation

Aggregates ports on ASR 5500 Management Input/Output (MIO) cards, and sets related parameters in accordance with IEEE 802.3ad.

**Product**

WiMAX  
 PDSN  
 HA  
 FA  
 GGSN  
 SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Ethernet Port Configuration

**configure > port ethernet slot\_number/port\_number**

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

In releases prior to StarOS 21.26:

```
link-aggregation { distribution { block | random | rotate | simple } |
lacp { active | passive } [ rate { auto | fast | slow } ] [ timeout {
long | short } ] | master { global group group_number | group group_number |
local group group_number } | member { global group group_number | group
group_number | local group group_number [ min-link number_links mode {
non-redundant | redundant } ] } | redundancy { standard | switched } [
hold-time sec ] [ preferred slot { card_number | none } ] | toggle-link }
no link-aggregation [ toggle-link ]
default link-aggregation { distribution | lacp | redundancy | toggle-link
}
```

From StarOS 21.26 and later releases:

```
link-aggregation { distribution { block | random | rotate | simple } |
lacp { active | passive } [ rate { auto | fast | slow } ] [ timeout {
long | short } ] | primary { global group group_number | group group_number |
local group group_number } | member { global group group_number | group
group_number | local group group_number [ min-link number_links mode {
non-redundant | redundant } ] } | redundancy { standard | switched } [
hold-time sec ] [ preferred slot { card_number | none } ] | toggle-link }
no link-aggregation [ toggle-link ]
default link-aggregation { distribution | lacp | redundancy | toggle-link
}
```

**distribution { block | random | rotate | simple }**

**Important**

The **distribution** keyword is not supported on the ASR 5500.

Configures link aggregation distribution and controls how a Link Aggregation Group (LAG) hash map is generated. This method is required for Equal Cost Multi-Path (ECMP) routing over LAG. Set this option on

the primary port for use with the whole group. The following list defines the distribution options (assuming port index 0,1,2,3 were selected):

**block:** Blocks of the same port index (Example: 0000111122223333)

**random:** Based on pseudo random number

**rotate:** Repetition of rotated port index (Example: 0123123023013012...)

**simple:** Repetition of all selected port indexes (Example: 0123012301230123...)

### **lACP { active | passive }**

Configures the Link Aggregation Control Protocol (LACP). Set this option on the master port for use with the whole group.

**active** mode sends out LACP packets periodically. This is the default setting.

**passive** mode only responds to LACP packets received.

### **rate { auto | fast | slow }**

Configures the rate at which the LACP sends packets.

**auto:** rate is controlled by the peer

**fast:** 1 second

**slow:** 30 seconds (Default) [ASR 5000 only]

### **timeout { long | short }**

Configures LACP timeout events. Set this option on the master port for use with the whole group.

**long:** Set LACP to long timeout (30 seconds)

**short:** Set LACP to short timeout (3 seconds)

### **master { global group group\_number | group group\_number | local group group\_number }**

This command creates the Master port for the aggregated group.

**global:** Set group global across slots.

**group group\_number:** Set link aggregation group number. The *group\_number* must be an integer from 1 through 1023.

**local:** Set group local within same slot.

### **member { global group group\_number | group group\_number | local group group\_number }**

This command makes the port a member of the aggregated group.

**global:** Set group global across slots.

**group group\_number:** Set link aggregation group number. The *group\_number* must be an integer from 1 through 1023.

**local:** Set group local within same slot.

**min-link *number\_links***

**Important** This feature is only supported on the ASR 5500.

Specifies that a Link Aggregation Group (LAG) is up /usable only when a minimum number of links are available for aggregation. This guarantees that a minimum amount of bandwidth is available for use.

The *number\_links* specifies the minimum number of links required to avoid a LAG switchover. It is an integer from 1 through 255.

When this feature is enabled, a LAG is not usable when the number of links in a LAG goes below the configured min-link value. Switchover to another LAG bundle (if available) automatically occurs when the number of links in the current active bundle goes below the configured min-link value.

**mode { non-redundant | redundant }**

**Important** This feature is only supported on the ASR 5500.

Specifies whether the LAG is configured in *non-redundant* (Active-Active mode) or *redundant* (Active-Standby) mode.

**redundancy { standard | switched } [ hold-time *sec* ] [ preferred slot { *card\_number* | none } ]**

Connects ASR 5500 MIOs to different Ethernet switches. The master port must be set to make this effective for the group.

**standard:** Treats all cards in the group as one group. (Default)

**switched:** Assumes cards are connected to different switches. [ASR 5000 only]

**hold-time *sec*:** Sets the amount of time to hold (in seconds) before switching between cards. Applies to standard and switched modes. The *sec* must be an integer from 0 through 3600. Default: 10

**preferred slot { *card\_number* | none }:** Specifies the preferred behavior for a LAG using two Ethernet switches. Applies to standard and switched modes. The *card\_number* is an integer with value 5 or 6 on an ASR 5500.

When a card number is specified, system behavior varies based on the card type. For MIO (ASR 5500) card, the preferred slot is selected for the initial timeout period to make the selection of an Ethernet switch less random.

**none:** Specifies no preferred slot.

**toggle-link**

**Important** The **toggle-link** keyword is not supported on the ASR 5500.

Set to toggle link on port switch.

**default**

Restores the default values.

**no**

This command deletes the Ethernet port from any group it might be in. If the port was the Master of a group, the whole group would be deleted.

**Usage Guidelines**

Configure from one to four ports on a QGLC (vertical aggregation) or the single port on XGLCs (horizontal aggregation), or traffic ports on an MIO card to be in an aggregation group that links to an aggregation group on a remote Ethernet switch. Very large files can be downloaded across all ports in a group, which makes for a faster download when compared to serial downloads over a single link.

Related **link-aggregation** commands are described in the *Card Configuration Mode Commands* and *Global Configuration Mode Commands* chapters of this guide. For additional information, also refer to the *System Administration Guide*.

**Example**

The following example configures the port to be part of Master Group 2:

```
link aggregation master group 2
```

# media

This command configures the port interface type. (ASR 5000 only)

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Ethernet Port Configuration

```
configure > port ethernet slot_number/port_number
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
media { rj45 | sfp }
```

**rj45**

Sets the physical interface to a copper RJ-45 connector.

**sfp**

Sets the physical interface connection to optical Small Form Factor (SFP) gigabit via an SFP transceiver.

**Usage Guidelines**

Set the media option when the physical cabling interface is changed.



**Example**

The following command sets the physical interface to RJ-45:

```
media rj45
```

# medium

Configures the port speed and communication mode. (ASR 5000 only)

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Ethernet Port Configuration

**configure > port ethernet** *slot\_number/port\_number*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
medium { auto | speed { 10 | 100 | 1000 | 10000 } duplex { full | half } }
```

```
{ auto | speed { 10 | 100 | 1000 | 10000 } duplex { full | half } }
```

Default: **auto**

Optionally sets the speed of the interface and the communication mode.

**auto**: Configures the interface to auto-negotiate the interface speed.

**speed** { **10** | **100** | **1000** | **10000** }: Specifies the speed to use at all times.

**duplex** { **full** | **half** }: Sets the communication mode of the interface to either **full** or **half** duplex.

**Important**

Ethernet networking rules dictate that if a device whose interface is configured to auto-negotiate is communicating with a device that is manually configured to support full duplex, the first device will negotiate to the manually configured speed of the second device but will only communicate in half duplex mode.

**Usage Guidelines**

Set the medium options when the physical interface changes.

**Important**

The **speed** keyword in the **medium** command is not supported on the ASR 5500.

**Example**

The following command configures the port's speed and communication mode to be auto-negotiated.

```
medium auto
```

The following command configures the port's interface speed to gigabit with full duplex communication.

```
medium speed 1000 duplex full
```

## preferred slot

Assigns revertive or non-revertive control to port redundancy auto-recovery. (ASR 5x00 only)

Default: non-revertive operation

---

### Product

PDSN  
FA  
HA  
SGSN  
GGSN

---

### Privilege

Security Administrator, Administrator

---

### Command Modes

Exec > Global Configuration > Ethernet Port Configuration

**configure** > **port ethernet** *slot\_number/port\_number*

Entering the above command sequence results in the following prompt:

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

---

### Syntax Description

[ **no** ] **preferred slot** *slot\_number*

**no**

Disables revertive or auto-recovery operation for the selected port.

**preferred slot** *slot\_number*

Identifies the physical chassis slot where the ASR 5500 MIO card is installed.

---

### Usage Guidelines

This command enables or disables revertive port redundancy, wherein after a port failover, when the original port is restored to service (such as link up) the system will return service to that port automatically.

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

This command must be issued on a per port basis, allowing you to configure specific ports to be used on individual line card, SPIO, or an MIO card.




---

### Important

This command is not supported on all platforms.

---

**Example**

For ASR 5000:

The following command identifies the chassis slot 17 where the line card or SPIO card is installed.

**preferred slot 17**

For ASR 5500:

The following command identifies the chassis slot 5 where the MIO card is installed.

**preferred slot 5**

# shutdown

Terminates all processes supporting the port or blocks the shutting down of the port. Conversely, the port is enabled with the use of the **no** keyword.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > Global Configuration > Ethernet Port Configuration <b>configure &gt; port ethernet slot_number/port_number</b> Entering the above command sequence results in the following prompt: [local]host_name(config-port-slot_number/port_number) #
<b>Syntax Description</b>	<b>[ no ] shutdown</b>  <b>no</b> Enables the port and places it in service.
<b>Usage Guidelines</b>	Shuts down a port prior to re-cabling and/or other maintenance activities. This command powers down the ports on MIO/UMIO cards (ASR 5500). To enable a port (bring it into service) use the <b>no</b> keyword.

**Example**

Use the following command to disable the port:

**shutdown**

Use the following command to enable the port for service:

**no shutdown**

## snmp trap link-status

Enables or disables the generation of an SNMP trap for link status changes.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > Global Configuration > Ethernet Port Configuration

**configure** > **port ethernet** *slot\_number/port\_number*

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description**

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

**no**

Disables the sending of traps for link status changes.

---

**Usage Guidelines**

Enable link status change traps when a monitoring facility can use the information or if there are troubleshooting activities in progress.

**Example**

Use the following command to disable sending of traps:

```
no snmp trap link-status
```

## srp virtual-mac-address

Configures the Standby Router Protocol (SRP) virtual MAC address for the port on an ICSR chassis.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > Global Configuration > Ethernet Port Configuration

**configure** > **port ethernet** *slot\_number/port\_number*

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description**

**srp virtual-mac-address** *mac\_address*  
**no srp virtual-mac-address**

**no**

Disables the SRP virtual MAC addressing for Ethernet ports. The block of virtual MAC addresses is not saved.

**mac\_address**

Enables SRP virtual addressing for the specified MAC address. The MAC address should be specified as six groups of two hexadecimal digits separated by hyphens. For example, 01-23-45-67-89-ab.

**Usage Guidelines**

The SRP virtual MAC address is applied to the port when the chassis is in SRP ACTIVE state. The default is **no srp virtual-mac-address**.

**Important**

This command is not supported on all platforms.

**Example**

Use the following command to enable the SRP's virtual MAC addressing:

```
srp virtual-mac-address 09-33-48-67-99-ae
```

## threshold high-activity

Configures thresholds for high port activity for the port.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Ethernet Port Configuration

```
configure > port ethernet slot_number/port_number
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

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

**high\_thresh**

Specifies the high threshold high port activity percentage that must be met or exceeded within the polling interval to generate an alert or alarm. The percentage is expressed as an integer from 0 through 100. Default: 50

**clear**

Allows the configuration of the low threshold.

***low\_thresh***

Specifies the low threshold high port activity percentage that maintains a previously generated alarm condition. If the activity percentage falls below the low threshold within the polling interval, a clear alarm will be generated. The percentage is expressed as an integer from 0 through 100. Default: 50

**Important**

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

**Usage Guidelines**

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

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

- **Enter condition:** Actual percent utilization of a port is greater than High Threshold.
- **Clear condition:** Actual percent utilization of a port is less than Low Threshold.

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

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

**Example**

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

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

## threshold monitoring

Enables or disables thresholding for port-level values.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Ethernet Port Configuration

```
configure > port ethernet slot_number/port_number
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no ] threshold monitoring
```

**no**

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

**Usage Guidelines**

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

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps:** SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Complete descriptions and other information pertaining to these traps is located in the `starentMIB(8164).starentTraps(2)` section of the *SNMP MIB Reference*. The generation of specific SNMP traps can be enabled or disabled on the system allowing you to view only those traps that are most important to you.
- **Logs:** The system provides a facility called `threshold` for which active and event logs can be generated. As with other system facilities, logs are generated. Log messages pertaining to the condition of a monitored value are generated with a severity level of `WARNING`.
- **Alarm System:** High threshold alarms generated within the specified polling interval are considered "outstanding" until a the condition no longer exists and/or a condition clear alarm is generated.

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

The following table indicates the reporting mechanisms supported by each of the above models.

**Table 1: Thresholding Reporting Mechanisms by Model**

Model	SNMP Traps	Logs	Alarm System
Alert	X	X	
Alarm	X	X	X

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

## threshold rx-utilization

Configures thresholds for receive port utilization.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Ethernet Port Configuration

**configure** > **port ethernet** *slot\_number/port\_number*

Entering the above command sequence results in the following prompt:

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

**Syntax Description** `threshold rx-utilization high_thresh [ clear low_thresh ]`

### **high\_thresh**

Specifies the high threshold receive port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. The percentage is expressed as an integer from 0 through 100. Default: 80

### **clear**

Allows the configuration of the low threshold.

### **low\_thresh**

Specifies the low threshold receive port utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a Clear Alarm will be generated. The percentage is expressed as an integer from 0 through 100. Default: 80



#### **Important**

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

#### **Usage Guidelines**

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



#### **Important**

Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive **or** transmit utilization threshold be configured.

Alerts or alarms are triggered for receive port utilization based on the following rules:

- **Enter condition:** Actual percent utilization of a port for received data is greater than High Threshold
- **Clear condition:** Actual percent utilization of a port for received data is less than Low Threshold

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

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

### **Example**

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

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



# threshold tx-utilization

Configures thresholds for transmit port utilization.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > Global Configuration > Ethernet Port Configuration

**configure** > **port ethernet** *slot\_number/port\_number*

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description**

**threshold tx-utilization** *high\_thresh* [ **clear** *low\_thresh* ]

***high\_thresh***

The high threshold transmit port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. The percentage is expressed as an integer from 0 through 100. Default: 80

**clear**

Allows the configuration of the low threshold.

***low\_thresh***

The low threshold transmit port utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated. The percentage is expressed as an integer from 0 through 100. Default: 80




---

**Important**

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

---

**Usage Guidelines**

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




---

**Important**

Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive **or** transmit utilization threshold be configured.

Alerts or alarms are triggered for transmit port utilization based on the following rules:

- **Enter condition:** Actual percent utilization of a port for transmit data is greater than High Threshold
- **Clear condition:** Actual percent utilization of a port for transmit data is less than Low Threshold

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

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

### Example

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

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

## vlan

Enters VLAN Configuration mode. Creates VLAN if necessary.

### Product

HA  
HSGW  
PDSN  
P-GW  
SAEGW  
SGSN

### Privilege

Security Administrator, Administrator

### Command Modes

Exec > Global Configuration > Ethernet Port Configuration

```
configure > port ethernet slot_number/port_number
```

Entering the above command sequence results in the following prompt:

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

### Syntax Description

```
vlan vlan_id [ inline-process | subscriber-vlan ] [ -noconfirm ]
```

#### **vlan\_id**

Specifies a VLAN identifier as an integer from 1 through 4094. If this identifier does not already exist you are prompted to confirm the identifier and a new one is created.

#### **inline-process**

Specifies that this VLAN will be used for inline processing.

#### **subscriber-vlan**

Specifies that this VLAN will be used for subscriber-based processing.

**-noconfirm**

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

---

**Usage Guidelines**

Use this command to specify an existing VLAN ID or create a new VLAN ID and enter the VLAN Configuration mode.

For additional information, refer to the *VLAN Configuration Mode Commands* chapter.

**Example**

The following command creates the VLAN ID 234.

```
vlan 234
```

```
Are you sure? [Yes|No]: y
```





# CHAPTER 16

## Exec Mode Commands (A-C)

The Exec Mode is the initial entry point into the command line interface system. Exec mode commands are useful in troubleshooting and basic system monitoring.

### Command Modes

This section includes the commands **aaa test** through **crypto-group**.

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```



### Important

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

- [aaa test](#), on page 171
- [abort](#), on page 173
- [active-charging service](#), on page 173
- [alarm](#), on page 174
- [aps](#), on page 175
- [autoconfirm](#), on page 176
- [bulkstats force](#), on page 177
- [call-home send](#), on page 178
- [call-home test](#), on page 178
- [card busy-out](#), on page 179
- [card halt](#), on page 181
- [card migrate](#), on page 182
- [card reboot](#), on page 183
- [card restart](#), on page 184
- [card switch](#), on page 186
- [card upgrade](#), on page 187
- [cdr-push](#), on page 188
- [chassis](#), on page 189
- [clear aaa](#), on page 190
- [clear active-charging analyzer statistics](#), on page 190
- [clear active-charging charging-action statistics](#), on page 202

- clear active-charging content-filtering server-group statistics, on page 202
- clear active-charging credit-control statistics, on page 203
- clear active-charging dns-learnt-ip-addresses, on page 204
- clear active-charging edr-format statistics, on page 205
- clear active-charging edr-udr-file statistics, on page 206
- clear active-charging firewall statistics, on page 206
- clear active-charging firewall track-list, on page 208
- clear active-charging fw-and-nat policy statistics, on page 208
- clear active-charging group-of-ruledefs statistics, on page 209
- clear active-charging nat statistics, on page 210
- clear active-charging regex statistics, on page 211
- clear active-charging rulebase statistics, on page 211
- clear active-charging ruledef statistics, on page 212
- clear active-charging subsystem, on page 213
- clear active-charging tcp-proxy statistics, on page 214
- clear active-charging tethering-detection statistics, on page 215
- clear active-charging tpo policy statistics, on page 215
- clear active-charging tpo profile statistics, on page 215
- clear active-charging blockedlisting statistics, on page 215
- clear active-charging video detailed-statistics, on page 216
- clear administrator, on page 217
- clear alarm, on page 218
- clear alcap, on page 219
- clear asngw-service, on page 219
- clear asnpc-service, on page 220
- clear apn statistics, on page 221
- clear bcmcs statistics, on page 222
- clear blockedlisted-gtpu-bind- address, on page 222
- clear bssap+ statistics, on page 223
- clear bssgp statistics, on page 224
- clear bulkstats, on page 225
- clear ca-certificate-list statistics, on page 226
- clear cae-group statistics server, on page 226
- clear call-home statistics, on page 227
- clear cdr statistics, on page 227
- clear cli history, on page 228
- clear cmp cert-name, on page 228
- clear cmp statistics, on page 229
- clear confdmgr confd cdb, on page 230
- clear confdmgr statistics, on page 231
- clear config, on page 231
- clear congestion-control statistics, on page 232
- clear content-filtering category statistics, on page 234
- clear crash, on page 234
- clear credit-control statistics, on page 235
- clear crypto, on page 236

- [clear cs-network statistics](#), on page 237
- [clear dhcp statistics](#), on page 238
- [clear dhcpv6 statistics](#), on page 239
- [clear diameter aaa-statistics](#), on page 240
- [clear diameter route](#), on page 241
- [clear diameter statistics](#), on page 242
- [clear diameter-service](#), on page 243
- [clear diameter tps-statistics](#), on page 245
- [clear dns-client](#), on page 246
- [clear dns-proxy statistics](#), on page 247
- [clear dynamic-policy statistics](#), on page 248
- [clear egtpc](#), on page 249
- [clear event-notif statistics](#), on page 251
- [clear event-record](#), on page 251
- [clear firewall](#), on page 252
- [clear fng-service statistics](#), on page 252
- [clear gmb statistics](#), on page 253
- [clear gmm-sm statistics](#), on page 253
- [clear gprsns statistics](#), on page 256
- [clear gprssf statistics](#), on page 257
- [clear gtpc statistics](#), on page 258
- [clear gtp statistics](#), on page 259
- [clear gtp storage-server local file statistics](#), on page 260
- [clear gtp storage-server statistics](#), on page 261
- [clear gtpu statistics](#), on page 261
- [clear hd-storage-policy](#), on page 262
- [clear hcnbgw-access-service statistics](#), on page 263
- [clear hcnbgw-network-service statistics](#), on page 264
- [clear hexdump-module statistics](#), on page 265
- [clear hcnbgw sessions](#), on page 266
- [clear hcnbgw statistics](#), on page 268
- [clear hsgw-service](#), on page 270
- [clear hss-peer-service](#), on page 271
- [clear ims-authorization](#), on page 271
- [clear ims-sh-service statistics](#), on page 272
- [clear ip access-group statistics](#), on page 273
- [clear ip arp](#), on page 273
- [clear ip bgp peer](#), on page 274
- [clear ip localhosts](#), on page 275
- [clear ip ospf process](#), on page 276
- [clear ipne statistics](#), on page 276
- [clear ipsg statistics](#), on page 277
- [clear ipv6 neighbors](#), on page 277
- [clear ipv6 ospf process](#), on page 278
- [clear l2tp](#), on page 278
- [clear lawful-intercept](#), on page 280

- clear llc statistics, on page 280
- clear lma-service statistics, on page 281
- clear local-policy, on page 281
- clear local-user, on page 282
- clear location-service, on page 283
- clear mag-service statistics, on page 284
- clear map statistics, on page 284
- clear maximum-temperatures, on page 285
- clear mipfa statistics, on page 286
- clear mipha statistics, on page 286
- clear mipmn statistics, on page 287
- clear mipv6ha statistics, on page 288
- clear mme-service db record, on page 288
- clear mme-service db statistics, on page 289
- clear mme-service statistics, on page 290
- clear multicast-sessions, on page 292
- clear nat-ip, on page 294
- clear pcc-policy service statistics, on page 295
- clear pcc-policy session, on page 295
- clear pcc-sp-endpoint statistics, on page 296
- clear pdg-service statistics, on page 297
- clear pgw-service, on page 298
- clear port, on page 299
- clear ppp statistics, on page 300
- clear prepaid 3gpp2 statistics, on page 301
- clear prepaid wimax, on page 302
- clear ps-network statistics, on page 303
- clear qos npu stats, on page 304
- clear radius accounting archive, on page 304
- clear radius counters, on page 305
- clear rlf-context-statistics, on page 306
- clear rohc statistics, on page 307
- clear rp service-option, on page 308
- clear rp statistics, on page 309
- clear rsvp statistics, on page 309
- clear saegw-service, on page 310
- clear samog-service statistics, on page 311
- clear sbc statistics, on page 311
- clear sccp statistics, on page 312
- clear security, on page 313
- clear session disconnect-reasons, on page 314
- clear session-event-record statistics, on page 314
- clear session setuptime, on page 315
- clear session subsystem, on page 316
- clear sgsn-fast-path statistics, on page 316
- clear sgsn-map-app, on page 317



- clear sgsn rlf-context-statistics, on page 318
- clear sgs-service, on page 319
- clear sgtpc statistics, on page 320
- clear sgtpu statistics, on page 321
- clear sgw-service statistics, on page 322
- clear sls-service statistics, on page 323
- clear sms statistics, on page 324
- clear sndcp statistics, on page 324
- clear snmp trap, on page 325
- clear srp, on page 326
- clear ss7-routing-domain, on page 327
- clear subscribers, on page 328
- clear super-charger, on page 346
- clear supplementary-service statistics, on page 347
- clear tacacs session, on page 348
- clear task resources, on page 349
- clear tcap statistics, on page 353
- clear wsg-service statistics, on page 354
- cli, on page 355
- clock set, on page 356
- cmp enroll current-cert, on page 357
- cmp fetch cert-name, on page 358
- cmp initialize, on page 359
- cmp poll, on page 360
- cmp update, on page 361
- commandguard, on page 362
- configure, on page 363
- context, on page 365
- copy, on page 366
- crash copy, on page 369
- crypto blockedlistfile update, on page 371
- crypto rsa-keygen modulus, on page 371
- crypto permitlistfile update, on page 372
- crypto-group, on page 373

## aaa test

Tests Authentication, Authorization and Accounting (AAA) functionality between this system and a remote server.

---

**Product**

ASN-GW  
GGSN  
HA  
PDSN

SGSN

---

**Privilege**

Security Administrator, Administrator, Operator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
aaa test { accounting username user_name | authenticate user_name password | session user_name password }
```

**accounting username user\_name**

Tests RADIUS or GTPP accounting functionality for the specified user.

*user\_name* must be the name of a user configured on the RADIUS or CFG server.




---

**Important**

GTPP is used only in conjunction with the GGSN or SGSN product.

**authenticate user\_name password**

Tests RADIUS authentication functionality for the specified user.

*user\_name* is the name of a user configured on the RADIUS server. *password* is the user's password.

**session user\_name password**

Tests both RADIUS authentication and RADIUS or GTPP accounting functionality for the specified user.

*user\_name* is the name of a user configured on the RADIUS server. *password* is the user's password.




---

**Important**

GTPP is used only in conjunction with the GGSN or SGSN product.

---

**Usage Guidelines**

This command is used to test RADIUS-based authentication and RADIUS or GTPP accounting. This command may be useful for diagnosing problems with subscribers and access to the system and/or billing data.

**Example**

The following command verifies accounting for a user named *user1*:

```
aaa test accounting username user1
```

The following command tests authentication for a user named *user1* with the password *abc123*:

```
aaa test authentication user1 abc123
```

The following command tests both accounting and authentication for the user named *user1* with the password *abc123*:

```
aaa test session user1 abc123
```

# abort

Stops software patch or upgrade process.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
abort { patch | upgrade } [ -noconfirm ]
```

**patch**

Stops a running software patch process.

**upgrade**

Stops a running software upgrade process.




---

**Important**

The **abort upgrade** command can only be used during Stage 1 (busy-out) of an on-line software upgrade.

---

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

---

**Usage Guidelines**

Use this command to stop a running StarOS patch or upgrade process. For additional information on software patches and upgrades, refer to the *System Administration Guide*.

**Example**

The following command stops an in-progress StarOS upgrade:

```
abort upgrade
```

## active-charging service

Creates an active charging service (ACS).

---

**Product**

ACS

---

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

**active-charging service** *ecs\_service\_name* [ **-noconfirm** ]

***ecs\_service\_name***

Specifies name of the active charging service.

*ecs\_service\_name* must be an alphanumeric string of 1 through 15 characters.

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

If the named service already exists, the CLI mode changes to the ACS Configuration mode wherein the specified active charging service can be configured.

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

**Usage Guidelines**

Use this command to create an active charging service in the system. This command can be used directly in Exec Mode after issuing the **require active-charging** command in the Global Configuration Mode.

This command allows an operator (rather than security administrators and administrators) to configure the ACS functionality only.

On entering this command, the CLI prompt changes to:

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

**Important**

Operators need special CLI privilege for ACS functionality to be able to use this CLI command.

**Example**

The following command creates an active charging service named *test*:

```
active-charging service test
```

# alarm

Disables the internal audible alarm on the MIO card.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

**alarm cutoff**

---

**Usage Guidelines**

Alarm cutoff disables the audible alarm. The alarm may be enabled following this command if an event within the system results in the audible alarm being enabled.

**Example**

```
alarm cutoff
```

## aps

Allows the operator to perform SONET Automatic Protection Switching (APS) administrative operations.




---

**Important**

Use of this command is limited to the OLC2 and the CLC2 line cards.

---

**Product**

SGSN

---

**Privilege**

Security Administrator, Administrator, Operator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
aps { clear slot#/port# | exercise slot#/port# | lockout slot#/port# | switch { force | manual } slot#/port# }
```

**clear slot#/port#**

Clears the last switch command on the specified channelized port.

*slot#/port#* is the CLC2/OLC2 slot number (valid range is 17 - 48) and appropriate port number (CLC2 valid range is 1 - 4; OLC2 valid value is 1).

**exercise slot#/port#**

Tests the APS protocol on line connected to port.

*slot#/port#* is the CLC2/OLC2 slot number (valid range is 17 - 48) and appropriate port number (CLC2 valid range is 1 - 4; OLC2 valid value is 1)

**lockout slot#/port#**

Prevents the working port from switching to the protection port.

*slot#/port#* is the CLC2/OLC2 slot number (valid range is 17 - 48) and appropriate port number (CLC2 valid range is 1 - 4; OLC2 valid value is 1)

**switch { force | manual } *slot#/port#***

Switch to either the working port or the protection port:

- **force**: Forces a switch of ports, even if there is an active alarm state.
- **manual**: Implements a switch of ports if there are no active alarms.

*slot#/port#* is the CLC2/OLC2 slot number (valid range is 17 - 48) and appropriate port number (CLC2 valid range is 1 - 4; OLC2 valid value is 1)

### Usage Guidelines

This command allows an operator to perform administrative/maintenance APS tasks such as testing the APS protocol, switching the working port to the protection port, and locking out the switching function.

### Example

The following command starts an APS protocol test on port 2 of card 27:

```
aps exercise 27/2
```

## autoconfirm

Enables or disables confirmation for certain commands. This command affects the current CLI session only.



### Important

Use the **autoconfirm** command in the Global Configuration Mode to change the behavior for all future CLI sessions.

### Product

All

### Privilege

Security Administrator, Administrator, Operator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

**[ no ] autoconfirm**

**no**

Disables autoconfirm if it has been enabled.

### Usage Guidelines

When **autoconfirm** is enabled, certain commands ask you to answer yes or no to confirm that you want to execute the command. When **autoconfirm** is disabled, the confirmation prompts never appear. Disabling **autoconfirm** in the Exec mode is active for the current CLI session only.

By default **autoconfirm** is enabled.



#### Important

If commandguard is enabled, autoconfirm will disable commandguard.

#### Example

The following command enables command confirmation:

```
autoconfirm
```

## bulkstats force

Manages the collection and delivery of system statistics (bulkstats) to the configured server.

#### Product

All

#### Privilege

Security Administrator, Administrator, Operator

#### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

#### Syntax Description

```
bulkstats force { gather | transfer }
```

#### gather

Immediately collects the system statistics.

#### transfer

Immediately sends the currently collected statistics to the configured server.

#### Usage Guidelines

When the current system statistics are desired immediately as opposed to the normal scheduled collection and delivery intervals issue this command.

Troubleshooting the system may require the review of statistics at times when the scheduled delivery is not timely.

#### Example

The following causes the chassis to immediately collect system statistics. This would be in anticipation of a transfer command.

```
bulkstats force gather
```

The following command causes the chassis to immediately send all collected statistics to the configured server.

```
bulkstats force transfer
```

## call-home send

Manages how Cisco Smart Call Home messages are sent to alert groups.

---

**Product** All

---

**Privilege** Security Administrator, Administrator, Operator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **call-home send alert-group { configuration profile *profile name* | inventory profile *profile name* }**

### **configuration profile *profile name***

Sends configuration messages to the previously defined profile, expressed as an alphanumeric string of 1 through 31 characters.

### **inventory profile *profile name***

Sends inventory messages to the previously defined profile, expressed as an alphanumeric string of 1 through 31 characters.

---

### **Usage Guidelines**

Use this command to send specified alert-group call-home message from the CLI to all profiles subscribed to the specified alert group, or to a specified profile which does not need to be subscribed to the specified alert-group. For additional information, refer to the *Call-Home Configuration Mode Commands* and *Call-Home Profile Configuration Mode Commands* chapters.

### **Example**

The following command sets the system to send configuration related call-home messages to the profile named *Profile1*.

```
call-home send alert-group configuration profile Profile1
```

## call-home test

Sends a test Smart Call Home event message to a specified profile.

---

**Product** All

---

**Privilege** Security Administrator, Administrator, Operator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:



```
[local]host_name#
```

---

**Syntax Description** `call-home test message { test_message_content | profile profile_name }`

**call-home test message message test\_message\_content**

Defines the message to send to the defined profile as an alphanumeric string of 1 through 128 characters.

**profile profile\_name**

Specifies the previously defined profile to which the message will be sent, expressed as an alphanumeric string of 1 through 31 characters.

---

**Usage Guidelines** Use this command to send test call-home messages from the CLI to a specified profile. If a message is not specified, the system sends out a default message.

#### Example

The following command sets the system to send a test call-home message *Test\_Message\_1* to the profile named *Profile1*.

```
call-home test message Test_Message_1 profile Profile1
```

## card busy-out

Moves processes from the source packet processing card to the destination packet processing card, or disables the packet processing card from accepting any new calls. When busy-out is enabled, the packet processing card stops receiving new calls but continues to process calls until they are completed. The command prompt is returned once the command is initiated. The busy-out procedure is completed in background. (ASR 5x00 only)

---

**Product** All

---

**Privilege** Security Administrator, Administrator, Operator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `card busy-out { migrate from src_slot to dst_slot } [ -noconfirm ]`  
`no card busy-out`

**no**

Disables busy-out. The packet processing card is re-enabled to accept new calls.

**migrate from *src\_slot* to *dst\_slot***

Moves processes from the specified source packet processing card to the specified destination packet processing card. The command prompt is returned once the command is initiated. The card migration is completed in background.

*src\_slot* indicates the source slot number of the card from which processes will be migrated. *dst\_slot* indicates the destination slot number of the card to which processes will be migrated.

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

**Usage Guidelines**

Migrating a packet processing card changes the active/standby status of a packet processing card. This results in the active sessions/processes being moved to the newly active card. This is useful when there is a maintenance activity on the active card which requires removing the card from service.

The destination slot specified must contain a packet processing card which is in the standby state for the command to complete successfully.

**Caution**

Be cautious when executing this command. Depending on the number of active sessions being migrated, some subscribers may experience service interruptions.

Using busy-out to refuse new calls on a packet processing card allows you to take a card out of service without any interruptions to the end user. An individual system can be taken completely out of service gracefully by enabling busy-out on all packet processing cards and waiting for current calls to complete. The **show card info** command shows if busy-out is enabled.

**Important**

When a packet processing card fails, is migrated, or is restarted for any reason, busy-out is reset to disabled, the default behavior.

**Important**

This command is not supported on all platforms.

**Example**

The following command migrates the active processes from the packet processing card in slot 12 to the card in slot 14. This command executes after you provide confirmation of the request.

```
card migrate from 12 to 14
```

The following command migrates the active processes from the packet processing card in slot 1 to the card in slot 8. This command executes after you provide confirmation of the request.

```
card migrate from 1 to 8
```

The following command sets the packet processing card in slot 1 to stop accepting new calls:

```
card busy-out 1
```

# card halt

Halts all StarOS processes on a card. A **card reboot** command must be issued to bring the card back into service after it is halted. (ASR 5x00 only)

---

**Product** All

---

**Privilege** Security Administrator, Administrator, Operator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **card halt** *slot\_num* [ **-force** ] [ **-noconfirm** ]

***slot\_num***

Indicates the slot number of the card of interest.

**-force**

Overrides any warnings to force the card to be halted.

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

---

**Usage Guidelines** Halt a card to stop it for maintenance or emergency situations.



**Caution**

Caution should be taken in using this command. Halting a card which has no redundant card available may cause a service interruption and loss of active sessions.



**Important**

On the ASR 5500, do not initiate a **card halt** for an active FSC if there are less than two active FSCs in the system. The system returns an error message if there are less than four active FSCs.



**Caution**

The **-force** and **-noconfirm** options should only be used concurrently by experienced users as this will cause an immediate halt regardless of warnings and no confirmation from the user.



**Important**

This command is not supported on all platforms.

**Example**

The following command temporarily stops the card in slot 1.

```
card halt 1
```

The following commands force the card to halt and indicate no confirmation is to take place, respectively.

```
card halt 1 -force -noconfirm
card halt 1 -noconfirm
```

# card migrate

Migrates StarOS processes from an active packet processing card to a standby packet processing card. (ASR 5x00 only)

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `card migrate from src_slot to dst_slot -force-smaller [ -noconfirm ] [ stop-checkpoint ]`

***src\_slot***

Indicates the slot number of the packet processing card from which processes will be migrated.



**Important** The packet processing card in this slot must be in Active mode.

***dst\_slot***

Indicates the slot number of the packet processing card to which processes will be migrated.

***-force-smaller***

Indicates the force migration to a smaller card even though tasks may not fit.

***-noconfirm***

Executes the command without any additional prompt and confirmation from the user.

**stop-checkpoint**

This command is used instead of the default “live migration” algorithm. The stop and checkpoint algorithm stops the migrating procket, migrates procket, then restarts the procket on the destination card. This migration process is typically faster than the live migration algorithm. However, the migrating procket does not process call requests when stopped.



**Note** Prockets are migrated sequentially and that only one procket is stopped at any point in time. For more information about the usage of **stop-checkpoint** keyword, contact your Cisco Account representative.

**Usage Guidelines**

This command allows an operator to move processes from an active to a standby packet processing card.

**Example**

The following will cause processes currently running on the card in slot 8 to migrate to the standby card in slot 9. The migration will not occur if any warnings are generated.

```
card migrate from 8 to 9
```

## card reboot

Performs reset of the target card. For ASR 5500, rebooting a card will result in the card downloading the image from the active MIO card.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
card reboot target_slot [ -force ] [ -noconfirm ]
```

**target\_slot**

Initiates a reboot of the card in the specified the slot number.

**-force**

Indicates that the reboot is to take place ignoring any state or usage warnings that might be generated.

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

**Usage Guidelines**

A reboot is used to reset the card and receive a new download. This may be useful when a card is not responding or when it is necessary to cause the card to reload its image and restart.

**Caution**

Caution should be taken in using this command. Rebooting a card which has no redundant card available may cause a service interruption and loss of active sessions.

**Important**

On the ASR 5500, do not initiate a **card reboot** for an active FSC if there are less than four active FSCs in the system. The system returns an error message if there are less than four active FSCs.

**Caution**

The **-force** and **-noconfirm** options should only be used concurrently by experienced users as this will cause an immediate reboot regardless of warnings and no confirmation from the user.

**Important**

This command is not supported on all platforms.

**Example**

The following will cause the card in slot 8 to reboot without any confirmation from the user. The card will not reboot if there are any warnings generated.

```
card reboot 8 -noconfirm
```

The following command will cause the card in slot 8 to reboot regardless of any warnings. The user must provide confirmation prior to this command executing.

```
card reboot 8 -force
```

The following command will cause the card in slot 8 to reboot regardless of any warnings with no additional user confirmation.

```
card reboot 8 -force -noconfirm
```

## card restart

Performs a soft-reset of the target card causing all application processes to restart. (ASR 5x00 only)

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
card restart target_slot [ -force ] [ -noconfirm ]
```

**target\_slot**

Initiates a restart of the card in the specified slot number.

**-force**

Indicates the restart is to take place ignoring any state or usage warnings that might be generated.

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

---

**Usage Guidelines**

Restarting a card may be useful when a card is not performing as expected (performance drop, increased response delays, etc.). A restart may be preferred to a reboot as the card becomes available in less time than a reboot.

When this command is issued for an active card, the user is prompted for confirmation unless the **-force** and/or **-noconfirm** keywords are used. Because the reboot of standby or redundant cards is non-service impacting, the reboot proceeds immediately after the command execution without user confirmation.

**Caution**

Caution should be taken in using this command. Restarting a card which has no redundant card available may cause a service interruption and loss of active sessions.

---

**Important**

This command is not supported on all platforms.

---

**Caution**

The **-force** and **-noconfirm** options should only be used concurrently by experienced users as this will cause an immediate restart regardless of warnings and no confirmation from the user.

---

**Example**

The following will cause the card in slot 8 to restart without any confirmation from the user. The card will not reboot if there are any warnings generated.

```
card restart 8 -noconfirm
```

The following command will cause the card in slot 8 to restart regardless of any warnings. The user must provide confirmation prior to this command executing.

```
card restart 8 -force
```

The following command will cause the card in slot 8 to restart regardless of any warnings with no additional user confirmation.

```
card restart 8 -force -noconfirm
```

# card switch

Manages card pairs and their active/standby status (ASR 5x00 and VPC-DI only).

---

**Product** All

---

**Privilege** Security Administrator, Administrator, Operator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `card switch { from target_slot | to target_slot } [ -noconfirm ]`

### **from *target\_slot***

Specifies the slot number of a currently active card that is to be switched. The slot number must be valid and contain a card in active mode.

### **to *target\_slot***

Specifies the slot number of a standby card which is to become the active card. The slot number must be valid and contain a card in standby.

### **-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

---

## Usage Guidelines

Card switch-overs change the active/standby status of a card. This is useful when there is a maintenance activity on the active card which requires removing the card from service.

On VPC-DI, a warning is presented during the switchover between Control Functions (CFs) if the HD RAID is degraded.

Warning: RAID is degraded. Switchover might lead to data loss.



### Caution

Caution should be taken in using this command. Depending on the amount of bandwidth/traffic being switched, some subscribers may experience service interruptions.

---

### Example

The following command switches the active/standby status of the line cards in slots 17 and 18. This command only executes after you provide confirmation of the request.

```
card switch from 17 to 18
```

The following command switches the active/standby status of the cards in slots 1 and 2. This command executes immediately with no additional user confirmation.

```
card switch from 1 to 2 -noconfirm
```



# card upgrade

Upgrades the programmable memory on a card. (ASR 5x00 only)

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

**card upgrade** *slot\_number* [ **-noconfirm** ]

***slot\_number***

The slot number of the card to be upgraded from 1 through 10.

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.




---

**Caution**

Use this command only if instructed by or working with Technical Assistance Center personnel.




---

**Important**

On the ASR 5500, do not initiate a **card upgrade** for an active FSC if there are less than four active FSCs in the system. The system returns an error message if there are less than four active FSCs.

---

**Usage Guidelines**

You can only initiate an upgrade if:

- there is no migration occurring,
- the card is active or standby,
- there is no online upgrade in progress.




---

**Important**

The following operations are not allowed while a card is upgrading: change edc requirement (config), change card [no] shutdown (config), change card active (config), change card redundancy (config), card halt (exec), card reboot (exec), start an online upgrade.




---

**Important**

Level unlock operations are ignored while a card is upgrading.



**Important** This command is not supported on all platforms.

### Example

The following command initiates a packet processing card upgrade on slot number 10:

```
card upgrade 10
```

## cdr-push

Initiates a manual push of CDR files to a configured URL.

### Product

All

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
cdr-push { all | local-filename file_name }
```

#### **all**

Pushes all CDR files to the configured URL.

#### **local-filename** *file\_name*

Pushes only the specified file to the configured URL.

The *file\_name* must be the absolute path of the local file to push, and must be an alphanumeric string of 1 through 1023 characters.

### Usage Guidelines

Use this command to manually push CDR files to the configured URL or external storage.

For information on configuring the external storage, see the **cdr** command in the *EDR Module Configuration Mode Commands* and the *UDR Module Configuration Mode Commands* chapters.

**ASR 5000:** Run this command only from the local context. If you are in any other context, you will see this failure message: "Failure: Manual PUSH of CDRs supported only in the local context"

**ASR 5500:** Run this command only from the local context. If you are in any other context, you will see this failure message: "Failure: Manual PUSH of CDRs supported only in the local context"

### Example

The following command pushes all CDR files to the URL:

```
cdr-push all
```

# chassis

Specifies the chassis key that will be used to encrypt and decrypt encrypted passwords in the configuration file. If two or more chassis are configured with the same chassis key value, the encrypted passwords can be decrypted by any of the chassis sharing the same chassis key value. As a corollary to this, a chassis key value will not be able to decrypt the passwords that were encrypted using a different chassis key value.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
[ no ] chassis { key value key_string | keycheck key_string }
```

**no**

Resets the chassis key to the factory default value. The factory default value is a local MAC address for the chassis. Once this command is executed, the **chassis key value** command can be used to change the default chassis key.

**key value *key\_string***

Specifies the chassis key value as an alphanumeric string of 1 through 16 characters.

The chassis key value is stored as a one-way encrypted value, much like a password. It is never displayed in its plain-text form.

**keycheck *key\_string***

Generates a one-way encrypted key value based on the entered alphanumeric string of 1 through 16 characters.

The generated encrypted key value is compared against the encrypted key value of the previously entered chassis key value. If the encrypted values match, the command succeeds and key check passes. If the comparison fails, a message is displayed indicating that the key check has failed. Note that if the default chassis key (MAC address) is currently being used, this key check will always fail since there will be no chassis key value to compare against.




---

**Important**

For detailed information regarding the impact of using these commands in various StarOS releases, refer to the *System Settings* chapter of the *System Administration Guide*.

---



---

**Usage Guidelines**

Establish multiple, unique chassis keys to encrypt and decrypt passwords in configuration files.

**Example**

The following command generates a one-way encrypted key based on the string *tewks367*.

```
chassis key value tewks367
```

## clear aaa

Clears all Authentication, Authorization, and Accounting (AAA) statistics for the current context.

---

### Product

ASN-GW  
GGSN  
PDSN  
P-GW  
SAEGW

---

### Privilege

Security Administrator, Administrator, Operator

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

**clear aaa local counters**

---

### Usage Guidelines

Clearing the AAA statistics may be useful when monitoring the statistics manually. Clearing resets the counters to zero.

The keyword **local** is not intended to imply the local context defined for all systems. Rather, it indicates the statistics within the current context are to be cleared.

### Example

The following command zeroes out all the AAA statistics in the current context.

```
clear aaa local counters
```

## clear active-charging analyzer statistics

Clears protocol analyzer statistics.

---

### Product

ACS

---

### Privilege

Security Administrator, Administrator, Operator

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `clear active-charging analyzer statistics [ name protocol_name ] [ | { grep grep_options | more } ]`

**name** *protocol\_name*

Clears statistics for the specified protocol analyzer.

If this keyword is not specified all statistics are cleared.

*protocol\_name* must be one of the following:

- **cdp**
- **dns**
- **file-transfer**
- **ftp**
- **http**
- **icmp**
- **icmpv6**
- **imap**
- **ip**
- **ipv6**
- **mipv6**
- **mms**
- **p2p** [ **application** *p2p\_list* | **protocol-group** *group\_list* ]: Peer-to-peer analyzer.  
**p2p application** *p2p\_list*: The supported applications are:
  - **8tracks**
  - **abcnetworks**
  - **actionvoip**
  - **actsync**
  - **adobeconnect**
  - **aimini**
  - **amazoncloud**
  - **amazonmusic**
  - **amazonvideo**
  - **antisp2p**
  - **apple-push**
  - **apple-store**

- **applejuice**
- **applemaps**
- **ares**
- **armagettron**
- **avi**
- **badoo**
- **baidumovie**
- **battlefld**
- **bbm**
- **beatport**
- **betternet**
- **bitcasa**
- **bittorrent**
- **bittorrent-sync**
- **blackberry-store**
- **blackberry**
- **blackdialer**
- **box**
- **callofduty**
- **chikka**
- **cisco-jabber**
- **citrix**
- **clubbox**
- **clubpenguin**
- **comodounite**
- **crackle**
- **crossfire**
- **crunchyroll**
- **cyberghost**
- **ddlink**
- **deezer**
- **didi**

- **directconnect**
- **dish-anywhere**
- **disneymovies**
- **dofus**
- **dramafever**
- **dropbox**
- **ebuddy**
- **edonkey**
- **espn**
- **expressvpn**
- **facebook**
- **facetime**
- **fanor**
- **fasttrack**
- **feidian**
- **ficall**
- **fiesta**
- **filetopia**
- **filmontv**
- **flash**
- **flickr**
- **florensia**
- **foursquare**
- **fox-sports**
- **freenet**
- **friendster**
- **fring**
- **funshion**
- **gadugadu**
- **gamekit**
- **gmail**
- **gnutella**

- go90
- goober
- google-music
- google-push
- google
- googleplay
- googleplus
- gotomeeting
- gtalk
- guildwars
- halflife2
- hamachivpn
- hayu
- hbogo
- hbonow
- heytell
- hgtv
- hike-messenger
- hls
- hotspotvpn
- hulu
- hyves
- iax
- icall
- icecast
- icloud
- idrive
- igo
- iheartradio
- imesh
- imessage
- imgur



- imo
- implus
- instagram
- iplayer
- iptv
- irc
- isakmp
- iskoot
- itunes
- jabber
- jap
- jumblo
- kakaotalk
- kik-messenger
- kontiki
- kugoo
- kuro
- linkedin
- livestream
- lync
- magicjack
- manolito
- mapfactor
- mapi
- maplestory
- meebo
- mgcp
- mig33
- mlb
- mojo
- monkey3
- mozy

- **msn**
- **msrp**
- **mute**
- **mypeople**
- **myspace**
- **nateontalk**
- **naverline**
- **navigon**
- **nbc-sports**
- **netflix**
- **netmotion**
- **newsy**
- **nick**
- **nimbuzz**
- **nokia-store**
- **octoshape**
- **off**
- **ogg**
- **oist**
- **oovoo**
- **opendrive**
- **openft**
- **openvpn**
- **operamini**
- **orb**
- **oscar**
- **outlook**
- **paltalk**
- **pando**
- **pandora**
- **path**
- **pbs**

- pcan anywhere
- periscope
- pinterest
- plingm
- poco
- popo
- pplive
- ppstream
- ps3
- qq
- qqgame
- qqlive
- quake
- quic
- quicktime
- radio-paradise
- rdp
- rdt
- regram
- rfactor
- rhapsody
- rmstream
- rodi
- rynga
- samsung-store
- scydo
- secondlife
- shoutcast
- showtime
- silverlight
- siri
- skinny

- skydrive
- skype
- slacker-radio
- slingbox
- slingtv
- smartvoip
- snapchat
- softether
- sopcast
- soribada
- soulseek
- soundcloud
- spark
- spdy
- speedtest
- spike
- splashfighter
- spotify
- ssdp
- ssl
- starz
- stealthnet
- steam
- stun
- sudaphone
- svtplay
- tagged
- talkatone
- tango
- teamspeak
- teamviewer
- telegram

- **thunder**
- **tinder**
- **tmo-tv**
- **tor**
- **truecaller**
- **truphone**
- **tumblr**
- **tunnelvoice**
- **turbovpn**
- **tvants**
- **tvland**
- **tvuplayer**
- **twitter**
- **twitch**
- **ultrabac**
- **ultrasurf**
- **univision**
- **upc-phone**
- **usenet**
- **ustream**
- **uusee**
- **vchat**
- **veohtv**
- **vessel**
- **vevo**
- **viber**
- **vine**
- **voipdiscount**
- **vopium**
- **voxer**
- **vpnmaster**
- **vpnX**

- vtok
- vtun
- vudu
- warcft3
- waze
- webex
- wechat
- weibo
- whatsapp
- wii
- windows-azure
- windows-store
- winmx
- winny
- wmstream
- wofkungfu
- wofwarcraft
- wuala
- xbox
- xdcc
- xing
- yahoo
- yahoomail
- yiptv
- youku
- yourfreetunnel
- youtube
- zattoo

**p2p protocol-group** *group\_list*: The supported P2P protocol groups are:

- generic
- anonymous-access
- business

- communicator
  - cloud
  - e-store
  - e-mail
  - e-news
  - internet-privacy
  - filesharing
  - gaming
  - p2p-filesharing
  - p2p-anon-filesharing
  - remote-control
  - social-nw-gaming
  - social-nw-generic
  - social-nw-videoconf
  - standard
  - streaming
- **pop3**
  - **pptp**
  - **rtcp**
  - **rtp**
  - **rtsp**
  - **sdp**
  - **secure-http**
  - **sip**
  - **smtp**
  - **tcp**
  - **tftp**
  - **udp**
  - **wsp**
  - **wtp**

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Use this command to clear ACS analyzer statistics.

**Example**

The following command clears active charging service analyzer information for TCP analyzer:

```
clear active-charging analyzer statistics name tcp
```

## clear active-charging charging-action statistics

Clears ACS charging action statistics.

**Product**

ACS

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear active-charging charging-action statistics [ name charging_acion_name ] [ | { grep grep_options | more } ]
```

**name *charging\_acion\_name***

Clears statistics for the specified charging action.

*charging\_acion\_name* must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to clear active charging action statistics.

**Example**

The following command clears active charging action statistics information for charging action named **pre-paid**:

```
clear active-charging charging-action statistics name pre-paid
```

## clear active-charging content-filtering server-group statistics

Clears statistics for all/a specific CF server group.



---

**Product** CF

---

**Privilege** Security Administrator, Administrator, Operator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **clear active-charging content-filtering server-group statistics** [ **name** *cf\_server\_group\_name* ] [ | { **grep** *grep\_options* | **more** } ]

**name** *cf\_server\_group\_name*

Clears statistics for the specified CF server group.

*cf\_server\_group\_name* must be the name of a CF server group, and must be an alphanumeric string of 1 through 15 characters.

**grep** *grep\_options* | **more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines** Use this command to clear content filtering statistics for CF server groups.

### Example

The following command clears category-based content filtering statistics information for Rulebase named *cf\_rule1*:

```
clear active-charging content-filtering category statistics rulebase name
  cf_rule1
```

## clear active-charging credit-control statistics

Clears credit control statistics.

---

**Product** ACS

---

**Privilege** Security Administrator, Administrator, Operator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear active-charging credit-control statistics [ group cc_group_name |
server { all | ip-address ip_address | name cc_group_name } ]
```

**clear active-charging credit-control statistics**

Clears statistics for all credit control groups.

**group** *cc\_group\_name*

Clears statistics for the specified credit control group.

*cc\_group\_name* must be an alphanumeric string of 1 through 63 characters.

**server** { **all** | **ip-address** *ip\_address* | **name** *cc\_group\_name* }

Clears statistics for the credit control server specified as:

- **all**: for all the Diameter peers and hosts
- **ip-address**: an IP address for the credit control group entered in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation
- **cc\_group\_name**: name of the credit control group server entered as an alphanumeric string of 1 through 127 characters.

**Usage Guidelines**

Use this command to clear credit control statistics.

**Example**

The following command clears statistics information for credit control:

```
clear active-charging credit-control statistics
```

## clear active-charging dns-learnt-ip-addresses

Clears DNS learnt IP address statistics for the DNS Snooping feature.

**Product**

ACS

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear active-charging dns-learnt-ip-addresses statistics sessmgr { all |
instance sessmgr_instance } [ | { grep grep_options | more } ]
```

**sessmgr** { **all** | **instance** *sessmgr\_instance* }

Clears statistics for all or the specified Session Manager (SessMgr) instance.

- **all**: Clears statistics for all SessMgr instances.
- **instance** *sessmgr\_instance*: Clears statistics for the specified SessMgr instance.  
*sessmgr\_instance* must be an integer from 1 through 65535.

### grep *grep\_options* | more

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to clear DNS learnt IP address statistics for the DNS Snooping feature.

On clearing the statistics using this command, only the entries-flushed, entries-replaced, and IP-Overflows statistics are cleared as these are cumulative statistics. Total-entries will not be cleared as it is an instantaneous statistic of the current total entries in that rule line.

### Example

The following command clears all DNS learnt IP address statistics:

```
clear active-charging dns-learnt-ip-addresses statistics sessmgr all
```

## clear active-charging edr-format statistics

Clears ACS statistics for all or a specific Event Data Record (EDR) format.

### Product

ACS

### Privilege

Security Administrator, Administrator, Operator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
clear active-charging edr-format statistics [ name edr_format_name ]
```

#### **name** *edr\_format\_name*

Clears statistics for the specified EDR format.

*edr\_format\_name* must be the name of an EDR format, and must be an alphanumeric string of 1 through 63 characters.



### Important

If an EDR format name is not specified, statistics for all EDR formats are cleared.

**clear active-charging edr-udr-file statistics**

**Usage Guidelines** Use this command to clear the accumulated statistics for the specified EDR format.

**Example**

The following command clears the statistics for all EDR formats:

```
clear active-charging edr-format statistics
```

## clear active-charging edr-udr-file statistics

Clears Event Data Record (EDR) and Usage Data Record (UDR) file related statistics.

**Product** ACS

**Privilege** Security Administrator, Administrator, Operator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `clear active-charging edr-udr-file statistics`

**Usage Guidelines** Use this command to clear EDR and UDR file statistics.

**Example**

The following command clears statistical information for EDR and UDR files:

```
clear active-charging edr-udr-file statistics
```

## clear active-charging firewall statistics

Clears Stateful Firewall statistics.

**Product** PSF

**Privilege** Security Administrator, Administrator, Operator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `clear active-charging firewall statistics [ callid call_id | domain-name domain_name | nat-realm nat_realm_name | protocol { icmp | icmpv6 | ip | ipv6 | other | tcp | udp } | username user_name ] [ acsmgr instance instance_id ] [ | { grep grep_options | more } ]`

**acsmgr instance *instance\_id***

Specifies an ACS Manager instance ID as an integer from 1 through 65535.

**callid *call\_id***

Specifies a call identification number as an eight-byte hexadecimal number.

**domain-name *domain\_name***

Specifies the domain name.

*domain\_name* must be an alphanumeric string of 1 through 127 characters.

**nat-realm *nat\_realm\_name***

Specifies the NAT realm.

*nat\_realm\_name* must be an alphanumeric string of 1 through 31 characters.

**protocol { icmp | ip | other | tcp | udp }**

Specifies a protocol for the statistics.

- **icmp**: ICMPv4
- **icmpv6**
- **ip**: IPv4
- **ipv6**
- **other**: Protocols other than TCP, UDP, and ICMPv4/ICMPv6
- **tcp**
- **udp**

**username *user\_name***

Specifies the user name.

*user\_name* must be an alphanumeric string of 1 through 127 characters.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Use this command to clear Stateful Firewall statistics.

**Example**

The following command clears all Stateful Firewall statistics:

```
clear active-charging firewall statistics
```

## clear active-charging firewall track-list

Clears the list of servers being tracked for involvement in any Denial-of-Service (DOS) attacks.

---

**Product** PSF

---

**Privilege** Security Administrator, Administrator, Operator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `clear active-charging firewall track-list attacking-servers`

---

**Usage Guidelines** Use this command to clear the list of servers being tracked for involvement in any DOS attacks.

### Example

The following command clears the list of servers being tracked for involvement in any DOS attacks:

```
clear active-charging firewall track-list attacking-servers
```

## clear active-charging fw-and-nat policy statistics

Clears statistics for all or a specific Firewall-and-NAT policy.

---

**Product** PSF

NAT

---

**Privilege** Security Administrator, Administrator, Operator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `clear active-charging fw-and-nat policy statistics { all | name policy_name } [ | { grep grep_options | more } ]`

### all

Clears information for all Firewall-and-NAT policies.

**name *policy\_name***

Clears information for the specified Firewall-and-NAT policy.

*policy\_name* must be the name of a Firewall-and-NAT policy, and must be an alphanumeric string of 1 through 63 characters.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to clear statistics for all or a specific firewall-and-NAT policy.

**Example**

The following command clears statistics for the firewall-and-NAT policy named *test123*:

```
clear active-charging fw-and-nat policy statistics name test123
```

## clear active-charging group-of-ruledefs statistics

Clears ACS group of ruledefs statistics.

**Product**

ACS

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear active-charging group-of-ruledefs statistics [ name group_of_ruledefs ] [ | { grep grep_options | more } ]
```

**name *group\_of\_ruledefs***

Clears statistics for the specified group of ruledefs.

*group\_of\_ruledefs* must be the name of a group of ruledefs, and must be an alphanumeric string of 1 through 63 characters.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to clear statistical information related to all or specified Active Charging Service group of ruledefs.

**Example**

The following command clears statistical information related to the group of ruledefs named *ruledef\_group12*:

```
clear active-charging group-of-ruledefs statistics name ruledef_group12
```

## clear active-charging nat statistics

Clears NAT realm statistics.

**Product**

NAT

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear active-charging nat statistics [ nat-realm nat_realm_name ] [ | { grep
grep_options | more } ]
```

**nat statistics**

This command when issued in the local context clears statistics for all NAT realms in all contexts. When issued within a specific context, this command clears statistics for all NAT realms in that context.

**nat-realm *nat\_realm\_name***

This command when issued in the local context clears statistics for the specified NAT realm in all contexts. When issued in a specific context, this command clears statistics for the specified NAT realm in that context.

*nat\_realm\_name*: Specifies name of the NAT realm as an alphanumeric string of 1 through 31 characters.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to clear NAT realm statistics.



**Example**

The following command when issued in the local context, clears NAT realm statistics for NAT realms named *test135* in all contexts:

```
clear active-charging nat statistics nat-realm test135
```

## clear active-charging regex statistics

Clears regular expression (regex) related statistics.

<b>Product</b>	ACS
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<pre>clear active-charging regex statistics ruledef { all   instance instance_number }</pre> <p><b>all</b> Clears all regex-related statistics.</p> <p><b>instance <i>instance_number</i></b> Clears regex-related statistics for specified Session Manager instance. <i>instance_number</i> must be an integer from 1 through 65535.</p>
<b>Usage Guidelines</b>	Use this command to clear regular expression (regex) related statistics.

**Example**

The following command clears all regex-related statistics:

```
clear active-charging regex statistics ruledef all
```

## clear active-charging rulebase statistics

Clears ACS rulebase statistics.

<b>Product</b>	ACS
<b>Privilege</b>	Security Administrator, Administrator, Operator

**clear active-charging ruledef statistics****Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear active-charging rulebase statistics [ name rulebase_name ] [ | { grep
grep_options | more } ]
```

***rulebase\_name***

Clears statistics for the specified ACS rulebase.

*rulebase\_name* must be the name of a rulebase, and must be an alphanumeric string of 1 through 15 characters.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to clear ACS rulebase statistics.

**Example**

The following command clears statistics for the ACS rulebase named *postpaid*:

```
clear active-charging rulebase statistics name postpaid
```

## clear active-charging ruledef statistics

Clears statistics for rule definitions configured in the Active Charging Service (ACS).

**Product**

ACS

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear active-charging ruledef statistics [ charging | firewall | name
ruledef_name | tpo ] [ | { grep grep_options | more } ]
```

**charging**

Clears statistics for all charging ruledefs.

**firewall**

Clears statistics for all Stateful Firewall ruledefs.

**name *ruledef\_name***

Clears statistics for the specified ruledef.

*ruledef\_name* must be the name of a ruledef, and must be an alphanumeric string of 1 through 63 characters.

**tpo****Important**

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to clear ACS ruledef statistics.

**Example**

The following command clears all ruledef statistics:

```
clear active-charging ruledef statistics
```

## clear active-charging subsystem

Clears all ACS subsystem information.

**Product**

ACS

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear active-charging subsystem
```

**Usage Guidelines**

Use this command to clear all ACS subsystem information.

**Example**

The following command clears all ACS subsystem information:

```
clear active-charging subsystem
```

## clear active-charging tcp-proxy statistics

Clears ACS TCP Proxy statistics.

**Product**

ACS

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear active-charging tcp-proxy statistics [ all | ip-layer | proxy-fac
| rulebase rulebase_name | socket-migration | tcp-layer ]
```

**all**

Clears all TCP Proxy statistics.

**ip-layer**

Clears TCP Proxy statistics for IP layer.

**proxy-fac**

Clears TCP Proxy Flow Admission Control statistics.

**rulebase *rulebase\_name***

Clears TCP Proxy statistics for the specified rulebase.

*rulebase\_name* must be the name of a rulebase, and must be an alphanumeric string of 1 through 63 characters.

**socket-migration**

Clears TCP Proxy Socket Migration related statistics.

**tcp-layer**

Clears TCP Proxy statistics for TCP layer.

**Usage Guidelines**

Use this command to clear TCP Proxy statistics.

**Example**

The following command clears TCP Proxy statistics for the rulebase named *test14*:

```
clear active-charging tcp-proxy statistics rulebase test14
```

## clear active-charging tethering-detection statistics

Clears statistics pertaining to the Tethering Detection feature.

<b>Product</b>	ACS
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<b>clear active-charging tethering-detection statistics</b>
<b>Usage Guidelines</b>	Use this command to clear statistics pertaining to the Tethering Detection feature.

## clear active-charging tpo policy statistics

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

## clear active-charging tpo profile statistics

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

## clear active-charging blockedlisting statistics

Clears URL Blockedlisting feature related statistics.

<b>Product</b>	CF
<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	In releases prior to StarOS 21.26:

```
clear active-charging url-blacklisting statistics [ rulebase name
rulebase_name ] [ | { grep grep_options | more } ]
```

From StarOS 21.26 and later releases:

```
clear active-charging url-blockedlisting statistics [ rulebase name
rulebase_name ] [ | { grep grep_options | more } ]
```

#### **rulebase name** *rulebase\_name*

Clears URL blockedlisting information for the specified rulebase.

*rulebase\_name* must be the name of a rulebase, and must be an alphanumeric string of 1 through 63 characters.

#### **grep** *grep\_options* | **more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to clear URL Blockedlistingfeature related statistics, optionally for a specific rulebase.

### Example

In releases prior to StarOS 21.26:

The following command clears URL Blacklisting feature related statistics for *rulebase12*:

```
clear active-charging url-blacklisting statistics rulebase name rulebase12
```

From StarOS 21.26 and later releases:

The following command clears URL Blockedlisting feature related statistics for rulebase12 :

```
clear active-charging url-blockedlisting statistics rulebase name rulebase12
```

## clear active-charging video detailed-statistics

Resets the detailed statistics for TCP video flows.



### Important

In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

### Product

MVG

### Privilege

Security Administrator, Administrator, Operator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `clear active-charging video detailed-statistics`

---

**Usage Guidelines** Use this command to reset the detailed statistics for TCP video flows.

### Example

The following command resets the detailed statistics for TCP video flows:

```
clear active-charging video detailed-statistics
```

## clear administrator

Ends the session of an administrative user specified by either user name or session ID.

---

**Product** All

---

**Privilege** Security Administrator, Administrator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `clear administrator { name user_name | session id id_num }`

**name *user\_name***

Identifies the user name of the administrative user.

**session id *id\_num***

Identifies the ID number of the administrative user session as displayed in the output of the **show administrators session id** command.

---

**Usage Guidelines** This command is used to terminate command line interface sessions for other administrative users.

### Example

The following command ends the session of the administrative user identified as *user1*:

```
clear administrator name user1
```

The following command ends the session of the administrative user with the session ID of 3:

```
clear administrator session id 3
```

# clear alarm

Clears outstanding alarm conditions

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator, Operator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
clear alarm { all | chassis | id num | port slot/port | slot slot }
```

**all**

Clear all outstanding alarms.

**chassis**

Clears chassis-wide and fan tray alarms.

**id *num***

Clears a specific alarm by its internal alarm ID. *num* is the internal alarm identification number.

**port *slot/port***

Clears alarms for the specified port. *slot/port* is the card slot and port on the card for which to clear alarms.

**slot *slot***

Clears alarms for the specified slot. *slot* is the card slot for which to clear alarms.

---

**Usage Guidelines**

Use this command to clear outstanding alarm conditions.

**Example**

To clear all outstanding alarms, use the following command:

```
clear alarm all
```

To clear all alarms for slot 7, enter the following command:

```
clear alarm slot 7
```



## clear alcap

Clears the Access Link Control Application Part (ALCAP) session statistics of an ALCAP service associated with a Home-NodeB Gateway (HNB-GW) service instance configured and running on a system.

**Product** HNB-GW

**Privilege** Operator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **clear alcap statistics** [ **alcap-service** *alcap\_svc\_name* [ **aal2-node** *aal2\_node\_name* [ **aal2-path** *aal2\_path\_id* ] ] ]

**alcap-service** *alcap\_svc\_name*

Specifies the name of the ALCAP service for which statistics are to be cleared.

**aal2-node** *aal2-node*

Specifies the name of the ATM Adaptation Layer 2 (AAL2) node for which ALCAP service statistics will be cleared.

**aal2-path** *aal2\_path\_id*

Specifies the identity number of the AAL2 path on a specific ATM Adaptation Layer 2 (AAL2) node for which ALCAP service statistics will be cleared.

**Usage Guidelines** This command is used to clear the sessions statistics and counters for ALCAP service.

### Example

The following command clears the service session statistics of ALCAP service named as *alcap\_hnb\_svc1*:

```
clear alcap statistics alcap-service alcap_hnb_svc1
```

## clear asngw-service

Clears the service session statistics for an Access Service Network Gateway (ASN-GW) service specified by either service name or trusted peer address.

**Product** ASN-GW

**Privilege** Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear asngw-service statistics [ name svc_name | peer-address ip_address ]
```

**name *svc\_name***

Identifies the name of the ASN-GW service for which statistics will be cleared. *svc\_name* must be an alphanumeric string of 1 through 63 characters.

**peer-address *ip\_address***

Identifies the IP address of the ASN-GW peer for which service statistics will be cleared. *ip\_address* must be entered in IPv4 dotted-decimal notation.

**Usage Guidelines**

This command is used to terminate command line interface sessions for ASN GW services.

**Example**

The following command clears the service session statistics of the ASN-GW service named *aasn\_svc1*:

```
clear asngw-service statistics name asn_svc1
```

## clear asnpc-service

Clears the service session statistics of an ASN paging controller service specified by either ASN PC service name or trusted paging controller peer address.

**Product**

ASN-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear asnpc-service statistics [ name svc_name | peer-address ip_address ]
```

**name *svc\_name***

Identifies the name of the ASN PC service for which session statistics will be cleared. *svc\_name* must be an alphanumeric string of 1 through 63 characters.

**peer-address *ip\_address***

Identifies the IP address of the ASN PC peer for which all service statistics will be cleared. *ip\_address* must be entered in IPv4 dotted-decimal notation.

**Usage Guidelines**

This command is used to terminate command line interface sessions for ASN PC services.

**Example**

The following command clears the service session statistics of ASN PC service named as *asnpc\_svc1*:

```
clear asnpc-service statistics name asnpc_svc1
```

## clear apn statistics

Deletes all previously gathered statistics for either a specific Access Point Name (APN) or all APNs configured with the given context.

**Product**

GGSN  
P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear apn statistics [ name apn_name | smgr-instance instance ] [ | { grep  
grep_options | more } ]
```

**name *apn\_name***

Specifies the name of a specific APN configured in the context for which to clear statistics. *apn\_name* is the name of the APN expressed as an alphanumeric string of 1 through 63 characters that is case sensitive.

**smgr-instance *instance***

Specifies a particular Sessmgr instance in the context for which to clear APN statistics. *instance* must be an integer from 1 to 4294967295.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Statistics for a single APN can be cleared using the **name** keyword. Statistics for all APNs in the context can be deleted by entering the command with no keywords.

If this command is executed from within the local context with no keywords, statistics will be cleared for every APN configured on the system regardless of context. In addition, if the **name** keyword is used when

executing from within the local context, statistics for all APNs configured with the specified name will be cleared regardless of context.

### Example

The following command clears statistics for an APN called *isp1*:

```
clear apn statistics name isp1
```

## clear bcmcs statistics

Clears Broadcast Multicast Service (BCMCS) statistics.

<b>Product</b>	PDSN
<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `clear bcmcs statistics [ pdsn-service service_name ]`

### **pdsn-service service\_name**

Specifies a specific PDSN service for which to clear BCMCS-specific statistics. This value must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines** Use this command to clear accumulated BCMCS statistics. You may specify an individual PDSN or peer to selectively clear statistics.

### Example

```
clear bcmcs statistics
clear bcmcs statistics pdsn-service service_name
```

## clear blockedlisted-gtpu-bind- address

Clears the GTP-U loopback address blockedlisted by a specific radio network controller (RNC) as defined for a specific IuPS Service configuration.

<b>Product</b>	SGSN
<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

In releases prior to StarOS 21.26:

```
clear blacklisted-gtpu-bind-address ip_address rnc-id rnc_id mcc mcc_num mnc
mnc_num iups-service name
```

From StarOS 21.26 and later releases:

```
clear blockedlisted-gtpu-bind-address ip_address rnc-id rnc_id mcc mcc_num mnc
mnc_num iups-service name
```

### *ip\_address*

Specifies the IP loopback address that has been blockedlisted in IPv4 dotted-decimal notation. This loopback address was originally defined with the **associate-gtpu-bind-address** command in the Radio-Network-Controller Configuration mode of the IuPS Service.

### Usage Guidelines

This command enables this loopback address to be used for future RAB-assignment requests.

In releases prior to StarOS 21.26:

### Example

```
clear blacklisted-gtpu-bind-address 1.1.1.1 rnc-id 2 mcc 123 mnc 321
iups-service iups1
```

## clear bssap+ statistics

Clears the BSSAP+ protocol (base station subsystem GPRS protocol) statistics collected for the Gs interface between the SGSN and the MSC/VLR.

### Product

SGSN

### Privilege

Security Administrator, Administrator, Operator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
clear bssap+ statistics [ gs-service gs_svc_name ] [ vlr { isdn-number
ISDN_Num | name vlr_name } ] [ | { grep grep_options | more } ]
```

### **gs-service** *gs\_svc\_name*

Specifies the name of a preconfigured Gs service handling BSSAP+ information as an alphanumeric string of 1 through 63 characters that is case sensitive.

**vlr** { **isdn-number** *ISDN\_Num* | **name** *vlr\_name* }

Specifies a VLR (by ISDN number or name) handling BSSAP+ information.

**isdn-number** *ISDN\_num* is the configured E.164-type ISDN number for the VLR. Enter a numerical string of 1 to 15 digits.

**name** *vlr\_name* is the configured name of the VLR entered as an alphanumeric string of 1 through 63 characters.

### Usage Guidelines

Use this command to delete or clear collected BSSAP+ protocol statistics for the entire SGSN or for a specified Gs interface. Using the keywords of this command, the interface can be identified by defining a specific VLR connected to the SGSN or by identifying the Gs service to which the interface has been configured.

### Example

The following command clears the BSSAP+ statistics collected for the Gs interface configured for the Gs service named *gssvc1*.

```
clear bssap+ statistics gs-service gssvc1
```

## clear bssgp statistics

Clears collected BSSGP protocol (base station subsystem GPRS protocol) statistics for traffic between the base station subsystem (BSS) and the SGSN.

### Product

SGSN

### Privilege

Security Administrator, Administrator, Operator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
clear bssgp statistics [ gprs-service gprs_svc_name | nse nse_id [ bvc bvc_id ] ] [ | { grep grep_options | more } ]
```

#### **gprs-service** *gprs\_svc\_name*

Specifies the name of a preconfigured GPRS service for which the BSSGP statistics have been collected as an alphanumeric string of 1 through 63 characters that is case sensitive.

#### **nse** *nse\_ID*

Clears the BSSGP statistics collected for the network service entity (NSE) specified as an integer from 0 through 65535.

#### **bvc** *bvc\_ID*

Enter this keyword to clear the BSSGP statistics collected for the identified BSSGP virtual connection (BVC) specified as n integer from 0 through 65000.

**grep** *grep\_options* | **more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to clear the BSSGP statistics for a particular GPRS service or NSEI.

**Example**

The following command deletes the collected BSSGP statistics for the GPRS service named *gprs1*.

```
clear bssgp statistics gprs-service gprs1
```

## clear bulkstats

Clears counters and accumulated bulk statistics related information.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear bulkstats { counters | data }
```

**counters**

Clears the counters maintained by the system's "bulkstats" facility.

**data**

Clears any accumulated data that has not been transferred. This includes any "completed" files that have not been successfully transferred.

**Usage Guidelines**

Once bulk statistics collection is enabled, the system stores the information until the specified transfer criteria is met or until a manual transfer is initiated. The system maintains counters for the "bulkstats" software facility. (Refer to the **data** keyword for the **show bulkstats** command for information on viewing the counters.)

This command can be used to delete bulk statistics information that has been collected but not transferred and/or to clear the counters that have been maintained.

**Example**

The following command clears bulk statistics-related counters:

```
clear bulkstats counters
```

## clear ca-certificate-list statistics

This command clears CA-Certificate-List with matched count.

**Product** ePDG

**Privilege** Security Administrator, Administrator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `clear ca-certificate-list statistics`

**Usage Guidelines** Use this command to clears CA-Certificate-List with matched count.

### Example

The following command clears CA-Certificate-List with matched count:

```
clear ca-certificate-list statistics
```

## clear cae-group statistics server

This command resets the discardable statistics, which are the Hit Count, Timeout Consecutive (Cumulative), and Last Failure statistics, for all CAEs or for a specific CAE. The CAE (Content Adaptation Engine) is an optional component of the Mobile Videoscape.



### Important

In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

**Product** MVG

**Privilege** Security Administrator, Administrator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `clear cae-group statistics server { all | name cae_name }`

### all

Resets the discardable statistics for all CAEs.



**namecae\_name**

Specifies the name of a CAE.

**Usage Guidelines**

Use this command to reset the discardable statistics for all CAEs or for a specific CAE. This command must be issued in the same context in which the associated CAE group is defined.

**Example**

The following command clears the discardable statistics for the CAE named *server\_1*:

```
clear cae-group statistics server name server_1
```

## clear call-home statistics

Clears Cisco Call Home feature statistics.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear call-home statistics
```

**Usage Guidelines**

Use this command to reset the statistics for all Call Home events.

**Example**

The following command clears the discardable statistics for the Call Home feature:

```
clear call-home statistics
```

## clear cdr statistics

Clears statistics related to charging data records (CDRMOD).

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `clear cdr statistics`

**Usage Guidelines** Use this command to reset the statistics for charging data records.

**Example**

The following command clears the discardable statistics related to CDRs:

```
clear cdr statistics
```

## clear cli history

Clears the tracking history of command line interface (CLI) command usage.

---

**Product** All

---

**Privilege** Security Administrator, Administrator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `clear cli history`

**Usage Guidelines** Use this command to clear the tracking history of CLI command usage.

**Example**

The following command clears the CLI history:

```
clear cli history
```

## clear cmp cert-name

Clears information stored for the specified IPsec Certificate Management Protocol v2 (CMPv2) certificate.

---

**Product** All products supporting IPsec CMPv2 features




---

**Important**

This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

---



---

**Privilege** Security Administrator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

**clear cmp cert-name** *cert\_name*

**cert-name** *cert\_name*

Specifies the CMP certificate name as an alphanumeric string of 1 through 129 characters.

---

**Usage Guidelines**

Use this command to clear the information for the specified CMP certificate.

**Example**

The following command clears information for the specified CMP certificate:

```
clear cmp cert-name certificate01
```

## clear cmp statistics

Clears statistics for IPsec Certificate Management Protocol v2 (CMPv2) certificates.

---

**Product**

All products supporting IPsec CMPv2 features




---

**Important**

This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

---



---

**Privilege**

Security Administrator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

**clear cmp statistics**

---

**Usage Guidelines**

Use this command to clear statistics for IPsec CMPv2 certificates.

**Example**

The following command clears CMPv2 certificates:

```
clear cmp statistics
```

# clear confdmgr confd cdb

Erases the configuration in the ConfD Database (CDB) which is an XML database used by ConfD to store configuration objects. StarOS accesses the database via ConfD-supplied APIs.



**Caution** Clearing the CDB is a terminal operation. The CDB must be repopulated afterwards.



**Note** The CDB cannot be erased unless the Context Configuration mode **no server confd** command is run in the local context to disable ConfD and NETCONF protocol support.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `clear confdmgr confd cdb [ -noconfirm ]`

### **-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

### **Usage Guidelines**

This command clears the CDB of all existing entries. Before the command executes you are prompted as follows:

```
About to delete the ConfD configuration database
The running configuration is NOT affected.
Are you sure? [Yes|No]:
```



**Important** If you re-enable **server confd** after running **clear confd**, there will be no default CDB to support NETCONF protocol and associated API exchanges.

### **Example**

The following command erases the entries in the CDB:

```
clear confdmgr confd cdb
```

# clear confdmgr statistics

Clears everything listed in the "Statistics" section of the output of the **show confdmgr** command.

---

**Product** All

---

**Privilege** Security Administrator, Administrator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **clear confdmgr statistics**

## **statistics**

Clears everything listed in the "Statistics" section of the output of the **show confdmgr** command, including:

- Triggers
- Notifications
- Successful notifications
- Failed notifications
- Unexpected

---

**Usage Guidelines** This command clears operational statistics associated with the ConfD engine and NETCONF protocol.

## **Example**

The following command clears confdmgr statistics:

```
clear cnfdmgr statistics
```

# clear config

Replaces the active configuration source file with an empty configuration where possible.

---

**Product** All

---

**Privilege** Security Administrator, Administrator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `clear config [ -noconfirm ]`

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

---

**Usage Guidelines** This command clears the current configuration when a complete overwrite is desired or if it is necessary to start from an empty configuration.



**Important**

Clearing the configuration will cause the active configuration source file to be empty and of no use in configuring the system to an active state providing service.



**Important**

This command should only be performed on configurations that have been previously backed up for easy restoration.

---

**Example**

The following command clears the active configuration after the user provides confirmation of the request.

```
clear config
```

The following command clears the active configuration source file immediately with no user confirmation.

```
clear config -noconfirm
```

## clear congestion-control statistics

Clears the congestion control statistics for all instances of the specified manager type.

---

**Product** All

---

**Privilege** Security Administrator, Administrator, Operator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `clear congestion-control statistics { allmgr | asngwmgr | asnpcmgr | bindmux | gtpcmgr | hamgr | hnbmgr | imsimgr | ipsecmgr | ipsgmgr | imsimgr | l2tpmgr }`

**allmgr**

Clears the statistics for all A11 Manager instances.

**asn timer**

Clears the statistics for all ASN GW Manager instances

**asnpcmgr**

Clears the statistics for all ASN PC-LR Manager instances

**bindmux**

Clears the statistics for all IPCF BindMux-Demux Manager instances.

**gtpcmgr**

Clears the statistics for all GTPC Manager instances.

**hamgr**

Clears the statistics for all HA Manager instances.

**hnbmgr****Important**

---

In Release 20 and later, HNBDGW is not supported. This keyword must not be used for HNBDGW in Release 20 and later. For more information, contact your Cisco account representative.

---

Clears the statistics for all HNB Manager instances.

**imsimgr**

Clears the statistics for all IMSI Manager instances.

**ipsecmgr**

Clears the statistics for all IPSEC Manager instances.

**ipsgmgr**

Clears the statistics for all IPSG Manager instances.

**l2tpmgr**

Clears the statistics for all L2TP Manager instances.

**Usage Guidelines**

Use this command to statistics for all instances of the specified manager.

**Important**

---

When this command is issued in any context other than the local context, only instances of the specified manager for the current context have the statistics cleared. When the current context is the local context, all instances of the specified manager type in all contexts have the statistics cleared.

---

**Example**

The following command clears the statistics for all instances of the All manger:

```
clear congestion-control statistics allmgr
```

## clear content-filtering category statistics

Clears the Category-based Content Filtering application statistics.

<b>Product</b>	CF
<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<pre>clear content-filtering category statistics [ facility srdmgr instance instance_value ]</pre> <p><b>facility srdmgr instance <i>instance_value</i></b></p> <p>Clears logged events for the specified SRDB Manager instance. <i>instance_value</i> must be an integer from 1 through 8. In release 9.0 and later, <i>instance_value</i> must be an integer from 1 through 10000.</p>
<b>Usage Guidelines</b>	Use this command to clear all Category-based Content Filtering application statistics, or statistics for a specific SRDB Manager instance.

**Example**

The following command clears all Category-based Content Filtering application statistics:

```
clear content-filtering category statistics
```

## clear crash

Removes a specific crash file or all crash files.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec



The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

**clear crash [ list | number *crash\_num* ]**

**list | number *crash\_num***

**list:** removes all crash files.

**number *crash\_num*:** removes only the crash file specified as an integer from 1 through 30.

---

**Usage Guidelines**

Clear crashes for general maintenance activities in cleaning out old, unused, or files which are of no importance.

**Example**

The following will remove all crash files.

```
clear crash list
```

The following command will remove only crash file 27.

```
clear crash numer 27
```

## clear credit-control statistics

Clears credit control statistics.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator, Operator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

**clear credit-control statistics cc-service *cc\_service\_name***

**cc-service *cc\_service\_name***

Specifies an existing Credit Control service name as an alphanumeric string of 1 through 63 characters.

---

**Usage Guidelines**

Use this command to clear active credit control statistics.

**Example**

The following command clears the configured credit control statistics for a service named *service1*:

```
clear credit-control statistics cc-service service1
```

# clear crypto

Clears crypto associations or crypto statistics.

---

## Product

ePDG  
PDSN  
HA  
GGSN  
PDG/TTG  
PDIF  
SCM

---

## Privilege

Security Administrator, Administrator, Operator

---

## Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

## Syntax Description

```
clear crypto { isakmp [ tag map_name | peer peer_ip ] | security-association
  { counters tag map_name [ tx | rx ] | tag map_name | peer peer_ip[ sa-index
numbr ] } | statistics { ikev2 } [service-ip-address ip-address | service-name
name ] }
```

### **isakmp** [ **tag** *map\_name* | **peer** *peer\_ip* ]

When no keywords are specified, this command clears all of the ISAKMP security associations for the current context.

**tag** *map\_name*: Clears the ISAKMP SAs for the specified crypto map. *map\_name* is the name of an existing crypto map.

**peer** *peer\_ip*: Deletes the ISAKMP SAs for the specified peer. *peer\_ip* must be entered in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

### **security-association** { **counters** **map** *map\_name* [ **tx** | **rx** ] | **tag** *map\_name* | **peer** *peer\_ip* [ **sa-index** *numbr* ] }

**counters** **tag** *map\_name* [ **tx** | **rx** ]: Resets the counters for the specified crypto map. *map\_name* is the name of an existing crypto map. **tx** specifies that only the transmit SA counters are reset. **rx** specifies that only the receive SA counters are reset. If neither **tx** or **rx** are specified, both transmit and receive SA counters are reset.

**tag** *map\_name*: Tears down a Security Association (SA) for the specified crypto map. *map\_name* is the name of an existing crypto map.

**peer** *peer\_ip*: Clears the SAs for all tunnels who have the peer at the specified IP address. *peer\_ip* must be entered in Pv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

[ **sa-index** *numbr*: Clears a specified security association. *numbr* is an integer from 1 to 4 for releases prior to 15.0, or 1 to 5 for release 15.0 and higher.



**Caution** Modification(s) to an existing crypto map and/or ISAKMP policy configuration will not take effect until the related security association has been cleared.

**statistics ikev2 [ service-ip-address *ip-address* | service-name *name* ]**

**ikev2:** Clears global IKEv2 statistics for the current context.

**service-ip-address *ip-address*:** Clears statistics for the specified service-ip address. **service-name *name*:** Clears statistics for the specified service name.

### Usage Guidelines

Clear SAs and apply changes to the crypto map or clear the crypto statistics for this context.

### Example

The following clears all IKEv2 crypto statistics for the current context:

```
clear crypto statistics ikev2
```

## clear cs-network statistics



**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Clears the HNB-Circuit Switched (CS) network service associated for an HNB-GW service instance.

### Product

HNB-GW

### Privilege

Operator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

**clear cs-network statistics [ name *cs\_svc\_name* | ranap-only | rtp-only | sccp-only ]**

**name *cs\_svc\_name***

Clears the session statistics for an HNB-CS Network service name configured and running on this system. *cs\_svc\_name* must be an alphanumeric string of 1 through 63 characters.

### ranap-only

Clears the session statistics limited to Radio Access Network Application Protocol (RANAP) traffic only for the specified HNB-CS Network service.

**rtp-only**

Clears the session statistics limited to Real Time Protocol (RTP) traffic only for the specified HNB-CS Network service.

**sccp-only**

Clears the session statistics limited to Signaling Connection Control Part (SCCP) traffic only for the specified HNB-CS Network service.

**Usage Guidelines**

Use this command to clear the session statistics for overall session or in selected part of user session for HNB-CS Network services configured and running on a system.

**Example**

The following command clears the session statistics for RANAP part of session for the HNB-CS Network service *hnb\_CS\_1*:

```
clear cs-network statistics name hnb_CS_1 ranap-only
```

## clear dhcp statistics

Deletes all previously gathered statistics for either a specific or all DHCP IPv4 servers configured within the given context.

**Product**

GGSN  
ASN-GW  
P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear dhcp statistics [ dhcp-service svc_name | server ip_address ]
```

**dhcp-service *svc\_name***

Specifies the name of a specific DHCP service for which to clear statistics as an alphanumeric string of 1 through 63 characters that is case sensitive.

**server *ip\_address***

Specifies the IP address of a DHCP server in IPv4 dotted-decimal notation as configured in the context for which to clear statistics.

**Usage Guidelines**

Statistics for a single server can be cleared using the **server** keyword. Statistics for all DHCP servers in the context can be deleted by entering the command with no keywords.

This command can be executed from any context configured on the system.

If this command is executed from within the local context with no keywords, statistics will be cleared for every DHCP server configured on the system regardless of context. In addition, if the server keyword is used when executing from within the local context, statistics for all DHCP servers configured with the specified name will be cleared regardless of context.

**Example**

The following command clears statistics for all configured DHCP servers within the context:

```
clear dhcp statistics
```

## clear dhcpv6 statistics

Deletes all previously gathered statistics for either a specific or all DHCP IPv6 (DHCPv6) servers configured within the given context.

**Product**

ASN-GW  
GGSN  
P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear dhcpv6 statistics [ server ipv6_address | service svc_name ]
```

**server ipv6\_address**

Specifies the IP address of a DHCP server in IPv6 colon-separated-hexadecimal notation as configured in the context for which to clear statistics.

**service svc\_name**

Specifies the name of a specific DHCPv6 service for which to clear statistics as an alphanumeric string of 1 through 63 characters that is case sensitive.

**Usage Guidelines**

Statistics for a single server can be cleared using the **server** keyword. Statistics for all DHCPv6 servers in the context can be deleted by entering the command with no keywords.

This command can be executed from any context configured on the system.

If this command is executed from within the local context with no keywords, statistics will be cleared for every DHCPv6 server configured on the system regardless of context. In addition, if the server keyword is used when executing from within the local context, statistics for all DHCPv6 servers configured with the specified name will be cleared regardless of context.

### Example

The following command clears statistics for all configured DHCPv6 servers within the context:

```
clear dhcpv6 statistics
```

## clear diameter aaa-statistics

Clears Diameter AAA statistics.

### Product

All

### Privilege

Security Administrator, Administrator, Inspector, Operator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
clear diameter aaa-statistics [ all | debug-info | group aaa_group | server diameter_server ] [ | { grep grep_options | more } ]
```

#### **all**

Clears all Diameter server statistics.

#### **debug-info**

Clears Diameter debug statistics.

#### **group** *aaa\_group*

Clears Diameter server statistics for the specified AAA group.

*aaa\_group* must be the name of a AAA server group, and must be an alphanumeric string of 1 through 64 characters.

#### **server** *diameter\_server*

Clears Diameter server statistics for the specified Diameter server.

*diameter\_server* must be an alphanumeric string of 1 through 64 characters.

#### **grep** *grep\_options* | **more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines** Use this command to clear Diameter AAA statistics.

### Example

The following command clears Diameter server statistics for the specified AAA group:

```
clear diameter aaa-statistics group aaagroup3
```

## clear diameter route

Clears the Diameter routes in the Database.

<b>Product</b>	ASN GW ePDG GGSN HA HSGW IPSG MME PDG/TTG PDSN P-GW SCM SGSN S-GW
----------------	---

<b>Privilege</b>	Security Administrator, Administrator, Operator
------------------	---

<b>Command Modes</b>	Exec  The following prompt is displayed in the Exec mode: [local]host_name#
----------------------	--

<b>Syntax Description</b>	<b>clear diameter route dynamic</b> [ <b>endpoint</b> <i>endpoint_name</i>   <b>peer</b> <i>peer_name</i>   <b>facility</b> { <b>aaamgr</b>   <b>sessmgr</b> } [ <b>instance</b> <i>instance_number</i> ] ] [   { <b>grep</b> <i>grep_options</i>   <b>more</b> } ]
---------------------------	---

### dynamic

Clears all dynamic routes under all the Diameter endpoints.

**endpoint *endpoint\_name***

Clears the dynamic routes for the specified endpoint.

*endpoint\_name* must be the name of a Diameter endpoint, and must be an alphanumeric string of 1 through 63 characters.

**peer *peer\_name***

Clears the dynamic routes for the specified peer.

*peer\_name* must be an alphanumeric string of 1 through 63 characters.

**facility { *aaamgr* | *sessmgr* } [ instance *instance\_number* ]**

Clears the dynamic routes for the specified facility – AAA Manager or Session Manager.

Specify the instance number to clear the dynamic routes for a particular facility's instance. The *instance\_number* must be an integer from 1 through 99999.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to clear the Diameter routing tables that gets added in the system whenever messages are routed through the Diameter proxy/Diabase. These message remain in the system for a long period.

The user has the flexibility to clear the route based on any combination of these keyword options. Running the command **clear diameter route dynamic endpoint *endpoint-name* peer *peer-name*** will result in flushing of the routes that match both endpoint and peer value. Similarly, with this CLI command "**clear diameter route dynamic endpoint *endpoint-name* peer *peer-name* facility { *aaamgr* | *sessmgr* } instance *instance\_number***", the routes in a particular facility with the specified endpoint and peer name can be deleted.

**Example**

The following command clears all dynamic Diameter routes for the specified peer:

```
clear diameter route dynamic peer p1
```

## clear diameter statistics

Clears the Diameter statistics.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:



```
[local]host_name#
```

---

**Syntax Description**

```
clear diameter statistics [ [ proxy ] endpoint endpoint_name [ peer-host
host_id [ peer-realm realm_id ] ] ] [ | { grep grep_options | more } ]
```

**endpoint *endpoint\_name***

Clears statistics for the specified endpoint.

*endpoint\_name* must be the name of a diameter endpoint, and must be an alphanumeric string of 1 through 63 characters.

**proxy**

Clears proxy related statistics.

**peer-host *host\_id***

Clears statistics for the specified Diameter peer host ID.

*host\_id* must be an alphanumeric string of 1 through 255 characters.

**peer-realm *realm\_id***

Clears statistics for the specified Diameter peer realm.

*realm\_id* must be an alphanumeric string of 1 through 127 characters.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Use this command to clear Diameter statistics.

**Example**

The following command clears all Diameter statistics for the specified endpoint:

```
clear diameter statistics endpoint endpt345
```

## clear diameter-service

Clears information pertaining to configured Diameter services.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator, Operator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
clear diameter-service { eap { all | session-id session_id } | lte-s6b { all | session-id session_id } | mbms { bearer-contexts { all | bmsc-bearer-service name service_name } | ue-context { all | bmsc-bearer-service name service_name } } | statistics name service_name [ vpn-name vpn context_name ] }
```

#### **eap** { **all** | **session-id** *session\_id* }

Clears subscribers from the EAP interface.

**all**: Clears all subscribers.

**session-id** *session\_id*: Clears a call for the session ID specified as an alphanumeric string of 1 through 63 characters.

#### **lte-s6b** { **all** | **session-id** *session\_id* }

Clears subscribers from the S6b interface.

**all**: Clears all subscribers.

**session-id** *session\_id*: Clears a call for the session ID specified as an alphanumeric string of 1 through 63 characters.

#### **lte-sta** { **all** | **session-id** *session\_id* }

Clears subscribers from STa interface.

**all**: Clears all subscribers.

**session-id** *session\_id*: Clears a call for the session ID specified as an alphanumeric string of 1 through 63 characters.

#### **mbms** { **bearer-contexts** { **all** | **bmsc-bearer-service** **name** *service\_name* } | **ue-context** { **all** | **bmsc-bearer-service** **name** *service\_name* } }

Clears information from the SGSN-APP interface.

**bearer-contexts** { **all** | **bmsc-bearer-service** **name** *service\_name* }: Clears information from the bearer-context gmb-interface.

**all**: Clears all subscribers.

**bmsc-bearer-service** **name** *service\_name* }: Specifies the name of a bmsc-bearer-service as an alphanumeric string of 1 through 63 characters.

**ue-context** { **all** | **bmsc-bearer-service** **name** *service\_name* } : Clear information UE context for gmb-interface.

**all**: Clears all subscribers.

**bmsc-bearer-service** **name** *service\_name* } : Specifies the name of a bmsc-bearer-service as an alphanumeric string of 1 through 63 characters.

**service\_name**

*service\_name* must be a name of a Diameter service expressed as an alphanumeric string of 1 through 63 characters.

**statistics name service\_name [ vpn-name vpn\_context\_name ]**

Clears the Diameter service associated with the specified statistics.

**name** *service\_name*: Specifies the name of a Diameter service as an alphanumeric string of 1 through 63 characters.

**vpn-name** *vpn\_context\_name*: Clears statistics for the vpn-context name specified as an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to clear information pertaining to configured Diameter services.

**Example**

The following command clears Diameter service information for all subscribers associated with EAP interface:

```
clear diameter-service eap all
```

## clear diameter tps-statistics

Clears Diameter Transactions Per Second (TPS) statistics information.

**Product**

ePDG  
P-GW  
SAEGW  
S-GW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear diameter tps-statistics application { auth-eap | e2 | gmb | gx |
gy | rf | s6a | s6b | sgmb | sta | swm } | endpoint endpoint_name [ | {
grep grep_options | more } ]
```

**endpoint endpoint\_name**

Clears the TPS KPI information only for the endpoint specified as a string of size ranging from 1 through 255 characters.

**Important**

The Diameter Endpoints configured on ASR 5500 platform are not shared between various Diameter applications. For example, Gx and Gy should have separate Diameter endpoints configured.

**application { auth-eap | e2 | gmb | gx | gy | rf | s6a | s6b | sgmb | sta | swm }**

Clears the TPS KPI information only for the specified Diameter application.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to clear both historical as well as cumulative KPIs for Session and Network Initiated Setup/Teardown events. For example, if this clear CLI command is invoked at time 2:31:20, then all KPI information pegged till time "2:31:20" is cleared.

**Example**

The following command clears Diameter TPS statistics for the endpoint named *edp1*:

```
clear diameter tps-statistics endpoint edp1
```

## clear dns-client

Clears DNS cache and/or statistics for a specified DNS client.

**Product**

SCM

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear dns-client name { cache [ query-name name | query-type { A | AAAA | NAPTR | SRV } ] | statistics }
```

**dns-client *name***

Specifies the name of an existing DNS client whose cache and/or statistics are being cleared as an alphanumeric string of 1 through 255 characters.

**cache** [ **query-name** *name* | **query-type** { **A** | **AAAA** | **NAPTR** | **SRV** } ]

Specifies that the cache for the defined DNS client is to be cleared.

**query-name** *name*: Filters DNS results based on the domain name. The name is an alphanumeric string of 1 through 255 characters. that is the domain name used to perform the DNS query. This name is different from the actual domain name which is resolved. For example, to resolve the SIP server for *service.com*, the query name is *\_sip.\_udp.service.com* and the query type is **SRV**.

**query-type**:

- **A**: Filters DNS results based on domain IP address records (A records).
- **AAAA**: Filters DNS results based on AAAA records (AAAA resource records).
- **NAPTR**: Filters DNS results based on Name Authority Pointer records.
- **SRV**: Filters DNS results based on service host records (SRV records).

**statistics**

Specifies that statistics for the defined DNS client are to be cleared.

#### Usage Guidelines

Use this command to clear DNS cache and/or statistics for a specified DNS client.

#### Example

The following command clears statistics for a DNS client named *domain1.com*:

```
clear dns-client domain1.com statistics
```

## clear dns-proxy statistics

Clears all DNS proxy statistics.

#### Product

SCM

#### Privilege

Security Administrator, Administrator, Operator

#### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

#### Syntax Description

```
clear dns-proxy statistics
```

#### Usage Guidelines

Use this command to clear all DNS proxy statistics.

#### Example

The following command clears DNS proxy statistics:

```
clear dns-proxy statistics
```

# clear dynamic-policy statistics

Clears policy control and charging (PCC) statistics from the interface communicating with the Policy and Charging Rules Function (PCRF) via Gx(x).

<b>Product</b>	HSGW
	PDSN
	SAEGW
	S-GW

<b>Privilege</b>	Inspector
------------------	-----------

<b>Command Modes</b>	Exec
----------------------	------

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

<b>Syntax Description</b>	<b>clear dynamic-policy statistics</b> { <b>hsgw-service</b> <i>name</i>   <b>pdsn-service</b> <i>name</i>   <b>sgw-service</b> <i>name</i> }
---------------------------	---

### **hsgw-service name**

Clears policy control and charging statistics from the Gxa interface communicating with the PCRF. *name* must be an existing HSGW service name and be from 1 to 63 alphanumeric characters.

### **pdsn-service name**

Clears policy control and charging statistics from the Gx interface communicating with the PCRF. *name* must be an existing PDSN service name and be from 1 to 63 alphanumeric characters.

### **sgw-service name**

Clears policy control and charging statistics from the Gxc interface communicating with the PCRF. *name* must be an existing S-GW service name and be from 1 to 63 alphanumeric characters.

<b>Usage Guidelines</b>	Use this command to clear PCC statistics for the specified service and its Gx interface communicating with the PCRF.
-------------------------	--

### **Example**

The following command clears HSGW statistics for an HSGW service named *hsgw4*:

```
clear dynamic-policy statistics hsgw-service hsgw4
```

The following command clears PCC statistics for a PDSN service named *cdma4*:

```
clear dynamic-policy statistics pdsn-service cdma4
```

The following command clears S-GW statistics for an S-GW service named *sgw4*:

```
clear dynamic-policy statistics sgw-service sgw4
```

# clear egtpc

Clears enhanced GPRS Tunneling Protocol control plane (eGTP-C) statistics and counters found in **show** command outputs and bulk statistics associated with all eGTP-C-related services or those defined by the parameters in this command.

---

## Product

MME  
P-GW  
S-GW  
SAEGW

---

## Privilege

Operator

---

## Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

## Syntax Description

```
clear egtpc statistics [ egtp-service name [ interface { s2a | s2b | s5s8 } ] ] | interface-type { interface-mme | interface-pgw-ingress [ interface { s2a | s2b | s5s8 } ] ] | interface-sgsn | interface-sgw-egress | interface-sgw-ingress } | mme-address ip_address | pgw-address ip_address | sgsn-address ip_address | sgw-address ip_address ]
```

**egtp-service** *name* [ **interface** { **s2a** | **s2b** | **s5s8** } ]

Clears all statistics and counters associated with an existing eGTP service name specified as an alphanumeric string of 1 through 63 characters.

**interface**: Clears the eGTP-C sub-interface statistics only for the specified eGTP-C service. Possible interfaces are:

- **s2a**: Interface type Sa
- **s2b**: Interface type Sb
- **s5s8**: Interface type S5/S8




---

## Important

The keywords **s2a** and **s2b** are only visible if WiFi Integration functionality is enabled. WiFi Integration requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

**interface-type** { **interface-mme** | **interface-pgw-ingress** [ **interface** { **s2a** | **s2b** | **s5s8** } ] ] | **interface-sgsn** | **interface-sgw-egress** | **interface-sgw-ingress** }

**interface-mme**: Clears statistics and counters derived from all MME interface types associated with this system.

**interface-pgw-ingress**: Clears statistics and counters derived from all P-GW ingress interface types associated with this system.

**interface:** Clears the eGTP-C interface statistics of a particular sub-interface of P-GW ingress. Possible interfaces are:

- **s2a:** Interface type Sa
- **s2b:** Interface type Sb
- **s5s8:** Interface type S5/S8



### Important

The keywords **s2a** and **s2b** are only visible if WiFi Integration functionality is enabled. WiFi Integration requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

**interface-sgw-egress:** Clears statistics and counters derived from all S-GW egress interface types associated with this system.

**interface-sgsn:** Clears statistics and counters derived from all SGSN S4 interface types associated with this system.

**interface-sgw-ingress:** Clears statistics and counters derived from all S-GW ingress interface types associated with this system.

### **mme-address *ip\_address***

Clears all statistics and counters derived from an existing MME IP address specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

### **pgw-address *ip\_address***

Clears all statistics and counters derived from an existing P-GW IP address specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

### **sgw-address *ip\_address***

Clears all statistics and counters derived from an existing S-GW IP address specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

### **sgsn-address *ip\_address***

Clears all statistics and counters derived from an existing SGSN S4 IP address specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

### Usage Guidelines

Use this command to clear running statistics and counters found in show command and bulk statistics outputs for all eGTP-C-related services or for specific interfaces, services, or IP addresses as specified by parameters in this command.

### Example

The following command clears eGTP-C statistics and counter associated with all P-GW ingress interfaces configured on this system:

```
clear egtpc statistics interface-type interface-pgw-ingress
```



The following command clears eGTP-C statistics and counter associated with all MME interfaces configured on this system:

```
clear egtpc statistics interface-type interface-mme
```

## clear event-notif statistics

Clears the statistical information collected over a configured Event Notification (SNMP) interface based on specific criteria.

---

**Product** All

---

**Privilege** Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `clear event-notif statistics`

---

**Usage Guidelines** Use this command to clear the statistical information collected over configured Event Notification interface based on specific criteria.

### Example

The following command clears the counter information for all Event Notification collection servers configured in a context:

```
clear event-notif server all
```

## clear event-record

Clears event record statistics for a P-GW node.

---

**Product** P-GW

---

**Privilege** Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `clear event-record statistics pgw [ | { grep grep_options | more } ]`

**grep *grep\_options* | more**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on using the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to clear event record statistics for a P-GW node.

**Example**

The following command clears all P-GW event level statistics:

```
clear event-record statistics pgw
```

## clear firewall

This command is obsolete.

## clear fng-service statistics

Deletes all previously gathered statistics for a specific Femto Network Gateway (FNG) service or all FNG services configured within a context.

**Product**

FNG

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear fng-service statistics { name service_name }
```

**name *service\_name***

Specifies the name of a specific FNG service configured in the context for which to clear statistics as an alphanumeric string of 1 through 63 characters that is case sensitive.

**Usage Guidelines**

Statistics for a single FNG service can be cleared using the **name** keyword. Statistics for all FNG services in the context can be deleted by entering the command with no keywords.

If this command is executed from within the local context with no keywords, statistics will be cleared for every FNG service configured on the system regardless of context. In addition, if the **name** keyword is used when executing from within the local context, statistics for all FNG services configured with the specified name will be cleared regardless of context.

**Example**

The following command clears statistics for an FNG service named fng1:

```
clear fng-service statistics name fng1
```

## clear gmb statistics

Deletes the collected statistics for the Gmb reference point. Gmb handles broadcast multicast service center (BM-SC) related signaling, which includes the user specific and bearer service messages for Multimedia Broadcast/Multicast Service (MBMS) service.

<b>Product</b>	GGSN
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<pre>clear gmb statistics [ apn <i>name</i>   bmsc-profile <i>profile_name</i></pre> <p><b>apn <i>name</i></b> Deletes only the Gmb information for the specified Access Point Name (APN) specified as an alphanumeric string of 1 through 62 characters.</p> <p><b>bmsc-profile <i>profile_name</i></b> Deletes only the Gmb information for the specified BM-SC profile specified as an alphanumeric string of 1 through 79 characters.</p>
<b>Usage Guidelines</b>	Use this command to delete usage statistics for the Gmb reference point.

**Example**

The following command deletes all Gmb statistics:

```
clear gmb statistics
```

## clear gmm-sm statistics

Deletes the collected statistics for the GPRS Mobility Management and Session Management (GMM/SM) configurations for various SGSN services.

<b>Product</b>	SGSN
----------------	------

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

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **clear gmm-sm statistics** [ **gmm-only** | **gprs-service** *service\_name* | **iups-service** *service\_name* | **plmn-id** *mcc mcc mnc mnc* | **recovered-values** | **sgsn-service** *service\_name* | **sm-only** ]

#### **gmm-only**

Deletes only GPRS mobility management (GMM) information for the specified filter. Filter options include:

- **gprs-service** *service\_name*
- **iups-service** *service\_name*
- **plmn-id**
- **recovered values**
- **sgsn-service** *service\_name*

#### **gprs-service *srcv\_name***

Deletes the statistics for a 2.5G GPRS service specified as an alphanumeric string of 1 through 63 characters that uniquely identifies a preconfigured GPRS service. The delete request can be narrowed by adding either the **nsei** or **routing-area** keywords.

#### **iups-service *srcv\_name***

Deletes the statistics for a IuPS service specified as an alphanumeric string of 1 through 63 characters that uniquely identifies a preconfigured IuPS service. The delete request can be narrowed by adding either the **rnc** or **routing-area** keywords.

#### **plmn-id *mcc mcc mncmnc* [ **access-type** { **gprs** | **umts** } ]**

Deletes the statistics for services within a specified PLMN.

**mcc** Specifies the mobile country code (MCC) as part of the identification of the RNC or RA. *mcc\_id* must be an integer from 100 to 999.

**mnc** Specifies the mobile network code (MNC) as part of the identification of the RNC or RA. *mnc\_id* must be a 2- or 3-digit integer from 00 to 999.

**access-type** keyword fine-tunes the delete procedure and only deletes GMM/SM statistics for the IuPS (access-type UMTS) and/or the GPRS (access-type GPRS) services belonging to the PLMN.

#### **recovered-values**

Deletes only the recovered values for the backed-up key KPI counters. The delete request can be narrowed by adding one of three filters:

- **gprs-service** *service\_name*
- **iups-service** *service\_name*
- **sgsn-service** *service\_name*

**sgsn-service *srvc\_name***

Deletes the statistics for a 3G SGSN service specified as an alphanumeric string of 1 to 63 characters that uniquely identifies the SGSN service. The delete request can be narrowed by adding either the **rnc** or **routing-area** keywords.

**sm-only**

Deletes only session management (SM) information for the specified keyword parameters.

**mcc**

**mcc** Specifies the mobile country code (MCC) as part of the identification of the RNC or RA. *mcc\_id* must be an integer from 100 to 999.

**mnc**

**mnc** Specifies the mobile network code (MNC) as part of the identification of the RNC or RA. *mnc\_id* must be a 2- or 3-digit integer from 00 to 999.

**lac *lac\_id***

Specifies the location area code (LAC) as part of the identification of the RNC or RA. *lac\_id* must be an integer from 1 to 65535.

**nseinse *id***

Deletes the GMM/SM session statistics for the identified network service entity (NSEI). *nse\_id* must be an integer from 0 to 65535 that uniquely identifies a configured NSEI.

**rncrnc *id***

Fine-tunes the deletion of GMM/SM session statistics just for the specified radio network controller (RNC). *rnc\_id* must be an integer from 0 to 4095.

**rac *rac\_id***

Specifies the routing area code (RAC) as part of the identification of the RNC or RA. *rac\_id* must be an integer from 1 to 255.

**routing-area *mcc\_id mnc mnc\_id lac lac\_id rac rac\_id***

Enter the **routing-area** keyword to fine-tune the clearing of the GMM/SM statistics for a specified routing area (RA) identified by the MCC, MNC, LAC and RAC.

---

**Usage Guidelines**

Use this command to delete usage statistics for the GMM/SM session configurations for SGSN services, including BSC attaches, activations, and throughput.

**Example**

The following command deletes GMM/SM statistics for a specific routing area defined for the SGSN's GPRS service:

```
clear gmm-sm statistics gprs-service gprs1 routing-area mcc 123 mcc 131
lac 24 rac 11
```

The following command displays all possible information for GMM/SM statistics:

```
show gmm-sm statistics verbose
```




---

**Important** Output descriptions for **show** commands are available in the *Statistics and Counters Reference*.

---

## clear gprsns statistics

Deletes collected statistics for the 2.5G SGSN's General Packet Radio Service (GPRS) Network Service (NS) layer (link level).

---

**Product** SGSN

---

**Privilege** Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `clear gprsns statistics { msg-stats nse nse_id | sns-msg-stats } [ | { grep grep_options | more } ]`

### msg-stats

Deletes collected transmit (tx) and receive (rx) message statistics for the NS layer.

### consolidated nse nse\_id

*nse\_id*: Enter an integer from 0 to 65535.

### nse nse\_id

Deletes statistics for an NSE specified as an integer from 0 to 65535.

### sns-msg-stats

Deletes subnetwork service (SNS) sublayer message statistics.

### grep grep\_options | more

You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

This command is used to display Frame Relay statistics configured for the NSE/NSVC with the commands documented in the *Network Service Entity - Peer NSEI Configuration Mode* chapter.

Collected statistics are cleared (deleted) with the **clear gprsns statistics** described in the *Exec Mode Commands (A-C)* chapter.

**Example**

The following command displays the collected message statistics for NSEI 1422:

```
show gprsns statistics msg-stats nse 1422
```

**Important**

Output descriptions for **show** commands are available in the *Statistics and Counters Reference*.

## clear gprsssf statistics

Deletes all Customized Applications for Mobile networks Enhanced Logic (CAMEL) service gprsSSF (GPRS Service Switching Function) statistics collected since the last reset or **clear** command.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear gprsssf statistics [ camel-service svrc_name | gprs [ 2g-sgsn-app | 3g-sgsn-app ] | gsmscf-address { address | all } | sms ] [ | { grep | more } ]
```

**camel-service *svrc\_name***

Clears only CAMEL service statistics for the configured CAMEL service specified as an alphanumeric string of 1 through 63 characters.

**gprs [ 2g-sgsn-app | 3g-sgsn-app ]**

Clears only CAMEL service statistics for either a 2.5G or 3G SGSN.

**gsmscf-address { *address* | all }**

Filters the command to only clear CAMEL service statistics for specified GSM service control function (gsmSCF) addresses. *address* is a standard ISDN E.164 address of 1 to 15 digits.

**sms**

Filters the command to only clear CAMEL service statistics for SMS protocol information.

**grep *grep\_options* | more**

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

This command instructs the SGSN to delete collected CAMEL service statistics for either specified CAMEL services, or for SMS or GPRS applications in all contexts.

**Example**

The following command will delete gprsSSF statistics collected for the CAMEL service residing at SCP identified by the gsmSCF address:

```
clear gprsssf statistics gsmSCF-address 412211411151
```

## clear gtpc statistics

Deletes all previously gathered GTPC (GTPv0, GTPv1-C, GTPv1-U) statistics within the given context based on the specified criteria.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear gtpc statistics [ [ custom1 | gtpcmgr-instance gtpcmgr_instance_number
| smgr-instance sessmgr_instance_number ] [ apn apn_name | ggsn-service
ggsn_service_name | mseg-service mseg_service_name | sgsn-address sgsn_ipv4_address
] ]
```

**custom1**

Clears the statistics of GTP-C messages for preservation mode and free of charge service.

This keyword is a customer-specific function used for Preservation-Mode and Free-of-Charge Service that is enabled under customer-specific license. For more information on this support, contact your Cisco account representative.

**gtpcmgr-instance *gtpcmgr\_instance\_number***

Clears GTP-C statistics for a GTPC Manager instance specified as an integer from 1 through 4294967295.

**smgr-instance *sessmgr\_instance\_number***

Clears GTP-C statistics for a Session Manager instance specified as an integer from 1 through 4294967295.



**apn *apn\_name***

Clears GTP-C statistics for an existing APN specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**ggsn-service *ggsn\_service\_name***

Clears GTP-C statistics for an existing GGSN service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**mseg-service *mseg\_service\_name*****Important**

This keyword is not supported in this release.

**sgsn-address *sgsn\_ipv4\_address***

Clears GTP-C statistics for an existing SGSN specified by IP address in IPv4 dotted-decimal notation.

**Usage Guidelines**

GTPC statistics can be cleared for a single APN, GGSN service, or SGSN. All GTPC statistics in the context can be deleted by entering the command with no keywords.

This command can be executed from any context configured on the system.

If this command is executed from within the local context with no keywords, all GTPC statistics will be cleared regardless of context.

GTPP statistics are not affected by this command.

**Example**

The following command clears all GTPC statistics context:

```
clear gtpc statistics
```

## clear gtp statistics

Deletes all previously gathered GTPP statistics within the given context for either single or all Charging Gateway Functions (CGFs).

**Product**

ePDG  
GGSN  
P-GW  
SAEGW  
SGSN

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear gtp statistics [ cgf-address ipv4/ipv6_address [ port port_num ] ]
```

```
cgf-address ipv4/ipv6_address [ port port_num ]
```

Deletes statistics for a CGF identified by its IP address entered in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**port port\_num**: Specifies the port number of CGF server. The port number must be an integer ranging from 1 to 65535.

This optional keyword is introduced to ease the identification of product specific CDRs. This configuration provides the flexibility to send ePDG, SaMOG and P-GW LBO CDRs to the same CGF server on different ports.

When the port is specified, this command clears the GTPP statistics for specified CGF server IP address and port. If port is not provided then it will clear the statistics for all CGF servers with the specified IP address.

**Usage Guidelines**

Statistics for a single CGF can be cleared using the **cgf-address** keyword. Statistics for all CGFs in the context can be deleted by entering the command with no keywords.

This command can be executed from any context configured on the system.

If this command is executed from within the local context with no keywords, statistics will be cleared for every CGF configured on the system regardless of context. In addition, if the **cgf-address** keyword is used when executing from within the local context, statistics for all CGFs configured with the specified name will be cleared regardless of context.

**Example**

The following command deletes all GTPP statistics for a CGF server with an IP address of 192.168.1.42:

```
clear gtp statistics cgf-address 192.168.1.42
```

## clear gtp storage-server local file statistics

Clears AAA proxy GTPP group level statistics for CDRs stored on the local hard disk.

**Product**

GGSN  
SGSN

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `clear gtp storage-server local file statistics [ group name name ]`

**Usage Guidelines** If executed from the local context, this command clears statistics for all GTPP groups configured on the system. If executed from the context within which the storage servers (hard disk) is configured, statistics are deleted for only that context.

## clear gtp storage-server statistics

Clears statistics for configured GTPP storage servers (GSS).

**Product** GGSN

**Privilege** Security Administrator, Administrator, Operator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `clear gtp storage-server statistics`

**Usage Guidelines** If executed from the local context, this command clears statistics for all GTPP storage servers configured on the system. If executed from the context within which the servers are configured, statistics are deleted for only those servers.

## clear gtpu statistics

Clears enhanced GPRS Tunneling Protocol user plane statistics and counters found in **show** command outputs and bulk statistics associated with all GTP-U-related services or those defined by the parameters in this command.

**Product** P-GW  
S-GW  
MME  
SAEGW

**Privilege** Operator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `clear gtpu statistics [ gtpu-service gtpu_service_name | mseg-service mseg_service_name | peer-address { ipv4/ipv6_address | all} ]`

**gtpu-service *gtpu\_service\_name***

Clears GTP-U statistics for an existing GTP-U service specified as an alphanumeric string of 1 through 63 characters.

**mseg-service *mseg\_service\_name*****Important**

This keyword is not supported in this release.

**peer-address { [*ipv4/ipv6\_address* | all ] }**

Clears GTP-U statistics for an existing peer IP address entered in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**all**

Clears GTP-U statistics for all existing peers.

**Usage Guidelines**

Use this command to clear running statistics and counters found in show command and bulk statistics outputs for all GTP-U-related services or for specific services or IP addresses as specified by parameters in this command.

**Example**

The following command clears GTP-U statistics and counter associated with a GTP-U service name *gtpu-12* configured on this system:

```
clear gtpu statistics gtpu-service gtpu-12
```

## clear hd-storage-policy

Clears statistic information for HD storage policies configured on the system.

**Product**

HSGW  
P-GW  
S-GW  
SAEGW

**Privilege**

Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear hd-storage-policy statistics { all | name name }
```

**statistics { all | name *name* }**

**all:** Clears ACR statistical information for all HD storage policies configured on the system.

**name *name*:** Clears ACR statistical information for an existing HD storage policy specified as an alphanumeric string of 0 through 63 characters.

**Usage Guidelines**

Use this command to clear statistics for HD storage policies configured on the system.

**Example**

The following command clears statistics for an HD storage policy named *pgwsgw*:

```
clear hd-storage-policy statistics name pgwsgw
```

## clear henbgw-access-service statistics

**Important**

In Release 20, 21.0 and 21.1, HeNBGW is not supported. This command must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

Clears HENBGW ACCESS service statistics.

**Product**

HeNB-GW

**Privilege**

Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear henbgw-access-service statistics [ henbgw-access-service
henbgw_acc_svc_name | miscellaneous | peer-id peer_id_value | slap | sctp ] [
| { grep grep_options | more } ]
```

**henbgw-access-service *henbgw\_acc\_svc\_name***

Clear statistics per specified HENBGW ACCESS service.

*henbgw\_acc\_svc\_name* is a string of size 1 to 63.

**miscellaneous**

Clears Miscellaneous statistics.

**peer-id**

Clears information about HENB associations for the specified peer.

*peer\_id\_value* is an integer value ranging from 0 to 4294967295.

**s1ap**

Clears S1AP statistics.

**sctp**

Clears SCTP statistics.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to clear HENBGW ACCESS service statistics

**Example**

The following command clears S1AP statistics :

```
clear hcnbgw-access-service statistics s1ap
```

## clear hcnbgw-network-service statistics

**Important**

In Release 20, 21.0 and 21.1, HeNB-GW is not supported. This command must not be used for HeNB-GW in these releases. For more information, contact your Cisco account representative.

Clears HENBGW NETWORK service statistics.

**Product**

HeNB-GW

**Privilege**

Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear hcnbgw-network-service statistics [ hcnbgw-network-service
hcnbgw_net_svc_name | peer-id peer_id_value | s1ap | sctp ] [ | { grep
grep_options | more } ]
```

**hcnbgw-network-service *hcnbgw\_net\_svc\_name***

Clear statistics per specified HENBGW NETWORK service.

*hcnbgw\_net\_svc\_name* is a string of size 1 to 63.

**peer-id**

Clears information about MME associations for the specified peer.

*peer\_id\_value* is an integer value ranging from 0 to 4294967295.

**slap**

Clears S1AP statistics.

**sctp**

Clears SCTP statistics.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to clear HENBGW NETWORK service statistics

**Example**

The following command clears S1AP statistics :

```
clear henbgw-network-service statistics slap
```

## clear hexdump-module statistics

Clears and resets all information related to hexdump-module statistics.

**Product**

ePDG  
SaMOG

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear hexdump-module statistics [ | { grep grep_options | more } ]
```

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Please refer to the Regulating the *Command Output* section in this reference for details on the usage of `grep` and more.

### Usage Guidelines

Use this command to clear and reset all information related to hexdump-module statistics.

### Example

The following command resets hexdump-module statistics.

```
clear hexdump-module statistics
```

## clear hnbgw sessions



### Important

In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Clears the active/dormant session information about registered Nabs) on Home-NodeB Gateway (HNB-GW) service instances configured and running on this system based on different filter criteria.

### Product

HNB-GW

### Privilege

Operator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
clear hnbgw sessions { all | cell-id cell_id | hnb-address hnb_ip_address |
hnb-local-id hnb_id | hnbgw-service hnbgw_svc_name | hnbid hnb_glbl_id | mcc mcc
mnc mnc [ -noconfirm ] [ lac lac | rac rac ] }
```

#### all

Clears the summarized or full information for all registered HNB sessions on an HNB-GW service instance running on system. Clearing the statistics can be filtered based on given filtering.

#### cell-id *cell\_id*

Clears HNB session statistics for a registered cell ID on an HNB-GW service instance. *cell\_id* is the identification number of the Femto cell where the user/subscriber is geographically located expressed as an integer from 0 through 268435455.

#### hnb-address *hnb\_ip\_address*

Clears the session statistics for HNB session(s) based on a registered HNB IP address entered in IPv4 dotted-decimal notation.



**hnb-local-id *hnb\_id***

Clears the session statistics of HNB session(s) for a registered local id of HNB specified as an integer from 1 through 255.

**hnbgw-service *hnbgw\_svc\_name***

Clears the session statistics for registered HNB session(s) on an existing HNB-GW service name specified as an alphanumeric string of 1 through 63 characters.

**hnbid *hnb\_glbl\_id***

Clears the statistics for HNB session(s) based on the registered HNB global id specified as an integer from 1 through 255

**mcc *mcc***

Clears statistics for HNB session(s) based on the registered Mobile Country Code (MCC) identification number of the UE. *mcc* must be an integer from 101 through 999.

**mnc *mnc***

Clears the statistics for HNB session(s) based on the registered Mobile Network Code (MNC) identification number of the UE. *mnc* must be a 2- or 3-digit integer from 00 through 999

**lac *lac***

Clears the statistics for HNB session(s) based on the registered Location Area Code (LAC) identification number of the UE. *lac* must be an integer from 1 through 65535.

**rac *rac***

Clears the statistics for HNB session(s) based on the registered Radio Access Code (RAC) identification number of the UE. *rac* must be an integer from 1 through 255.

**rnc *rnc***

Clears the statistics for HNB session(s) based on the registered Radio Network Code (RAC) identification number of the HNB. *rnc* must be an integer from 1 through 65535.

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

**Important**

The Operator privilege does not have access to this keyword.

**Usage Guidelines**

Use this command to clear the session statistics of all or specific registered HNB session(s) or in selected part of user session for HNB-GW services configured and running on this system.

**Example**

The following command clears the session statistics for all registered HNBs on the HNB-GW service named *hnbgw1*:

```
clear hnbgw sessions hnbgw-service hnbgw1
```

# clear hnbgw statistics

**Important**

In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Clears the HNB-GW service and HNB related statistics from an HNB-GW node.

**Product**

HNB-GW

**Privilege**

Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear hnbgw statistics [ gtpu-only ] [ hnb-access-mode { closed | hybrid
| open } ] [ hnbap-only ] [ hnbgw-service hnbgw_svc_name [ gtpu-only |
hnb-access-mode { closed | hybrid | open } | hnbap-only | ipne-only |
ranap-only | rtp-only | rua-only | sabp-only | sctp-only ] ] [ hnbid
hnb_identifier] [ hnbap-only | ranap-only | rtp-only | rua-only ] ] [ hnbid
| ipne-only | ranap-only | rtp-only | rua-only | sabp-only | sctp-only
]
```

**gtpu-only**

Clears the statistics for GTP-U traffic only for the selected HNB/HNB-GW service.

**hnb-access-mode { closed | hybrid | open }**

Clears the session statistics of an existing HNB-GW service based on access mode filters.

- **closed**: clears the statistics of only those UEs which are connected through Closed HNBs to the HNB-GW services on a chassis. This command applies to all Closed HNB sessions on a chassis. If any other criteria specified it will filter the statistics based on given criteria.
- **hybrid**: clears the statistics of only those UEs which are connected through Hybrid HNBs to the HNB-GW services on a chassis. This command applies to all Hybrid HNB sessions on a chassis. If any other criteria specified it will filter the statistics based on given criteria.
- **open**: clears the statistics of only those UEs which are connected through Open HNBs to the HNB-GW services on a chassis. This command applies to all Open HNB sessions on a chassis. If any other criteria specified it will filter the statistics based on given criteria.

**hnbap-only**

Clears the statistics for Home NodeB Application Part (HNBAP) traffic only for the selected HNB/HNB-GW service.

**hnbgw-service *hnbgw\_svc\_name***

Clears the session statistics for an existing \HNB-GW service name specified as an alphanumeric string of 1 through 63 characters.

**hnbid *hnb\_identifier***

Clears the session statistics for an existing Home-NodeB identifier specified as an alphanumeric string of 1 through 255 characters.

**ipne-only**

Clears IPNE statistics for selected HNBGW Service.

**ranap-only**

Clears the session statistics for Radio Access Network Application Protocol (RANAP) traffic only for the selected HNB/HNB-GW service.

**rtp-only**

Clears the session statistics for Real Time Protocol (RTP) traffic only for the selected HNB/HNB-GW service.

**rua-only**

Clears the session statistics for RANAP User Adaptation (RUA) traffic only for the selected HNB/HNB-GW service.

**sabp-only**

Clears the session statistics for Signaling Connection Control Part (SCCP) traffic only for the selected HNB-GW service.

**sctp-only**

Filters the session statistics to display only Stream Control Transmission Protocol (SCTP) traffic for the selected HNB-GW service.

---

**Usage Guidelines**

Use this command to clear the session statistics for an overall session or in a selected part of a user session for HNB-GW services and/or HNBs configured and running on this system.

**Example**

The following command clear the session statistics for the HNBAP portion of session details for the HNB-GW service named *hnbgw1*:

```
clear hnbgw statistics hnbgw-service hnbgw1 hnbap-only
```

The following command clears the session statistics for the RANAP portion of session details for the HNB identified as *102*:

```
clear hnbgw statistics hnbid 102 ranap-only
```

## clear hsgw-service

Clears HRPD Serving Gateway (HSGW) statistics and counters found in **show** command outputs and bulk statistics associated with all HSGW services or a specific service defined by the parameter in this command.

---

**Product** HSGW

---

**Privilege** Operator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **clear hsgw-service statistics [ dns-stats | name service\_name [ dns-stats ] ] [ | { grep grep\_options | more } ]**

### **dns-stats**

Clears DNS-related statistics.

### **name name**

Clears statistics and counters for an existing HSGW service name specified as an alphanumeric string of 1 through 63 characters.

### **grep grep\_options | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines** Use this command to clear statistics for HSGW services configured on the system.

### **Example**

The following command clears statistics for an HSGW service named *hsgw3*:

```
clear hsgw-service statistics name hsgw3
```

## clear hss-peer-service

Clears statistic information for Home Subscriber Service (HSS) peer services configured on the system.

**Product** MME

**Privilege** Operator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **clear hss-peer-service statistics [ service *name* ]**

**statistics [ service *name* ]**

**statistics:** Clears HSS peer service statistical information for all HSS peer services configured on the system.

**service *name*:** Clears HSS peer service statistic information for an existing HSS peer service specified as an alphanumeric string of 1 through 64 characters.

**Usage Guidelines** Use this command to clear statistics for HSS peer services configured on the system.

### Example

The following command clears statistics for an HSS peer service named *hss4*:

```
clear hss-peer-service statistics service name hss4
```

## clear ims-authorization

Clears statistics for a specified or all IP Multimedia System (IMS) Authorization Service(s).

**Product** GGSN  
SCM

**Privilege** Security Administrator, Administrator, Operator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **clear ims-authorization { policy-control statistics [ ims-auth-service *service\_name* ] | service statistics [ name *service\_name* ] } [ | { grep *grep\_options* | more } ]**

**ims-auth-service *service\_name***

Clears statistics for the specified IMSA service.

*service\_name* must be an alphanumeric string of 1 through 64 characters.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to clear IMSA Service statistics.

**Example**

The following command clears IMSA policy-control statistics for an IMSA service named *test\_service*:

```
clear ims-authorization policy-control statistics ims-auth-service
test_service
```

## clear ims-sh-service statistics

Clears all IP Multimedia System (IMS) Sh interface (Diameter) statistics for a specific or all services using the Sh interface.

**Product**

PDIF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear ims-sh-service statistics [ service service_name ]
```

**service *service\_name***

Clears statistics for the specified existing IMS service.

*service\_name* must be an alphanumeric string of 1 through 64 characters.

**Usage Guidelines**

Use this command to clear interface Sh interface statistics for a specified or all IMS services.

**Example**

The following command clears all Sh interface statistics:

```
clear ims-sh-service statistics
```

## clear ip access-group statistics

Clears all interface access control list (ACL) statistics and the context level ACL statistics that have been configured in the current context. Be aware that updating an access list also causes all ip access-groups utilizing the list to be cleared.

---

**Product**

ASN-GW  
GGSN  
PDSN

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec  
The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

**clear ip access-group statistics**

---

**Usage Guidelines**

Use this command to clear all interface ACL statistics and the context level ACL statistics that have been configured in the current context.

**Example**

The following command clears the ACL statistics:

```
clear ip access-group statistics
```

## clear ip arp

Clears the address resolution protocol (ARP) cache for a given IP address.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec  
The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

**clear ip arp** *ip\_address*

***ip\_address***

Specifies the IP address for which to clear the ARP cache in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Usage Guidelines**

Clear the ARP cache when network changes have occurred for the case where the cached data may cause undue overhead in routing packets.

**Example**

The following command clears the ARP cache for the IP address *10.2.3.4*:

```
clear ip arp 10.2.3.4
```

## clear ip bgp peer

Resets Border Gateway Protocol (BGP) connections for all peers or for specified peers in the current context.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear ip bgp peer { ip_address | all | as as_num } [ in | out | soft | vpnv4
| vpn6 | vrf vrf_name [ in | out | soft ] ]
```

***ip\_address***

Specifies the IP address of the neighbor for which BGP connections should be reset in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**all**

Resets BGP connections for all peers.

**as *as\_num***

Resets BGP connections for all peers in the specified autonomous system (AS). *as\_num* must be an integer from 1 through 65535.

**in**

Softly reconfigures inbound updates.

**out**

Softly reconfigures outbound updates.

**soft**

Softly reconfigures inbound and outbound updates.



**vpn4**

Clears BGP sessions within the VPNv4 address family.

**vpn6**

Clears BGP sessions within the VPNv6 address family.

**vrf vrf\_name**

Clears BGP sessions within the specified VRF. *vrf\_name* is an alphanumeric string of 1 through 63 characters.

---

**Usage Guidelines**

Use this command to BGP information for the current context.

**Example**

The following command resets BGP connections for all neighbors:

```
clear ip bgp peer all
```

## clear ip localhosts

Removes the host specified from the current context's local host list for IP address mappings.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
clear ip localhosts [ host_name ]
```

**host\_name**

Specifies the name of the host to be removed as an alphanumeric string of 1 through 127 characters. When omitted, all local host name mappings will be removed.

---

**Usage Guidelines**

Clears a host name when it is no longer valid for the current context to access. The host name specified will be unrecognized by the current context once the command is performed.

**Example**

```
clear ip localhosts
clear ip localhosts 10.2.3.4
clear ip localhosts remoteABC
```

## clear ip ospf process

Clears Open Shortest Path First (OSPF) database information for the current context and re-establishes neighbor adjacency.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **clear ip ospf process**

**Usage Guidelines** Use this command to clear the OSPF database information for the current context and re-establishes neighbor adjacency.

### Example

The following command clears the OSPF database information for the current context and re-establishes neighbor adjacency:

```
clear ip ospf process
```

## clear ipne statistics

Clears IP Network Enabler (IPNE) statistics for a specified or all IPNE services.

**Product** MINE

**Privilege** Administrator, Security Administrator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **clear ipne statistics [ service service\_name ]**

**service service\_name**

Specifies the name of an existing IPNE service for which statistics will be cleared as an alphanumeric string of 1 through 64 characters.

**Usage Guidelines** Clears IPNE statistics for a specified or all IPNE services.

**Example**

The following example clears all IPNE statistics:

```
clear ipne statistics
```

## clear ipsg statistics

Clears IP Services Gateway (IPSG) statistics for a specified or all IPSG services.

**Product**

eWAG

IPSG

**Privilege**

Administrator, Security Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear ipsg statistics [ service service_name ]
```

**service *service\_name***

Specifies the name of an IPSG service for which statistics will be cleared.

*service\_name* must be an alphanumeric string of 1 through 64 characters.

**Usage Guidelines**

Clears IPSG service statistics for a specified or all IPSG services.

**Example**

The following command clears statistics for all IPSG services:

```
clear ipsg statistics
```

## clear ipv6 neighbors

Clears an IPv6 address from the neighbor cache.

**Product**

PDIF

**Privilege**

Administrator, Security Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `clear ipv6 neighbors ip_address`

*ip\_address*

Specifies the IP address in IPv6 colon-separated-hexadecimal notation.

---

**Usage Guidelines** Clears a specific address from the neighbor cache.

**Example**

Use the following example to clear `3ffe:ffff:101::230:6eff:fe04:d9aa/48`:

```
clear ipv6 neighbors 3ffe:ffff:101::230:6eff:fe04:d9aa/48
```

## clear ipv6 ospf process

Restarts Open Shortest Path First Version 3 (OSPFv3) with available configuration.

---

**Product** GGSN  
HA  
PDSN

---

**Privilege** Administrator, Security Administrator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `clear ipv6 ospf process`

---

**Usage Guidelines** Force a restart of OSPFv3 process using the available configuration.

**Example**

```
clear ipv6 ospf process
```

## clear l2tp

Clears all or specific Layer 2 Tunnelling Protocol (L2TP) statistics or clears and disconnects all or specified sessions or tunnels.

---

**Product** PDSN  
GGSN  
LNS

**Privilege** Security Administrator, Administrator, Operator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear l2tp { statistics [ lac-service service_name | lns-service service_name
| pdsnclosedrp-service service_name | peer-address ip_address ] | tunnels {
all [ clear-sa ] | callid call_id | lac-service service_name [ clear-sa ]
| lns-service service_name | pdsnclosedrp-service service_name | peer-address
ip_address [ clear-sa ] } }
```

**statistics** [ **lac-service** *service\_name* | **lns-service** *service\_name* | **peer-address** *ip\_address* ]

With no optional keywords specified, this command clears all L2TP statistics for the current context.

**lac-service** *service\_name*: Clears all L2TP statistics for the specified LAC service in the current context.

**lns-service** *service\_name*: Clears all L2TP statistics for the specified LNS service in the current context.

**pdsnclosedrp-service** *service\_name*: Clears all L2TP statistics for the specified PDSN closed R-P service in the current context.

**peer-address** *ip\_address*: Clears all L2TP statistics for the destination (peer LNS) at the specified IP address. The IP address is entered using IPv4 dotted-decimal notation.

**tunnels** { **all** [ **clear-sa** ] | **callid** *call\_id* | **lac-service** *service\_name* [ **clear-sa** ] | **peer-address** *ip\_address* [ **clear-sa** ] }

**all**: Clears all tunnels in the current context.

**lac-service** *service\_name*: Clears all tunnels in the current context that belong to the specified LAC service and closes the tunnels.

**lns-service** *service\_name*: Clears all tunnels in the current context that belong to the specified LNS service and closes the tunnels.

**pdsnclosedrp-service** *service\_name*: Clears all tunnels in the current context that belong to the specified PDSN Closed R-P service and closes the tunnels.

**peer-address** *ip\_address*: Clears all tunnels in the current context whose destination (peer LNS) is the system at the specified IP address. The IP address is specified using IPv4 dotted-decimal notation.

**callid** *call\_id*: Uses the unique identifier that specifies a particular tunnel in the system to clear that tunnel and disconnect it. The output of the command **show l2tp tunnels** contains a field labeled Callid Hint which lists the call id information to use with this command. This is an 8-byte hexadecimal number.

**clear-sa**: If any security associations have been established they are cleared.

**Usage Guidelines** Clear L2TP all or specific L2TP statistics or clear sessions in a tunnel and disconnect the tunnel.

### Example

To clear all L2TP statistics for the current context, use the following command:

```
clear l2tp statistics
```

To clear all L2TP statistics for the LAC service named *lac1*, use the following command:

```
clear l2tp statistics lac-service lac1
```

Use the following command to clear L2TP statistics for the LNS peer at the IP address *10.10.10.100*:

```
clear l2tp statistics peer-address 10.10.10.100
```

The following command clears and closes all tunnels in the current context:

```
clear l2tp tunnels all
```

The following command clears and closes all tunnels for the LAC service named *lac2*:

```
clear l2tp tunnels lac-service lac2
```

The following command clears and closes all tunnels the peer at the IP address *10.10.10.110*:

```
clear l2tp tunnels peer-address 10.10.10.110
```

## clear lawful-intercept

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

## clear llc statistics

Deletes collected traffic statistics for the GPRS logical link-control (LLC) layer.

---

**Product** SGSN

---

**Privilege** Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `clear llc statistics [ gprs-service svrc_name ] [ | { grep grep_options | more } ]`

**gprs-service *svrc\_name***

Clears the collected statistics for an existing GPRS service specified as an alphanumeric string of 1 through 63 characters.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For more information on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference*.

**Usage Guidelines**

This command deletes statistics collected for the traffic that has gone through the LLC layer for either all GPRS services or for a specified GPRS service.

**Example**

The following command deletes all LLC statistics for GPRS service *gprs1*:

```
clear llc statistics gprs-service gprs1
```

## clear lma-service statistics

Clears Local Mobility Anchor (LMA) statistics and counters found in **show** command outputs and bulk statistics associated with all LMA services or a specific service defined by the parameter in this command.

**Product**

P-GW  
SAEGW

**Privilege**

Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear lma-service statistics [ name service_name ]
```

**name service\_name**

Clears statistics and counters for an existing LMA service name specified as an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to clear statistics and counters in show command outputs and bulk statistics for all LMA services or for a specific LMA service.

**Example**

The following command clears statistics and counters for an LMA service named *lma3*:

```
clear lma-service statistics name lma3
```

## clear local-policy

Clears local Quality of Service (QoS) policy service statistics and counters found in **show** command outputs and bulk statistics associated with all local QoS policy services or a specific service defined by the parameter in this command.

**Product**

P-GW

## clear local-user

SAEGW

**Privilege** Operator**Command Modes** Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`**Syntax Description** `clear local-policy statistics [ service service_name ]`**service *service\_name***

Clears statistics and counters for an existing local policy service name specified as an alphanumeric string of 1 through 64 characters.

**Usage Guidelines** Use this command to clear statistics and counters in **show** command outputs and bulk statistics for all local QoS policy services or a specific service.**Example**The following command clears statistics and counters for a local QoS policy service named *lp3*:`clear local-policy statistics service lp3`

## clear local-user

Clears information pertaining to local-user administrative accounts.

**Product** All**Privilege** Security Administrator**Command Modes** Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`**Syntax Description** `clear local-user { database [ -noconfirm ] | statistics | username name lockout }`**clear local-user database**

Clears the local-user database by deleting all information for all local-user accounts.

**Caution**

Use this command only in the event of security concerns or to address concerns of the local-user account database integrity.



**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

**clear local-user statistics**

Clears statistics pertaining to local-user accounts.

**clear local-user username *name* lockout**

Removes lockouts associated with the local-user account expressed as an alphanumeric string of 3 through 16 characters that is case sensitive.

**Usage Guidelines**

This command can be used to remove local-user account lockouts, reset local-user-related statistics to 0, or to delete the local-user database.

**Example**

The following command removes the lockout placed on a local-user account named *SecureAdmin*:

```
clear local-user username SecureAdmin lockout
```

## clear location-service

Clears collected statistics and information pertaining to Location Services.

**Product**

MME  
SGSN

**Privilege**

Security Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear location-services statistics [ service location_svc_name ]
```

**statistics**

Clears all location service statistics.

**service *location\_svc\_name***

Clears statistics only for the specified location service.

**Usage Guidelines**

Use this command to clear location service statistics.

**Example**

The following command clears the Location service statistics only for the location service named *location\_service1*:

```
clear location-service statistics service location_service1
```

## clear mag-service statistics

Clears Mobile Access Gateway (MAG) statistics and counters found in **show** command outputs and bulk statistics associated with all MAG services or a specific service defined by the parameter in this command.

**Product**

HSGW  
S-GW  
SAEGW

**Privilege**

Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear mag-service statistics [ name service_name ]
```

**name** *service\_name*

Clears statistics and counters for an existing MAG service name specified as an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to clear statistics and counters in show command outputs and bulk statistics for all MAG services or for a specific MAG service.

**Example**

The following command clears statistics and counters for a MAG service named *mag1*

```
clear mag-service statistics name mag1
```

## clear map statistics

Clears Mobile Application Part (MAP) statistics (SS7) for a specified service or all services.

**Product**

GGSN  
SGSN

<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<b>clear map statistics</b> [ <b>name</b> <i>service_name</i> ] [ <b>recovered-values</b> ]  <b>name</b> <i>service_name</i> Clears statistics and counters for an existing MAP service name specified as an alphanumeric string of 1 through 63 characters.  <b>recovered-values</b> Clears only recovered values for key MAP KPI counters that were backed-up.
<b>Usage Guidelines</b>	Delete MAP statistics for a single or all GGSN/SGSN services.  <b>Example</b> The following command deletes all MAP statistics. <b>clear map statistics</b>

## clear maximum-temperatures

Clears information pertaining to component maximum temperatures. (ASR 5x00 only)

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<b>clear maximum-temperatures</b>
<b>Usage Guidelines</b>	Reset the timestamp to the current time and clear previous maximum temperatures for all temperature monitored components. This may be useful when preparing to study system performance, monitor usage, or troubleshoot the administrative interfaces.  <b>Example</b> The following command resets the maximum temperature statistics for all monitored chassis components. <b>clear maximum-temperatures</b>

## clear mipfa statistics

Clears the statistics for the mobile IP foreign agent (MIPFA). The statistics for a specific foreign agent service may be cleared by an explicit command.

---

### Product

PDSN  
GGSN  
ASN-GW

---

### Privilege

Security Administrator, Administrator, Operator

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

```
clear mipfa statistics [ fa-service name | peer-address ip_address ]
```

#### **fa-service** *name* | **peer-address** *ip\_address*

**fa-service** *name*: Clears the statistics for an existing FA service specified as an alphanumeric string of 1 through 63 characters. "Total sessions" counters for all peers associated with the service are also reset.

**peer-address** *ip\_address*: Clears the statistics for the peer IP address specified in IPv4 dotted-decimal notation. "Total sessions" counter for the specified peer is also reset.

---

### Usage Guidelines

Clear all statistics for the MIP foreign agent or for a specific service. This may be useful in monitoring performance and troubleshooting as the statistics may be cleared at a well known time and then collected and transferred for review.

#### Example

The following clears all statistics for the mobile IP foreign agent.

```
clear mipfa statistics
```

The following commands clear the statistics for the example service only.

```
clear mipfa statistics fa-service sampleService  
clear mipfa statistics peer-address 10.2.3.4
```

## clear mipha statistics

Clears the statistics for the mobile IP home agent (MIPHA). The statistics for a home agent service may be cleared by explicit command.

---

### Product

PDSN  
HA

<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<b>clear mipha statistics [ ha-service <i>name</i>   peer-address <i>ip_address</i> ]</b>  <b>ha-service <i>name</i>   peer-address <i>ip_address</i></b> <b>ha-service <i>name</i>:</b> Clears the statistics for an existing HA service name specified as an alphanumeric string of 1 through 63 characters. "Total sessions" counters for all peers associated with the service are also reset. <b>peer-address <i>ip_address</i>:</b> Clears the statistics for an IP address specified using IPv4 dotted-decimal notation. "Total sessions" counter for the specified peer is also reset.
<b>Usage Guidelines</b>	Clear all statistics for the MIP home agent or for a specific service. This may be useful in monitoring performance and troubleshooting as the statistics may be cleared at a well known time and then collected and transferred for review.

**Example**

The following clears all statistics for the mobile IP foreign agent.

```
clear mipha statistics
```

The following command clears the statistics for the example service only.

```
clear mipha statistics ha-service sampleService  
clear mipha statistics peer-address 10.2.3.4
```

## clear mipmn statistics

Clears the statistics for mobile IP mobile node (MIPMN).

<b>Product</b>	PDSN HA
<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<b>clear mipmn statistics</b>
<b>Usage Guidelines</b>	Clear all statistics for MIP mobile node. This may be useful in monitoring performance and troubleshooting as the statistics may be cleared at a well known time and then collected and transferred for review.

**Example**

The following clears all statistics for MIP mobile node:

```
clear mipmn statistics
```

## clear mipv6ha statistics

Clears the statistics for mobile IP IPv6 home agent (MIPv6HA).

**Product**

PDSN

HA

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear mipv6ha statistics
```

**Usage Guidelines**

Clear all statistics for a MIP IPv6 home agent. This may be useful in monitoring performance and troubleshooting as the statistics may be cleared at a well known time and then collected and transferred for review.

**Example**

The following clears all statistics for MIPv6 home agent:

```
clear mipv6ha statistics
```

## clear mme-service db record

Clears the MME database records all instances of session manager running for an MME service filtered with IMSI or GUTI as criteria.

**Product**

MME

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear mme-service db record { all | guti plmn plmn_id group-id mme_grp_id
code mme_code m-tmsi mtmsi_value | imsi imsi_identifier | instance instance_id }
```

**all**

Clears all detached database records.

**guti plmn *plmn\_id* group-id *mme\_grp\_id* code *mme\_code* m-tmsi *mtmsi\_value***

This set of keywords specifies the filter criteria as a Globally Unique Temporary Identifier (GUTI) to clear the database records for MME service.

The GUTI is constructed from the GUMMEI and the M-TMSI where GUMMEI is constructed from PLMN (MMC and MNC) *plmn\_id* and MME Identifier is constructed from an MME Group ID (MMEGI) *mme\_grp\_id* and an MME Code (MMEC) *mme\_code*.

Within the MME, the mobile is identified by the M-TMSI *mtmsi\_value*

**imsi *imsi\_identifier***

Specifies the filter criteria as International Mobile Subscriber Identity (IMSI) to clear the database records of a session instance. *imsi\_identifier* is a 15-character IMSI field that identifies the subscriber's home country and carrier.

**instance *instance\_id***

Clears all detached database records in an existing session manager instance specified as an integer from 1 through 4294967295.

**Usage Guidelines**

Use this command to clear/remove database records for all or a particular instance of session manager for MME services on this system.

**Example**

The following command clears the summary database records of a session instance for subscriber having IMSI as *123455432112345* in the MME service:

```
clear mme-service db record imsi 123455432112345
```

## clear mme-service db statistics

Clears the MME database statistics for MME sessions for all or specific session instances on this system.

**Product**

MME

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `clear mme-service db statistics [ instance smgr_instance ]`

**instance *smgr\_instance***

Specifies that MME database statistics for a specific instance of session manager running for MME service are to be removed. The instance ID expressed is an integer from 0 through 4294967295. If an instance is not specified, database statistics of all instances will be removed.

**Usage Guidelines** Use this command to clear/remove database statistics for all or a particular instance of session manager for MME services on this system.

**Example**

The following command removes/clears the database statistics of all instances of the MME service on a system:

```
clear mme-service db statistics
```

## clear mme-service statistics

Clears MME service statistics based on various criteria.

**Product** MME

**Privilege** Security Administrator, Administrator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `clear mme-service statistics [ dcnr | decor [ decor-profile profile_name ] | emm-only | esm-only | handover | mme-service mme_svc_name | offload | paging-profile [ profile-name paging_profile_name ] | peer-id peer_identifier | recovered-values | slap | sctp | tai all | taidb db_name ] + [ | { grep grep_options | more } ]`

**dcnr**

Clears the dual connectivity NR statistics.

**decor [ decor-profile *profile\_name* ]**

Clears the Decor statistics for all the configured Decor profile(s).

**decor-profile *profile\_name***: Clears the Decor statistics for the specified Decor profile. *profile\_name* must be an alphanumeric string of 1 through 63 characters.



**emm-only**

Clears EPS mobility management (EMM) related statistics for all MME services, or clears these statistics for a specific MME service name or a specific eNodeB association peer identifier.

**esm-only**

Clears EPS session management (ESM) related statistics for all MME services, or clears these statistics for a specific MME service name or a specific eNodeB association peer identifier.

**handover**

Clears handover related statistics (such as Intra-MME, EUTRAN<->EUTRAN via S10, EUTRAN<->UTRAN via GnGp, EUTRAN<->GERAN via GnGp, and EUTRAN<->UTRAN via S3) for all MME services, or clears these statistics for a specific MME service name or a specific eNodeB association peer identifier.

**mme-service *mme\_svc\_name***

Clears all statistics for the specified MME service name.

**offload**

Clears all load rebalancing (UE offload) statistics for all MME services, or clears these statistics for a specific MME service name or a specific eNodeB association peer identifier.

**paging-profile [ *profile-name paging\_profile\_name* ]**

Clears the paging profile statistics for all the configured paging-profile(s) one after another.

**profile-name** *paging\_profile\_name*: Clears the paging profile statistics for the given profile name. *paging\_profile\_name* must be an alphanumeric string of 1 through 63 characters.

**peer-id *peer\_identifier***

Clears all statistics for the specified eNodeB association peer identifier.

**recovered-values**

Clears all recovered statistics if the *Backup and Recovery of Key KPI Statistics* feature has been enabled. For details, refer to the **statistics-backup** command in the Global Configuration mode and the feature chapter in the *MME Administration Guide*.

**s1ap**

Clears all all S1-AP statistics for all MME services, or clears these statistics for a specific MME service name or a specific eNodeB association peer identifier.

**sctp**

Clears all all SCTP statistics for all MME services, or clears these statistics for a specific MME service name or a specific eNodeB association peer identifier.

**tai all**

Clears statistics stored for all TAIs in all TAI management databases.

**taidb *db\_name***

Clears statistics stored for all TAIs in the specified TAI management database.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

This command is used to clear the statistical information of an MME service based on various filter criteria.

**Example**

The following command clears the service statistics of all MME service on a system:

```
clear mme-service statistics
```

## clear multicast-sessions

Disconnects broadcast-multicast sessions based on specified criteria.

**Product**

PDSN  
SGSN

**Privilege**

Security Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear multicast-sessions [ -noconfirm ] [ keywords ] [ verbose ]
```

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

**all**

Disconnects all multicast sessions.

**callid *call\_id***

Clears the call specified by *call\_id*. The call ID is as an 8-byte hexadecimal number.

**card-num slot\_num**

Specifies the slot number of the packet processing card by which the multicast session is processed as a number from 1 through 7 or 10 through 16 (for the ASR 5000) or from 1 through 3 or 6 through 10 (for the ASR 5500).

**flowid id**

Clears calls for a specific Broadcast/Multicast Service (BCMCS) flow id, specified as a hexadecimal number.

**flowid-type [ flow | program ]**

Clears multicast sessions according to the type of flow.

**flow:** Clears all multicast sessions for the flow ID type "flow".

**program:** Clears all multicast sessions for the flow ID type "program".

**mcast-address ipv4\_address**

Clears multicast sessions for a specific multicast address. Must be followed by the IP address of an interface in IPv4 dotted-decimal notation.

**pct ipv4\_address**

Clears multicast sessions connected via the packet control function defined by an IP address in IPv4 dotted-decimal notation.

**pdsn\_service name**

Clears multicast sessions connected to an existing packet data service name.

**sgsn-service svc\_name**

Displays information for multicast sessions connected to an existing SGSN service name.

**verbose**

Displays as much information as possible. If this option is not specified, the output is the standard level which is the concise mode.

**Usage Guidelines**

Clear multicast sessions to aid in troubleshooting the system when no additional subscribers may connect or when a specific service or remote address may be having connection problems. This command may also be useful when preparing for maintenance activities such that connects may be cleared to perform any necessary procedures.

The keywords are filters that modify or filter the criteria for deciding which sessions to clear and are described below. Multiple keywords can be entered on a command line.

When multiple keywords are specified, the multicast sessions deleted must meet the specifications of all of the keywords.

**Example**

The following command clears the broadcast-multicast sessions having multicast address 10.2.3.4:

```
clear multicast-sessions mcast-address 10.2.3.4
```

The following command clears the broadcast-multicast session(s) having call id *00004e22*:

```
clear multicast-sessions callid 00004e22
```

## clear nat-ip

Clears the NAT IP addresses forcibly from NAT pools.

---

### Product

NAT

---

### Privilege

Security Administrator, Administrator, Operator

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

```
clear nat-ip { ip_address | pool pool_name } context context_name [ -noconfirm ]
```

#### ***ip\_address***

Specifies the NAT IP address to be released from subscribers, in IPv4 dotted-decimal notation.

#### **pool** *pool\_name*

Specifies the NAT pool name, that is an existing IP pool or IP pool group, specified as an alphanumeric string of 1 through 31 characters.

#### **context** *context\_name*

Clears statistics for the VPN context name where the NAT pool belongs to, specified as an alphanumeric string of 1 through 79 characters.

#### **-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

---

### Usage Guidelines

Use this command to clear the NAT IP addresses from Session Manager to VPN for NAT pools, by forcibly releasing the IP addresses from the subscriber calls.

### Example

The following command clears the NAT IP statistics for the configured IP address *1.1.1.1* in the **test123** VPN context:

```
clear nat-ip 1.1.1.1 context test123
```

The following command clears the NAT IP statistics for the **pool1** NAT pool in the **test123** VPN context without user confirmation:

```
clear nat-ip pool pool1 context test123 -noconfirm
```

## clear pcc-policy service statistics

Clears statistical information of all or a specific policy control and charging (PCC) service configured in a context.

---

**Product** IPCF

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **clear pcc-policy statistics** [ **name** *pcc\_plcy\_svc\_name* ]

**name** *pcc\_plcy\_svc\_name*

Clears information only for an existing PCC-Policy service in the current context, expressed as an alphanumeric string of 1 through 79 characters.

---

**Usage Guidelines**

Use this command to clear the statistical information of all or a specific PCC-Policy services configured in a context.

Clearing of statistics can further be filtered for specific PCC-Policy service name as well.

### Example

The following command clears the statistical information for the PCC-Policy service named *pcc\_policy1* in summarized output:

```
clear pcc-policy service statistics name pcc_policy1
```

## clear pcc-policy session

Clears the active/dormant session information about PCC-Policy service instances configured and running on this system based on different filter criteria.

---

**Product** IPCF

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `clear pcc-policy sessions [ all ] [ apn | call-id call_id | imsi imsi_id | ip-address pcc_pcef_ip_address | service pcc_plcy_svc_name ] [ local-purge ]`

**all**

Clears the session information of all registered IP-CAN session(s) on a PCC-Policy service instance running on the system. The display can be filtered based on given filtering criteria.

**apn *apn\_name***

Clears the session information for PCC-Policy service sessions connected via an existing APN,

**imsi *imsi\_id***

Clears the session information of IP-CAN session(s) based on the IMSI identifier of a subscriber on a PCC-Policy service instance. *imsi\_id* is the International Mobile Subscriber Identity (IMSI) and must be a 15-character field which identifies the subscriber's home country and carrier.

**ip-address *pcc\_pcef\_ip\_address***

Clears the session statistics of IP-CAN session(s) based on the registered PCEF (Policy and Charging Enforcement Function) node IP address expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**call-id *call\_id***

Clears the session statistics of IP-CAN session(s) based on the existing registered call id of an IP-CAN session subscriber specified in eight-byte hexadecimal format.

**pcc-policy-service *pcc\_plcy\_svc\_name***

Clears the session statistics of registered IP-CAN session(s) based on an existing PCC-Policy service name, expressed as an alphanumeric string of 1 through 63 characters.

**local-purge**

Clears the session information for PCC-Policy service sessions locally only.

**Usage Guidelines**

Use this command to clear the session statistics of all or specific registered IP-CAN session(s) or in selected part of user session for PCC-Policy services configured and running on this system.

**Example**

The following command clears the session statistics for all registered PCC-Policy service instances on a system/context locally only:

```
clear pcc-policy sessions all local-purge
```

## clear pcc-sp-endpoint statistics

Clears the statistical information of all or specific PCC-Sp-Endpoint instance configured in a context.

<b>Product</b>	IPCF
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<b>clear pcc-sp-endpoint statistics [ name <i>sp_endpt_name</i> ]</b>  <b>name <i>sp_endpt_name</i></b> Clears information only for an existing PCC-Sp-Endpoint instance specified as an alphanumeric string of 1 through 79 characters.
<b>Usage Guidelines</b>	Use this command to clear the statistical information of all or an specific PCC-Sp-Endpoint interface configured in a context. Clearing of statistics can further be filtered for specific PCC-Sp-Endpoint instance name as well.  <b>Example</b> The following command clears the statistical information for the PCC-Sp-Endpoint instance named <i>sp1</i> in summarized output: <b>clear pcc-sp-endpoint statistics name sp1</b>

## clear pdg-service statistics

Deletes all previously gathered statistics for a specific Packet Data Gateway (PDG) service or all PDG services configured within a context.

<b>Product</b>	PDG/TTG
<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<b>clear pdg-service statistics [ name <i>service_name</i> ]</b>  <b>name <i>service_name</i></b> Clears the statistics for the PDG service name configured in the context, expressed as an alphanumeric string of 1 through 63 characters that is case sensitive.
<b>Usage Guidelines</b>	Usage Statistics for a single PDG service can be cleared using the name keyword. Statistics for all PDG services in the context can be deleted by entering the command with no keywords.

If this command is executed from within the local context with no keywords, statistics will be cleared for every PDG service configured on the system regardless of context. In addition, if the name keyword is used when executing from within the local context, statistics for all PDG services configured with the specified name will be cleared regardless of context.

### Example

The following command clears statistics for a PDG service named *pdg1*:

```
clear pdg-service statistics pdg1
```

## clear pgw-service

Clears PDN Gateway (P-GW) statistics and counters found in **show** command outputs and bulk statistics associated with all P-GW services or a specific service defined by the parameter in this command.

### Product

P-GW  
SAEGW

### Privilege

Operator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
clear pgw-service statistics [ name service_name ] [ [ | { grep grep_options | more } ]
```

#### **name** *service\_name*

Clears statistics and counters for an existing P-GW service name, expressed as an alphanumeric string of 1 through 63 characters.

#### **grep** *grep\_options* | **more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to clear statistics and counters in show command outputs and bulk statistics for all P-GW services or for a specific P-GW service.

### Example

The following command clears statistics and counters for an P-GW service named *pgw5*:

```
clear pgw-service statistics name pgw5
```



# clear port

Clears port related statistics.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator, Operator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
clear port { datalink counters { all | slot/port } | npu counters { all | slot/port [ untagged | vlan tag_id ] } }
```

**datalink counters**

Clears data link port statistics.

**npu counters**

Clears statistics for the network processing unit(s).

**all**

Clears counters for all datalink or NPU ports.

**slot/port**

Clears the statistics for the specified slot and port number.

**untagged**

Clears NPU statistics for all ports that do not have a VLAN tag.

**vlan tag\_id**

Clears NPU statistics for the port that has a previously configured VLAN tag ID.

---

**Usage Guidelines**

Manually clear the statistics for a specified port. This is useful when preparing to troubleshoot or monitor the system.

**Example**

The following command clears the data link related statistics for port 1 in slot 17.

```
clear port datalink counters 17/1
```

The following command clears the network processing unit related statistics for port 1 in slot 17.

```
clear port npu counters 17/1
```

The following command clears the network processing unit related statistics for port 10 in slot 5.

```
clear port npu counters 5/10
```

## clear ppp statistics

Clears point-to-point protocol (PPP) related statistics. All PPP statistics may be cleared or just those for a specific packet data service may be cleared.

---

### Product

PDSN  
GGSN

---

### Privilege

Security Administrator, Administrator, Operator

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

```
clear ppp statistics [ ggsn-service ggsn_name | lns-service lns_name |  
pcf-address [ pcf_ip_addr | all ] | pdsn-service pdsn_name |  
pdsnclosedrp-service pdsnclosedrp_name ]
```

#### **ggsn-service** *ggsn\_name*

Clears statistics only for the time the session is connected to the named GGSN service.

#### **lns-service** *lns\_name*

Clears statistics only for the time the session is connected to the named LNS service.

#### **pcf-address** [ *pcf\_ip\_addr* | **all** ]

Clears statistics only for the time the session is connected to the specified PCF (Packet Control Function) or for all PCFs. *pcf\_ip\_addr* must be entered using IPv4 dotted-decimal notation.

#### **pdsn-service** *pdsn\_name*

Clears statistics only for the named PDSN service.

#### **pdsnclosedrp-service** *pdsnclosedrp\_name*

Clears statistics only for the time the session is connected to the named PDSN Closed RP service.

---

### Usage Guidelines

Allows you to manually reset PPP statistics when it is desired to have counts begin again from a specific point in time.

### Example

The following clears the statistics for all PPP counters and services.

```
clear ppp statistics
```

The following clears only the point-to-point protocol statistics for the service named *sampleService*.

```
clear ppp statistics pdsn-service sampleService
```

## clear prepaid 3gpp2 statistics

Clears all of the statistics counters for 3GPP2 Pre-paid accounting. Statistics may be cleared for all services or for an individual service.

<b>Product</b>	PDSN GGSN
<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec  The following prompt is displayed in the Exec mode:  [local]host_name#
<b>Syntax Description</b>	<pre>clear prepaid 3gpp2 statistics { all   { ggsn-service   ha-service   lns-service   pdsn-service   pdsnclosedrp-service } { all   name service_name } }</pre> <p><b>all</b> Clears prepaid statistics for all services.</p> <p><b>ggsn-service</b> Clears statistics for GGSN service(s).</p> <p><b>ha-service</b> Clears statistics for HA service(s).</p> <p><b>lns-service</b> Clears statistics for LNS service(s).</p> <p><b>pdsn-service</b> Clears statistics for PDSN service(s).</p> <p><b>pdsnclosedrp-service</b> Clears statistics for PDSN Closed-RP service(s).</p> <p><b>{ all   name service_name }</b> <b>all:</b> Clears statistics for all services of the specified type.</p>

**name** *service\_name*: Clears statistics for the named service of the specified service type.

### Usage Guidelines

Use this command to clear Pre-paid statistics for a particular named service or for all services.

### Example

To clear statistics for a PDSN service name *PDSNI*, enter the following command:

```
clear prepaid 3gpp2 statistics pdsn-service name PDSN1
```

## clear prepaid wimax

Clears all of the statistical counters for WiMAX prepaid accounting. Statistics may be cleared for all services or for an individual service.

### Product

ASN-GW

### Privilege

Operator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
clear prepaid wimax statistics { all | asngw-service { all | name
service_name } | ha-service { all | name service_name } }
```

#### all

Clears prepaid statistics for all services.

#### asngw-service

Clears prepaid statistics for ASN-GW service(s).

#### ha-service

Clears prepaid accounting statistics for HA service(s).

#### { all | name *service\_name* }

**all**: Clears statistics for all services of the specified type.

**name** *service\_name*: Clears statistics for the named service of the specified service type.

### Usage Guidelines

Use this command to clear prepaid WiMAX accounting statistics for named service or for all services.

### Example

The following command clears prepaid WiMAX accounting statistics for an ASN-GW service name *asn1*:

```
clear prepaid wimax statistics asngw-service name asn1
```

## clear ps-network statistics



**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Clears the HNB-Packet Switched (PS) network service associated with an HNB-GW service instance.

**Product** HNB-GW

**Privilege** Operator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `clear ps-network statistics [ name cs_svc_name | gtpu-only | ranap-only | rtp-only | sccp-only ]`

**name *ps\_svc\_name***

Clears the session statistics based on an existing HNB-PS network service name, expressed as an alphanumeric string of from 1 through 63 characters.

**gtpu-only**

Clears the session statistics for GTP-U traffic only for the specified HNB-PS Network service.

**ranap-only**

Clears the session statistics for Radio Access Network Application Protocol (RANAP) traffic only for the specified HNB-PS Network service.

**sccp-only**

Clears the session statistics for Signaling Connection Control Part (SCCP) traffic only for the specified HNB-PS Network service.

**Usage Guidelines** Use this command to clear the session statistics for overall session or in selected part of user session for HNB-CS Network services configured and running on a system.

**Example**

The following command clears the session statistics for RANAP part of session for the HNB-PS Network service *hnb\_PS\_1*:

```
clear ps-network statistics name hnb_PS_1 ranap-only
```

## clear qos npu stats

Clears information pertaining to NPU QoS priority queue bandwidth allocation and sharing.

<b>Product</b>	GGSN
<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `clear qos npu stats inter-subscriber traffic slot slot_num`

### inter-subscriber traffic slot *slot\_num*

Clears inter-subscriber traffic statistics for the ASR 5000 application or line card or the ASR 5500 DPC or MIO card installed in the specified slot.

*slot\_num* indicates the number of the chassis slot in which the card is installed and can be configured to an integer value from 1 through 48 (for the ASR 5000 or 1 through 10 (for the ASR 5500).

**Usage Guidelines** Allows you to manually reset statistics pertaining to NPU QoS priority queue bandwidth allocation.

### Example

The following command clears statistics for a card installed in chassis slot 3:

```
clear qos npu stats inter-subscriber traffic slot 3
```

## clear radius accounting archive

Clears archived RADIUS accounting messages associated with an AAA group, or all the archived RADIUS accounting messages in the context in which the command is executed depending on the option chosen. The scope of the command is limited to the context in which it is executed (including the local context).



### Important

This command is only available in StarOS 8.3 and later. For more information, please contact your local service representative.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear radius accounting archive { all | radius group group_name } [
-noconfirm ]
```

**all**

Clears all archived RADIUS accounting messages in the context.

**radius group *group\_name***

Clears all archived RADIUS accounting messages for the specified RADIUS group.

*group\_name* must be the name of a RADIUS server group, and must be an alphanumeric string of 0 through 64 characters.

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

**Usage Guidelines**

Use this command to clear the archived RADIUS accounting messages associated with an AAA group, or all the archived RADIUS accounting messages in the context in which the command is executed.

**Example**

Use the following command to clear all archived RADIUS accounting messages for the group named *test12*.

```
clear radius accounting archive radius group test12
```

## clear radius counters

Clears the statistics for all RADIUS servers or a server group.

**Product**

ASN-GW  
GGSN  
PDSN  
P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear radius counters { all | radius group group_name | server ip_address [
port number ] }
```

**all | radius group *group\_name* | server *ip\_address* [ port *number* ]**

**all:** Clears statistics for all servers.

**radius group *group\_name*:** Clears all configured authentication/accounting servers in the specified RADIUS group. *group\_name* must be the name of server group configured in a specific context for authentication/accounting, expressed as an alphanumeric string of 1 through 63 characters.

**server *ip\_address* [ port *number* ]:** Clears statistics only for the server specified using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. Optionally, you can specify the port which is to have its RADIUS statistics cleared as an integer from 0 through 65535.

**Usage Guidelines**

Clears all the configured RADIUS servers' statistics to reset them to zero prior to logging or monitoring the system for troubleshooting, performance measurements, etc.

Note that this CLI command will clear all the statistics associated with the configured RADIUS accounting and authentication servers except these two counters –

- Access Request current consecutive failures in a mgr
- Accounting-Request Current Consecutive Failures in a mgr

**Example**

The following command clears the statistics for all RADIUS servers.

```
clear radius counters all
```

The following command resets the statistics only for the server *10.2.3.4*.

```
clear radius counters server 10.2.3.4
```

The following command resets the statistics only for the server group named *star1*.

```
clear radius counters radius group star1
```

## clear rlf-context-statistics

Clears the statistics for all active Rate Limiting Function (RLF) contexts.

**Product**

GGSN  
P-GW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```



**Syntax Description**

```
clear rlf-context-statistics { diamproxy [ endpoint endpoint_name [ peer-realm
realm_name [ peer-host host_name ] ] ] | sessmgr [ gtpc-context-name
context_name grep_options ] ingress ] } [ | { grep | more } ]
```

**endpoint** *endpoint\_name*

Clears the context information only for the endpoint specified as a string of size ranging from 1 through 63 characters.

**realm** *realm\_name*

Clears the context information only for the realm specified as a string of size ranging from 1 through 127 characters.

**peer-host** *host\_name*

Clears the context information only for the host specified as a string of size ranging from 1 through 63 characters.

**grep** *grep\_options* | **more**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to clear the statistics for all active RLF contexts.

**Example**

The following command clears the statistics for all active RLF contexts:

```
clear rlf-context-statistics diamproxy
```

## clear rohc statistics

Clears statistics and counters collected since the last reload or **clear** command was issued for ROust Header Compression (ROHC) [RFC 3095].

**Product**

PDSN  
ASN-GW  
HSGW

**Privilege**

Administrator, Config-administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `clear rohc statistics [ pdsn-service pdsnsvc_name | asngw-service asngwsvc_name`

**pdsn-service *pdsnsvc\_name***

Clears ROHC statistics and counters for the specified PDSN service.

**asngw-service *asngwsvc\_name***

Clears ROHC statistics and counters for the specified ASN-GW service.

---

**Usage Guidelines** Use this command to clear ROHC statistics for all services or for a specific PDSN or ASNGW service.

**Example**

The following command clears ROHC statistics and counters for the PDSN service named *pdsn1*:

```
clear rohc statistics pdsn-service pdsn1
```

## clear rp service-option

Clears the radio-packet (R-P) interface service option statistics.

---

**Product** PDSN

---

**Privilege** Security Administrator, Administrator, Operator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `clear rp service-option statistics [ number option_num | pdsn-service pdsn_name`  
`]`

**number *option\_num* | pdsn-service *pdsn\_name***

Default: clears the statistics for all service options and all packet data services.

**number *option\_num***: Specifies the R-P service option number for which the statistics are to be cleared as an integer from 0 through 1000.

**pdsn-service *pdsn\_name***: Specifies the PDSN service name for which statistics will be cleared.

---

**Usage Guidelines** Clear the R-P service option statistics prior to monitoring the system for bench marking or for detecting areas of further research.

**Example**

The following resets the service option statistics for service option 23 and packet data service *sampleService*, respectively.

```
clear rp service-option statistics number 23
clear rp service-option statistics pdsn-service sampleService
```

## clear rp statistics

Clears the radio-packet (R-P) interface statistics. The statistics for a specific packet data server or peer node may be cleared if specified.

<b>Product</b>	PDSN
<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<pre>clear rp statistics [ pdsn-service name   peer-address [ peer_address   all ] ]</pre> <p><b>pdsn-service name   peer-address [ peer_address   all ]</b></p> <p>Default: clears all R-P associated statistics.</p> <p><b>pdsn-service name</b>: Specifies the packet data service name that is to have its statistics reset.</p> <p><b>peer-address [ ip_address   all ]</b>: Specifies that statistics for the specified peer, or all peers, are to be cleared. The <i>ip_address</i> must be specified using IPv4 dotted-decimal notation.</p>
<b>Usage Guidelines</b>	Clear the statistics to prepare for monitoring the system.

### Example

The following command resets all the associated statistics for the R-P interfaces.

```
clear rp statistics
```

The following command clears the statistics for the packet data service *sampleService*.

```
clear rp statistics pdsn-service sampleService
```

The following command resets the statistics associated with peer node with IP address *10.2.3.4*.

```
clear rp statistics peer-address 10.2.3.4
```

## clear rsvp statistics

Clears the Resource Reservation Protocol (RSVP) statistics.

<b>Product</b>	All
----------------	-----

**clear saegw-service**


---

**Privilege** Security Administrator, Administrator, Operator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **clear rsvp statistics**

---

**Usage Guidelines** Clear RSVP statistics.

### Example

The following command resets all RSVP statistics.

```
clear rsvp statistics
```

## clear saegw-service

Clears System Architecture Evolution Gateway (SAEGW) statistics and counters found in **show** command outputs and bulk statistics associated with all SAEGW services or a specific service defined by the parameter in this command.

---

**Product** SAEGW

---

**Privilege** Operator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **clear saegw-service statistics { all | name *service\_name* } [ | { **grep** *grep\_options* | **more** } ]**

### **all**

Clears all SAEGW node-level statistics.

### **name *service\_name***

Clears statistics and counters for an existing SAEGW service name, expressed as an alphanumeric string of 1 through 63 characters.

### **grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to clear statistics and counters in show command outputs and bulk statistics for all SAEGW services or for a specific SAEGW service.

**Example**

The following command clears statistics and counters for an SAEGW service named *saegw5*:

```
clear saegw-service statistics name saegw5
```

## clear samog-service statistics

Clear statistics associated with S2a Mobility Over GTP (SaMOG) services.

**Product**

SAMOG

**Privilege**

Inspector

**Syntax Description**

```
clear samog-service statistics samog_service_name
```

**clear samog-service statistics *samog\_service\_name***

Clears SaMOG service-related statistical information. Service name should be between 1 and 63.

**Usage Guidelines**

Use this command to clear statistics and counters in show command outputs and bulk statistics for all SaMOG services or for a specific SaMOG service.

**Example**

The following command clears SaMOG Statistics 21 :

```
clear samog-service statistics 21
```

## clear sbc statistics

Clears SBC service statistics based on various criteria.

**Product**

MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear sbc statistics { all | peer-id peer_id | sbc-service-name sbc_svc_name } | { | grep grep_options | more } ]
```

**all**

Clears statistics for all SBs services.

**peer-id *peer\_id***

Clears statistics for a Cell Broadcast Center (CBC) peer association specified as an integer value from 0 through 4294967295.

Use the **show sbc-service cbc-associations all** command to display the available CBC association peer IDs.

**sbc-service-name *sbc\_svc\_name***

Clears all statistics for an existing SBC service specified as an alphanumeric string of 1 through 63 characters.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to clear the statistical information of an SBC service based on various filter criteria.

**Example**

The following command clears all statistics for the SBC service named *sbc1*

```
clear sbc statistics sbc-service-name sbc1
```

## clear sccp statistics

Clears SS7 Signaling Connection Control Part (SCCP) statistics collected for services that use the SCCP protocol.

**Product**

SGSN

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear sccp statistics [ iups-service iups_srvc_name | map-service map_srvc_name
| sccp-network ntwk_index [ dpc dpc [ ssn ssn ] | global-title-translation
{ address-map instance add_map_inst | association instance assoc_inst } [
sessmgr instance sessmgr_inst ] ] [ | { grep grep_options | more } ]
```

**iups-service *iups\_srvc\_name***

Deletes collected SCCP protocol statistics for an existing Iu-PS service in the current context specified as an alphanumeric string of 1 through 63 characters.

**map-service *map\_srvc\_name***

Deletes collected SCCP protocol statistics for an existing MAP service specified as an alphanumeric string of 1 through 63 characters.

**sccp-network *ntwk\_index***

Deletes collected SCCP protocol statistics for the SCCP network configuration with the a network index specified as an integer from 1 through 12.

The following filters can be added to limit the clearing of SCCP network statistics:

- **dpc *dpc***: Specifies a differentiated pointcode address to limit the deletion of collected SCCP network statistics to those for the identified destination.
- **ssn *ssn***: Specifies a subsystem number as an integer from 1 to 255 to limit the deletion of collected SCCP network statistics.
- **global-title-translation address-map instance *add\_map\_inst***: Specifies an identified GTT address-map as an integer from 1 to 4096 to limit the deletion of collected SCCP network statistics.
- **global-title-translation association instance *assoc\_inst***: Specifies an identified GTT association as an integer from 1 to 16 to limit the deletion of collected SCCP network statistics.
- **sessmgr instance *sessmgr\_inst***: Specifies an identified session manager instance as an integer from 1 to 384 to limit the deletion of collected SCCP network statistics.

**Usage Guidelines**

Use this command to delete all collected SCCP statistics or to delete SCCP statistics for a specified service, SCCP network, or session manager.

**Example**

The following command deletes all collected SCCP statistics:

```
clear sccp statistics
```

The following command clears all collected SCCP statistics for the IuPS service named *iups-serv1*:

```
clear sccp statistics iups-service iups-serv1
```

# clear security

Clears the database statistics maintained by the system for the specified Talos Intelligence server.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `clear security server talos-intelligence server_name`

**server\_name**

Specifies the name of the Talos Intelligence server for which database statistics will be cleared. *server\_name* must be an alphanumeric string of 1 through 63 characters.

---

**Usage Guidelines** Use this command to reset the database statistics maintained by the system for the specified Talos Intelligence server.

## clear session disconnect-reasons

Clears the session disconnect reason statistics for all sessions on the system.

---

**Product** All

---

**Privilege** Security Administrator, Administrator, Operator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `clear session disconnect-reasons [ buckets ]`

**[ buckets ]**

This keyword option clears session disconnect reason statistics only from the three indexed buckets that may be associated with all session managers. The buckets are created when the Exec mode **session disconnect-reasons bucket-interval** command is enabled.

---

**Usage Guidelines** Sets the counters for session disconnect reasons to zero (0) in preparation for a monitoring or troubleshooting session.

### Example

```
clear session disconnect-reasons
```

## clear session-event-record statistics

Clears statistics collected during session event module transfers.

---

**Product** S-GW



SAEGW

**Privilege**

Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear session-event-record statistics
```

**Usage Guidelines**

Use this command to delete all collected session event record statistics.

## clear session setuptime

Clears the session setup time statistics for Packet Control Functions (PCFs) or SGSNs. If no keyword is specified the summary statistics displayed by the **show session setuptime** command are cleared.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear session setuptime [ pcf [ pcf_addr | all ] | sgsn-address [ sgsn_addr | all ]
```

```
pcf [ pcf_addr | all ]
```

*pcf\_addr*: Clears the setup time counters for the PCF at the IP address specified in IPv4 dotted-decimal notation.

**all**: Clears the setup time counters for all PCFs.

```
sgsn-address [ sgsn_addr | all ]
```

*sgsn\_addr*: Clears the setup time counters for the SGSN at the IP address specified in IPv4 dotted-decimal notation.

**all**: Clears the setup time counters for all SGSNs.

**Usage Guidelines**

Sets the counters for session disconnect reasons to zero (0) in preparation for a monitoring or troubleshooting session.

**Example**

To clear the statistics for the PCF at IP address *192.168.100.10*, enter the following command:

```
clear session setuptime pcf 192.168.100.10
```

## clear session subsystem

Clears all session subsystem statistics for the current context.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator, Operator

<b>Command Modes</b>	Exec
	The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

<b>Syntax Description</b>	<code>clear session subsystem</code>
---------------------------	--------------------------------------

<b>Usage Guidelines</b>	Clears the statistics in preparation for a troubleshooting or monitoring session so that the counters are at a well known values.
-------------------------	---

### Example

```
clear session subsystem
```

## clear sgsn-fast-path statistics

Clears information related to SGSN fast-path.



<b>Note</b>	This command is not supported by SGSN from software release 16.2 onwards as the NPU FastPath feature is not supported by SGSN from the 16.2 release.
-------------	--

<b>Product</b>	SGSN
----------------	------

<b>Privilege</b>	Inspector
------------------	-----------

<b>Command Modes</b>	Exec
----------------------	------

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

<b>Syntax Description</b>	<code>show sgsn-fast-path statistics [ all   smgr-instance smgr_inst ] [   { grep grep_options   more } ]</code>
---------------------------	--

### all

Deletes collected fast-path statistics for all session managers.

**smgr-instance *smgr\_inst***

Clears collected fast-path statistics for a session manager instance specified as an integer from 1 to 65535.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Please refer to the *Regulating the Command Output* section in this reference for details on the usage of **grep** and **more**.

**Usage Guidelines**

Use this command to clear all statistics for SGSN fast-path configurations.

**Example**

The following command deletes all collected fast-path statistics for all SGSN session managers:

```
clear sgsn-fast-path statistics
```

## clear sgsn-map-app

Deletes collected statistics for the SGSN Mobile Application Part (MAP).

**Product**

SGSN

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear sgsn-map-app statistics [ | { grep grep_options | more } ]
```

**clear sgsn-map-app statistics**

Clears all collected statistics for the SGSN MAP application.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Please refer to the *Regulating the Command Output* section in this reference for details on the usage of **grep** and **more**.

**Usage Guidelines**

Use this command to delete collected statistics for the SGSN MAP application.

**Example**

The following command clears all collected SGSN MAP statistics:

```
clear sgsn-map-app statistics
```

## clear sgsn rlf-context-statistics

Clears the Paging throttle RLF context statistics.

---

**Product** SGSN

---

**Privilege** Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **clear sgsn rlf-context-stats sessmgr** { **all** | **instance** *<instance\_value>* } [ **peer-nsei-id** *<NSE\_identifier>* | **peer-rnc-id** *<RNC\_identifier>* ] [ | { **grep** *grep\_options* | **more** } ]

### **sessmgr**

Clears the RLF statistics specific to Session Managers.

### **all**

Clears the RLF context statistics for all the Session Managers.

### **instance**

Clears the RLF context statistics for the specified Session Manager.

### ***instance\_value***

The Session Manager instance specified as an integer from 1 to 384.

### **peer-nsei-id**

Specifies the Peer NSEI ID for which RLF context statistics need to be cleared.

### ***NSE\_identifier***

The Peer NSEI identifier specified as an integer from 0 to 65535.

### **peer-rnc-id**

Specifies the Peer RNC ID for which RLF context statistics need to be cleared.

### ***RNC\_identifier***

The Peer RNC identifier specified as an integer from 0 to 65535.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Please refer to the *Regulating the Command Output* section in this reference for details on the usage of **grep** and **more**.

**Usage Guidelines**

This command can be configured to clear the Paging throttle RLF context statistics for:

- All the Session Managers.
- The specified Session Manager.
- The specified Peer NSEI.
- The specified Peer RNC.

The keyword **sessmgr** is a mandatory keyword. Specifying the **peer-nsei-id** or **peer-rnc-id** is optional. When the **peer-nsei-id** or **peer-rnc-id** is not specified the global statistics are cleared. If the Session Manager instance is specified, the RLF context statistics for that Session Manager are cleared. If the keyword **all** is configured the RLF statistics for all the Session Managers are cleared.

**Example**

The following command clears the Paging throttle RLF context statistics for all the Session Managers:

```
clear sgsn rlf-context-statistics sessmgr all
```

# clear sgs-service

Clears SGs interface statistics associated with a Visitor Location Register (VLR).

**Product**

MME

**Privilege**

Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear sgs-service { statistics [ name name ] | vlr-status [ service-name name ] [ vlr-name name ] }
```

**statistics [ name *name* ]**

Clears statistics for all SGs services or a specific SGs service.

**name *name***: Clears the statistics for an existing SGs service specified as an alphanumeric string of 1 through 63 characters.

**vlr-status [ service-name *name* ][ vlr-name *name* ] }**

Clears statistics for all VLRs, a VLR related to a SGs service, or a specific VLR.

**service-name name:** Clears the SGs statistics for an existing VLR specified as an alphanumeric string of 1 through 63 characters.

### Usage Guidelines

Use this command to clear statistics for all SGs services, Visitor Location Registers (VLRs), or a specific SGs service or VLR name.

### Example

The following command clears statistics for an SGs service named *sgs2*:

```
clear sgs-service statistics name sgs2
```

## clear sgtpc statistics

Clears all SGSN GTP-C (SGTPC) interface statistics for the current context.

### Product

MME  
SGSN

### Privilege

Security Administrator, Administrator, Operator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
clear sgtpc statistics [ gsn-address ipv4_address | sgtp-service sgtp_srvc_name ]
```

#### **gsn-address *ipv4\_address***

Clears GTPC packet statistics for the interface specified as an IP address in IPv4 dotted-decimal notation.

#### **sgtp-service *sgtp\_srvc\_name***

Clears GTPC packet statistics for an existing SGTP service specified as an alphanumeric string of 1 through 63 characters.

### Usage Guidelines

Use this command to clear the statistics in preparation for a troubleshooting or monitoring session.



#### Important

Statistics are vital for troubleshooting. We recommend that you check with your Cisco support personnel prior to clearing these statistics.

### Example

```
clear sgtpc statistics sgtp-service SGSN1sgtp12
```

# clear sgtpu statistics

Clears all SGSN GTP-U (SGTPU) statistics for the current context.

**Product** SGSN

**Privilege** Security Administrator, Administrator, Operator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **clear sgtpu statistics** [ **ggsn-address** *ipv4\_address* | **gprs-service** *gprs\_srvc\_name* **nsei** *nse\_id* | **iups-bind-address** *ipv4\_address* | **iups-service** *iups\_srvc\_name* | **recovered-values** | **rnc-address** *ipv4\_address* | **sgtp-service** *sgtp\_srvc\_name* ]

## **ggsn-address** *ipv4\_address*

Clears GTPU packet statistics for a specific GGSN specified as an IP address in IPv4 dotted-decimal notation.

## **gprs-service** *gprs\_srvc\_name* **nsei** *nse\_id*

**gprs-service** *gprs\_srvc\_name*: Clears GTPU packet statistics for the interface for a specific GPRS service specified as an alphanumeric string of 1 through 63 characters.

**nsei** *nse\_id*: Specifies a network service entity (NSEI) as an integer from 0 through 65535.

## **iups-bind-address** *ipv4\_address*

Clears GTPU packet statistics for the bind address of an IuPS interface specified as an IP address in IPv4 dotted-decimal notation.

## **iups-service** *iups\_srvc\_name*

Clears GTPU packet statistics for an active IuPS service interface specified as an alphanumeric string of 1 through 63 characters.

## **recovered-values**

Clears only recovered values for key SGTP KPI counters that were backed-up.

To narrow the results, this keyword can be combined with either the **iups-service** or the **sgtp-service** keywords.

## **rnc-address** *ipv4\_address*

Clears GTPU packet statistics for an RNC specified as an IP address in IPv4 dotted-decimal notation.

## **sgtp-service** *sgtp\_srvc\_name*

Clears GTPU packet statistics for an active SGTP service interface specified as an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to clear the statistics in preparation for a troubleshooting or monitoring session.

**Important**

Statistics are vital for troubleshooting. We recommend that you check with your Cisco support personnel prior to clearing these statistics.

**Example**

Use this command to clear collected SGTPU statistics for a specific NSEI of a configured GPRS service:

```
clear sgtpu statistics gprs-service SGSN1Gprs1 nsei 2445
```

## clear sgw-service statistics

Clears Serving Gateway (S-GW) statistics and counters found in **show** command outputs and bulk statistics associated with all S-GW services or a specific service defined by the parameter in this command.

**Product**

S-GW  
SAEGW

**Privilege**

Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear sgw-service statistics { all | name service_name }
```

**all**

Clears statistics and counters for all S-GW services configured on the system.

**name *service\_name***

Clears statistics and counters for an existing S-GW service name specified as an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to clear statistics and counters in show command outputs and bulk statistics for all S-GW services or for a specific S-GW service.

**Example**

The following command clears statistics and counters for an S-GW service named *sgw3*:

```
clear sgw-service statistics name sgw3
```



# clear sls-service statistics

Clears SLs service statistics based on various criteria.

---

**Product**

MME

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
clear sls-service statistics [ name svc_name ] [ sls | sctp ] [ esmlc-id esmlc-id ] [ | { grep grep_options | more } ]
```

**name** *svc\_name*

Clears all statistics for an existing SLs service specified as an alphanumeric string of 1 through 63 characters

**sls**

Clears only SLs interface related statistics.

**sctp**

Clears only SCTP related statistics.

**esmlc-id** *esmlc-id*

Clears all statistics for an existing E-SMLC peer specified as an integer value from 0 through 255.

**grep** *grep\_options* | **more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

This command is used to clear the statistical information of an SLs service based on various filter criteria.

**Example**

The following command clears only the SCTP statistics for the SLs service named *sls1*:

```
clear sls-service statistics name sls1 sctp
```

## clear sms statistics

Deletes collected traffic statistics for the Short Message Service (SMS).

---

**Product**

SGSN

---

**Privilege**

Administrator, Security Administrator, Operator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
clear sms statistics [ name map_srvc ] [ recovered-values ] [ | { grep
grep_options | more } ]
```

**name** *map\_srvc*

Specifies a MAP Service as an alphanumeric string of 1 to 63 characters.

**[ recovered-values ]**

Clears only recovered values for key SMS KPI counters that were backed-up.

**grep** *grep\_options* | **more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

---

**Usage Guidelines**

Use this command to delete collected traffic statistics for SMS. It is possible to clear the statistics of a specific MAP service associated with the SMS by including the **name** filter.

**Example**

Use the following command to clear SMS statistics for MAP service *MAP-LONDON1*:

```
clear sms statistics name MAP-LONDON1
```

## clear sndcp statistics

Deletes all collected statistics for the packet traffic going through the Subnetwork Dependent Convergence Protocol (SND CP) layer.

---

**Product**

SGSN

---

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear sndcp statistics [ gprs-service svrc_name ] [ | { grep grep_options | more } ]
```

**gprs-service *svrc\_name***

Specifies a GPRS service as an alphanumeric string of 1 through 63 characters.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage Guidelines**

Use this command to delete all collected SNDCP traffic statistics. Include the **gprs-service** keyword to filter the clearing action to only deleted statistics for one GPRS service.

**Example**

Use the following command to clear all collected SNDCP layer traffic statistics:

```
clear sndcp statistics
```

Use the following command to delete SNDCP layer traffic statistics for the *test1* GPRS service:

```
clear sndcp statistics gprs-service test1
```

## clear snmp trap

Clears all SNMP event trap notifications from the buffer.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear snmp trap { history | statistics }
```

**history**

Clears all SNMP historical trap information from the system buffer.

**statistics**

Clears all SNMP event trap information from the system buffer.

**Usage Guidelines**

Use this command to empty the buffer of all SNMP trap notifications.

**Example**

The following command clears the all historical SNMP traps from the system buffer:

```
clear snmp trap history
```

# clear srp

Clears system Service Redundancy Protocol (SRP) statistics.

**Product**

All products that support Interchassis Session Recovery (ICSR)

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear srp { audit-statistics | call-loss statistics | checkpoint statistics
           | statistics }
```

**audit-statistics**

Clears SRP audit statistics.

**call-loss statistics**

Clears SRP call loss history.

**checkpoint statistics**

Clears SRP checkpoint interface statistics.

**statistics**

Clears SRP statistics.

**Usage Guidelines**

Clears the SRP statistics to prepare the system for SRP monitoring.

**Example**

The following command resets all the associated statistics for SRP checkpoints.

```
clear srp checkpoint statistics
```

The following command resets all the associated statistics for SRP.

```
clear srp statistics
```

## clear ss7-routing-domain

Deletes specified statistics for an SS7 routing domain.

---

### Product

SGSN

---

### Privilege

Security Administrator, Administrator, Operator

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

```
clear ss7-routing-domain domain_index { asp | mtp2 | mtp3 | qsaal | sscf }
```

#### ***domain\_index***

Specifies the index number of the SS7 routing domain as an integer from 1 through 12.

#### **asp**

Clears statistics and status information for the SS7 Application Service Part (ASP) in the specified SS7 routing domain.

#### **m3ua**

Clears statistics and status information for the SS7 MTP3 User Adaptation Layer (M3UA) in the specified SS7 routing domain.

#### **mtp2**

Clears statistics and status information for the SS7 Message Transfer Part-2 (MTP2) in the specified SS7 routing domain.

#### **mtp3**

Clears statistics and status information for the SS7 Message Transfer Part-3 (MTP3) in the specified SS7 routing domain.

#### **qsaal**

Clears statistics and status information for the Service Specific Connection-Oriented Protocol (SSCOP) sub-layer of the Quasi Signaling Application Adaptation Layer (QSAAL) in the specified SS7 routing domain.

#### **sscf**

Clears statistics and status information for the Service Specific Coordination Function (SSCF [q.2140]) in the specified SS7 routing domain.

**Usage Guidelines** Deletes statistics for the specified SS7 routing domain.

### Example

The following command clears SS7 ASP routing statistics for domain index 4:

```
clear ss7-routing-domain 4 asp
```

## clear subscribers

Disconnects subscribers based on specified criteria.

**Product** All

**Privilege** Security Administrator, Administrator, Operator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `clear subscribers [ keywords ] [ verbose ] [ -noconfirm ]`

The keywords are filters that modify or filter the criteria for deciding which subscriber sessions to clear and are described below. Multiple keywords can be entered on a command line.

When multiple keywords are specified, the subscriber sessions deleted must meet the specifications of all of the keywords.

For example; if you enter the following command:

```
clear subscribers ip-pool pool1 card-num 1
```

Only subscriber sessions that were assigned an IP address from the IP pool named *pool1* and are also being processed by the processing card in slot *1* are cleared. All other subscriber sessions that do not meet these criteria remain and are not cleared.



### Important

Calls already marked as disconnecting will not be designated for clearing. For example, if 100 calls are temporarily in the disconnecting state, the **show subscribers all** command output displays all 100 calls. However, the **clear subscribers all** command output will indicate that there are no calls available for clearing, since they are already in the disconnecting state.

### **-noconfirm**

Executes the command without any additional prompt and confirmation from the user.



### Important

The Operator privilege does not have access to this keyword.

**active**

Only disconnects subscribers who currently have active sessions.

**active-charging-service *ecs\_service\_name***

Clears information for subscribers using the Active charging Service.

*ecs\_service\_name* must be the name of the Active Charging Service, expressed as an alphanumeric string of 1 through 15 characters.

**all**

Disconnects all subscribers.

**Important**

The Operator privilege does not have access to this keyword.

**apn *apn\_name* [ *rulename rule\_name* | **without-dynamic-rule** | **without-override-control** ]**

Clears all PDP contexts accessing a specific access point name (APN).

*apn\_name* is the name of the APN expressed as an alphanumeric string of 1 through 63 characters that is case sensitive.

[ *rulename rule\_name* | **without-dynamic-rule** | **without-override-control** ]

**rulename** *rule\_name* is the charging rule name.

**without-dynamic-rule** refers to subscribers without any dynamic rule associated with them.

**without-override-control** refers to subscribers without any override control rule associated with them.

**asn-peer-address *ip\_address***

Clears information for subscribers on an ASN-GW trusted peer.

*ip\_address* is the address of the ASN-GW peer server entered using IPv4 dotted-decimal notation.

**asn-gw-service *service\_name***

Clears counters for subscribers accessing the ASN-GW service.

*service\_name* must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

**asn-pc-service *service\_name***

Clears counters for subscribers accessing the ASN PC service.

*service\_name* must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

**bandwidth-policy *bandwidth\_policy\_name***

Clears information for subscribers using the specified bandwidth policy.

*bandwidth\_policy\_name* must be the name for an existing bandwidth policy, expressed as an alphanumeric string of 1 through 63 characters.

**bearer-establishment { direct-tunnel | normal | pending }**

Clears all subscribers from the specified bearer establishment type.

**direct-tunnel:** Select subscribers having direct tunnel established with the RNC.

**normal:** Select subscribers having bearer established with SGSN.

**pending:** Select subscribers for whom bearer is not fully established.

**bng-only**

Clears information related to BNG calls only.

**bng-service *service\_name***

Clears all subscribers from the specified BNG service.

*service\_name* must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

**callid *id***

Clears the call specified by *call\_id*. The call ID must be specified as a 4-byte hexadecimal number.

**card-num *card\_num***

The slot number of the processing card by which the subscriber session is processed. *card\_num* is a slot number from 1 through 7 or 10 through 16 (for the ASR 5000) or from 1 through 4 or 7 through 10 (for the ASR 5500).

**cbb-policy *cbb\_policy\_name***

Clears information for subscribers using the specified CBB policy.

*cbb\_policy\_name* must be the name for an existing CBB policy expressed as an alphanumeric string of 1 through 63 characters.

**ccoa-only**

This option clears the subscribers that registered a MIP co-located COA directly with the HA.

This option is only valid when MIPHA session license is enabled.

**cgw-only**

Clears information related to CGW calls only.

**configured-idle-timeout [ < | > | greater-than | less-than ] *value***

Disconnects subscribers whose idle timeout matches the specified criteria. A value of 0 (zero) indicates that the subscribers idle timeout is disabled.

<: Filters output so that only information less than the specified value is cleared.

>: Filters output so that only information greater than the specified value is cleared.

**greater-than:** Filters output so that only information greater than the specified value is cleared.

**less-than:** Filters output so that only information less than the specified value is cleared.



*value*: If no other filtering options are specified only output matching *value* is cleared. If *value* is not specified all data is cleared. *value* must be an integer from 0 through 4294967295.

**connected-time [ < | > | greater-than | less-than ] *value***

Disconnects subscribers who have been connected for the specified length of time.

<: Filters output so that only information less than the specified value is cleared.

>: Filters output so that only information greater than the specified value is cleared.

**greater-than**: Filters output so that only information greater than the specified value is cleared.

**less-than**: Filters output so that only information less than the specified value is cleared.

*value*: If no other filtering options are specified only output matching *value* is cleared. If *value* is not specified all data is cleared. *value* must be an integer from 0 through 4294967295.

**css-delivery-sequence *name***



**Important**

This is a restricted keyword. In StarOS 9.0 and later, this keyword is obsolete.

**css-service *name***



**Important**

This is a restricted keyword. In StarOS 9.0 and later, this keyword is obsolete.

**del-cause { none | reactiv-req }**

When subscribers are deleted, the GGSN/P-GW/SAEGW may include "Cause-IE" in the resulting Delete Bearer/Delete PDP Context Requests generated for default bearer.

**none**: Omit GTP "Cause-IE" in DBR/DPC generated for default bearer.

**reactiv-req**: The DBR/DPC will include "Cause-IE" with GTP cause code "Reactivation Requested".

The behavior for "Cause-IE" will be effective only if the **clear subscribers** command results in the sending of a Delete Bearer Request for default bearer, or Delete PDP Context is sent to delete the PDN connection or its last PDP context.

The behavior for "Cause-IE" specified in this CLI shall override the cause-code set by existing features.



**Important**

This option is only valid when Cause IE Enhancement for Delete Bearer Request license is enabled. Contact your Cisco account representative for more information.

**dhcp-server *address***

Clears all PDP contexts that currently possess an IP address assigned from a specific DHCP server. *dhcp\_address* is the IP address of the DHCP server expressed in IPv4 dotted-decimal notation.

**dormant**

Only disconnects subscriber sessions that are dormant (not transmitting or receiving data).

**ebi *number***

Clears subscribers based on an EPS bearer identity (EBI). *number* must be a valid EBI and an integer value from 5 to 15.

**enodeb-address *ip\_address***

Clears subscribers based on the eNodeB to which they are attached. *ip\_address* must be a valid IP address of an existing eNodeB entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**epdg-address *ip\_address***

Clears subscribers based on the ePDG to which they are attached. *ip\_address* must be a valid IP address of an existing ePDG entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

The following filter keywords are valid with this command:

```
epdg-address, epdg-service,
```

**epdg-service *service\_name***

Clears subscribers of a configured ePDG service. *service\_name* must be a valid string of size 1 to 63.

The following filter keywords are valid with this command:

```
epdg-address, epdg-service
```

**fa *ip\_address***

Disconnects all subscribers connected to the foreign agent specified by the IP address in IPv4 dotted-decimal notation.

**fa-service *fa\_name***

Disconnects all subscribers connected to an existing foreign agent name.

**firewall { *not-required* | *required* }**

Clears all subscriber information for the specified subscribers:

**not-required:** Subscribers for whom firewall processing is not-required.

**required:** Subscribers for whom firewall processing is required.

**firewall-policy *fw\_policy\_name***

This keyword is obsolete.

**fw-and-nat policy *fwnat\_policy\_name***

Clears information for subscribers using the specified Firewall-and-NAT policy.

*fwnat\_policy\_name* must be the name of an existing Firewall-and-NAT policy expressed as an alphanumeric string of 1 through 63 characters.

**fng-service *service\_name***

Clears subscriber sessions connected to the FNG service. *service\_name* must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

**ggsn-service *name***

Clears all PDP contexts accessing an existing GGSN service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**gprs-only *lai mcc mobile\_country\_code mnc mobile\_network\_code lac location\_area\_code***

Notes:

- **gprs-only**: Specifies the clearing of SGSN 2G subscribers only.
- **lai**: Specifies location area identity.
- **mcc *mobile\_country\_code***: Specifies mobile country code. *mobile\_country\_code* must be a string of size 3 to 3 ranging from 100 through 999.
- **mnc *mobile\_network\_code***: Specifies mobile network code. *mobile\_network\_code* must be a string of size 2 to 3 ranging from 00 through 999.
- **lac *location\_area\_code***: Specifies location area code. *location\_area\_code* must be an integer from 1 to 65535.

**gprs-service *name***

Clears all PDP contexts associated with the 2G SGSN. This keyword can be used with filtering keywords that are part of the **clear subscriber** command set.

Using this keyword can trigger a network-initiated service request (paging) procedure.

*name* identifies a specific GPRS service configuration expressed as an alphanumeric string of 1 through 63 characters.

**gsm-traffic-class { *background* | *conversational* | *interactive* { *priority* } | *streaming* }**

Subscribers whose traffic matches the specified 3GPP traffic class.

- **background**: 3GPP QoS background class.
- **conversational**: 3GPP QoS conversational class.
- **interactive**: 3GPP QoS interactive class. Must be followed by a traffic priority. priority can be configured to any integer value from 1 to 3.
- **streaming**: 3GPP QoS streaming class.

**gtpu-bind-address *ip\_address***

Disconnects all subscribers connected to the GTP-U service bind address.

*ip\_address* must be specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**gtpu-service *service\_name***

Disconnects all subscribers and erases subscriber information based on the GTP-U service name.

*service\_name* must be an existing GTP-U service expressed as an alphanumeric string of 1 through 63 characters.

**gtp-version**

Displays the specific GTP version number. Must be followed by one of the supported GTP versions (0 or 1).

The following filter keywords are valid with this command:

active-charging-service, apn, asngw-service, asnpc-service, asn-peer-address, bearer-establishment, callid, card-num, coaa-only, configured-idle-timeout, connected-time, dhcp-server, fa, fa-service, firewall, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, ha, ha-ipsec-service, ha-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, network-requested, network-type, pcf, pdg-service, pdif-service, pdsn-service, pdsnclosedrps-service, plmn-type, rulebase, rx-data, session-time-left, sgsn-address, sgsn-service, tx-data, username, grep, more

**ha address**

Disconnects all subscribers connected to the home agent.

*ha\_address* must be specified using IPv4 dotted-decimal notation.

**ha-ipsec-only**

Disconnects all MIP HA sessions with IPsec tunnels.

**ha-service name**

Disconnects all subscribers connected to the home agent specified by *ha\_name* must have been previously defined.

**henbgw-access-service *svc\_name*****Important**

In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

Disconnects all subscribers and erases subscriber information based on the HeNB-GW access service name.

**henbgw-only****Important**

In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

Disconnects subscribers emerging from a HeNBGW service configured on this system.

**hnbgw-service *svc\_name*****Important**

In Release 20 and later, HNBGW is not supported. This keyword must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Disconnects all subscribers and erase subscriber information based on the HNB-GW service name.

*svc\_name* must be an existing HNB-GW service expressed as an alphanumeric string of 1 through 63 characters.

**hsgw-only**

Disconnects subscribers emerging from a HRPD Serving Gateway (HSGW) service configured on this system.

**hsgw-service *name***

Disconnects subscribers using this HRPD Serving Gateway (HSGW) service configured on this system. *name* must be an existing HSGW service expressed as an alphanumeric string of 1 through 63 characters.

**idle-time [ < | > | greater-than | less-than ] *value***

Disconnects subscribers whose idle time matches the specified length of time.

<: Filters output so that only information less than the specified value is cleared.

>: Filters output so that only information greater than the specified value is cleared.

**greater-than**: Filters output so that only information greater than the specified value is cleared.

**less-than**: Filters output so that only information less than the specified value is cleared.

*value*: If no other filtering options are specified only output matching *value* is cleared. If *value* is not specified all data is cleared. *value* must be an integer from 0 through 4294967295.

**imei *imei***

SGSN only.

Disconnects one or more subscribers based on the international mobile equipment identity (IMEI or IMEI-SV) of the subscriber's mobile equipment.

*imei* - enter 14 to 16 digits to match the first 14 digits of a retrieved IMEI/IMEISV for a single subscriber. to match a range of subscribers, the string may be shorter and include '\$' as a wildcard for a single digit or '\*' as a wildcard for multiple digits.

**ims-auth-service *imsa\_service\_name***

Disconnects subscribers using this IMS Authorization Service configured on this system.

*imsa\_service\_name* must be an existing IMS Authorization Service expressed as an alphanumeric string of 1 through 63 characters.

**imsi *id***

Disconnects the subscriber with the specified id. The IMSI (International Mobile Subscriber Identity) ID is a 50-bit field which identifies the subscriber's home country and carrier. Wildcard characters \$ and \* are allowed. The \* wildcard matches multiple characters and the \$ wildcard matches a single character. If you do

not want the wildcard characters interpreted as a wildcard enclose them in single quotes ( ' ). For example; '\$'.

### **interface-type { S2bGTP | S5S8GTP }**

Disconnects subscribers based on their interface type.

**S2bGTP**: Indicates that the GTP protocol is used on the S2b interface for the subscribers being disconnected.

**S5S8GTP**: Indicates that the GTP protocol is used on the S5/S8 interface for the subscribers being disconnected.

### **ip-address *ip\_address***

Disconnects all subscribers connected to the specified *ip\_address*. The address must be specified using IPv4 dotted-decimal notation.

**Note**: This keyword is not supported for use with the MME or SGSN.

### **ip-alloc-method { aaa-assigned | dhcp [ relay-agent | proxy-client ] | dynamic-pool | l2tp-lns-assigned | mip-ha-assigned | ms-provided-static | not-ms-provided-static | static pool }**

Displays the specific IP Allocation Method. Must be followed by one of the IP Allocation Methods:

- **aaa-assigned**: Selects subscribers whose IP Addresses were assigned by AAA.
- **dhcp**: Selects subscribers whose IP Addresses were assigned by DHCP.
- **dynamic-pool**: Selects subscribers whose IP Addresses were assigned from a dynamic IP address pool.
- **l2tp-lns-assigned**: Selects subscribers whose IP Addresses were assigned by the Layer 2 Tunnelling Protocol Network Server.
- **mip-ha-assigned**: Selects subscribers whose IP Addresses were assigned by the Mobile IP Home Agent.
- **ms-provided-static**: Selects subscribers whose IP Addresses were provided by the Mobile Station.
- **not-ms-provided-static**: Selects subscribers whose IP Addresses were not provided by the Mobile Station.
- **proxy-client**: Selects subscribers whose IP Addresses were assigned by the DHCP Proxy Client
- **relay-agent**: Selects subscribers whose IP Addresses were assigned by the DHCP Relay Agent
- **static-pool**: Selects subscribers whose IP Addresses were assigned from a static IP address pool.

### **ip-pool *name***

Disconnects all subscribers assigned addresses from the IP address pool *pool\_name*. *pool\_name* must be the name of an existing IP pool or IP pool group.

### **ipv4**

Clears all subscribers with IPv4 Firewall enabled/disabled.

### **ipv6**

Clears all subscribers with IPv6 Firewall enabled/disabled.

**ipv6-address *ipv6\_address***

Clears all subscribers connected to the specified IPv6 *ipv6\_address* must be specified in IPv6 colon-separated-hexadecimal notation.

**Note:** This keyword is not supported for use with the MME or SGSN.

**ipv6-prefix *prefix***

Clears subscribers from a specific IPv6 address prefix.

**l3-tunnel-local-addr *ip\_address***

Disconnects all calls for this Layer 3 tunneling interface.

*ip\_address* must be specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**l3-tunnel-remote-addr *ip\_address***

Disconnects all calls for this Layer 3 tunneling peer.

*ip\_address* must be specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**lac *ip\_address***

Disconnects all calls to the peer LAC (L2TP access concentrator).

*ip\_address* must be specified using IPv4 dotted-decimal notation.

**lac-service *service\_name***

Disconnects all calls for this LAC service.

*service\_name* is an alphanumeric string of 1 through 63 characters.

**lma-service *lma\_name***

Disconnects subscribers using this LMA service configured on this system. *lma\_name* must be an existing LMA service expressed as an alphanumeric string of 1 through 63 characters.

**lns *ip\_address***

Disconnects calls to the peer LNS (L2TP network server) specified by *ip\_address* must be specified using IPv4 dotted-decimal notation.

**lns-service *name***

Disconnects calls associated with the LNS service named *name*. *name* is an alphanumeric string of 1 through 63 characters.

**long-duration-time-left [ < | > | greater-than | less-than ] *value***

Disconnects subscriber sessions whose time left for the maximum duration of their session matches the length of time specified.

<: Filters output so that only information less than the specified value is cleared.

>: Filters output so that only information greater than the specified value is cleared.

**greater-than:** Filters output so that only information greater than the specified value is cleared.

**less-than:** Filters output so that only information less than the specified value is cleared.

*value:* If no other filtering options are specified only output matching *value* is cleared. If *value* is not specified all data is cleared. *value* must be an integer from 0 through 4294967295.

#### **mag-service *name***

Disconnects subscribers using this Mobile Access Gateway (MAG) service configured on this system.

*name* must be an existing MAG service and be from 1 to 63 alphanumeric characters.

#### **max-subscribers *max\_count* [ *uniform* ]**

The maximum number of subscribers to be cleared.

*max\_count* must be an integer from 0 through 20000000.

**uniform:** Subscribers will be cleared uniformly.

#### **mip-udp-tunnel-only**

This option clears the subscribers that negotiated MIP-UDP tunneling with the HA.

This option is only valid when MIP NAT Traversal license is enabled.

#### **mipv6ha-service *service\_name***

Disconnects subscribers using this MIPv6 Home Agent service configured on this system.

*service\_name* must be an existing MIPv6 HA service and be from 1 to 63 alphanumeric characters.

#### **mme-address *ipv4\_addr***

Disconnects subscribers using this peer Mobility Management Entity (MME). *ipv4\_addr* must be an existing peer MME IP address entered using IPv4 dotted-decimal notation.

#### **mme-onlytai *mcc mobile\_country\_code mnc mobile\_network\_code tac tracking\_area\_code***

Disconnects all MME subscriber sessions on the system.

- **tai** : Specifies specific tai interface. Must be followed by *mcc*, *mnc* and *tac*.
- **mcc *mobile\_country\_code***: Specifies mobile country code. *mobile\_country\_code* must be a string of size 3 to 3 ranging from 100 through 999.
- **mnc *mobile\_network\_code***: Specifies mobile network code. *mobile\_network\_code* must be a string of size 2 to 3 ranging from 00 through 999.
- **tac *tracking\_area\_code***: Specifies tracking area code. *tracking\_area\_code* must be an integer value between 1 and 65535.

#### **mme-service *name***

Disconnects subscribers using this MME service configured on this system. *name* must be an existing MME service expressed as an alphanumeric string 1 through 63 characters.



**mseg-only**


---

**Important** This keyword is not supported in this release.

---

**mseg-service *mseg\_service\_name***


---

**Important** This keyword is not supported in this release.

---

**msid *id***

Disconnects the mobile user identified by *ms\_id*. *ms\_id* must be from 7 to 16 digits specified as an IMSI, MIN, or RMI. Wildcard characters \$ and \* are allowed. The \* wildcard matches multiple characters and the \$ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes ( ' ). For example; '\$'.

In case of **enforce imsi-min equivalence** is enabled on the chassis and MIN or IMSI numbers supplied, this filter will clear subscribers with a corresponding MSID (MIN or IMSI) whose lower 10 digits matches to lower 10 digits of the supplied MSID.

**clear subscribers msid** *111110123456789* or

**clear subscribers msid** *0123456789*

will clear any subscriber with a MSID that match the lower 10 digits of MSID supplied, i.e. 0123456789.

**msisdn *msisdn***

Clears information for the mobile user identified by Mobile Subscriber ISDN Number (MSISDN). *msisdn* must be from 7 to 16 digits specified as an IMSI, MIN, or RMI.

**nat** { **not-required** | **required** [ **nat-ip** *nat\_ip\_address* | **nat-realm** *nat\_realm\_name* ] }

Clears all subscriber information for the specified subscribers:

**not-required**: Subscribers for whom NAT processing is not required.

**required**: Subscribers for whom NAT processing is required.




---

**Important** The **nat-ip** keyword is only available in StarOS 8.3 and later.

---

**nat-ip** *nat\_ip\_address*: Subscribers for whom NAT processing is enabled and are using the specified NAT IP address. *nat\_ip\_address* specifies the NAT IP address using IPv4 dotted-decimal notation.

**nat-realm** *nat\_realm\_name*: Subscribers for whom NAT processing is enabled and are using the specified NAT realm. *nat\_realm\_name* specifies the NAT realm name expressed as an alphanumeric string of 1 through 63 characters.

**network-requested**

Disconnect subscriber sessions that were initiated by the GGSN network requested create PDP context procedure.

**network-type { gre | ipv4 | ipv6 | ipip | l2tp | mobile-ip | proxy-mobile-ip }**

Disconnects subscriber sessions based on the network type. The following network types can be selected:

- **gre**: Generic Routing Encapsulation (GRE) per RFC 2784
- **ipv4**: Internet Protocol version 4 (IPv4)
- **ipv6**: Internet Protocol version 6 (IPv6)
- **ipip**: IP-in-IP encapsulation per RFC 2003
- **l2tp**: Layer 2 Tunneling Protocol encryption per RFC 2661
- **mobile-ip**: Mobile IP
- **proxy-mobile-ip**: Proxy Mobile IP

**non-volte-call [ auto-delete ][ del-cause { none | reactiv-req } ][ max-subscribers *max\_count* [ uniform ] ][ pace-out-interval *interval\_in\_seconds* ]**

Disconnects PDN connections that do not have an active voice call.

This keyword is available for APN and chassis maintenance for P-GW, S-GW, SAEGW, GGSN, and ePDG.

**auto-delete**: Clears the PDN/call when the last VoLTE dedicated bearer goes down for P-GW, S-GW, SAEGW, GGSN, and ePDG.

Calls will not be cleared when one of the calls in a multiple PDN scenario is a VoLTE PDN. When the VoLTE PDN goes down, all of the other PDNs found for the same IMSI are brought down, which will bring down the call automatically.

**pace-out-interval *interval\_in\_seconds***

The **clear subscribers non-VoLTE auto-delete** command was implemented in StarOS release 17.0. This command can generate a burst of Delete Bearer Requests (DBR) and Delete Session Requests (DSR) in customer setups. To prevent the flooding of peer nodes with session removal control procedures, it is important to distribute these messages in a periodic manner.

The **pace-out-interval** keyword allows operators to specify the time duration for removing the sessions so that control messages sent across to peer nodes are evenly distributed.

Sessions that are "paced-out" over a period of time move into a disconnecting state; however, data and control path activity continue as usual until the system sends out session deletion message(s). In the case of session recovery, "paced-out" sessions are recovered in the connected state and the **clear subscriber** command must be initiated again to clear the recovered sessions.

**pace-out-interval** is the time, in seconds, that session deletion messages are distributed.

*interval\_in\_seconds* must be an integer from 0 to 86400.

**pcf** [ < | > | **less-than** | **greater-than** ] *ipv4\_address* [ [ < | > | **less-than** | **greater-than** ] *ipv4\_address* ]

Displays information for subscribers connected via the packet control function with a specific or range of IP address *ipv4\_address*. The address must be specified using IPv4 dotted-decimal notation.

- <: Filters output so that only information less than the specified IPv4 address value is displayed.
- >: Filters output so that only information greater than the specified IPv4 address value is displayed.
- **less-than**: Filters output so that only information less than the specified IPv4 address value is displayed.
- **greater-than**: Filters output so that only information greater than the specified IPv4 address value is displayed.

Note: It is possible to define a limited range of IP addresses by using the less-than and greater-than options to define minimum and maximum values.

**pcp** { **not-required** | **required** }

Clears all subscriber information for the specified subscribers:

**not-required**: Subscribers for whom PCP processing is not required.

**required**: Subscribers for whom PCP processing is required.

**pdsn-service** *name*

Disconnect all subscribers connected to the packet data service *pdsn\_name*. The packet data service must have been previously configured.

**pdsnclosedrp-service** *service\_name*

Disconnect all subscribers connected to the Closed R-P service *service\_name*. The Closed R-P service must have been previously configured.

**pdg-service** *service\_name*

Disconnects subscriber sessions that are using the PDG service.

*service\_name* must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

**pdif-service** *service\_name*

Clears counters for subscribers accessing the Packet Data Interworking Function (PDIF) service.

*service\_name* must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

**pgw-address** *ip\_address*

Clears specific P-GW interface.

*ip\_address* must be followed by IP address of interface, using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

The following filter keywords are valid with this command:

epdg-address, epdg-service,

**pgw-only** { **all** [ **del-cause** { **none** | **reactiv-req** } ] [ **max-subscribers** *max\_count* ] [ **pace-out-interval** *interval\_in\_seconds* ] | **imsi** *id* **ebi** *id* | **mag-address** *ip\_addr* | **pgw-service** *name* | **sgw-address** *ip\_addr* }

**all**: Disconnects all subscribers for all P-GW services on this system.

**imsi** *id*: Disconnects subscribers based on their International Mobile Subscriber Identification (IMSI). *id* must be the 3-digit MCC (Mobile Country Code), follow by the 2 or 3 digits of the MNC (Mobile Network Code) and the MSIN (Mobile Subscriber Identification Number).

*id* should not exceed 15 digits.

Example: 123-45-678910234 must be entered as 12345678910234

**ebi** *id*: The EBI (EPS Bearer Identity)

*id* must be a valid EBI and be an integer value from 5 to 15.

**mag-service** *ip\_addr*: Disconnects all subscribers using this MAG address.

**pgw-service** *name*: Disconnects all subscribers using this P-GW service.

*name* must be an existing P-GW service expressed as an alphanumeric string of 1 through 63 characters.

**sgw-address** *ip\_addr*: Disconnects all subscribers using this S-GW IP address.

*ip\_addr* must be an existing IP address entered using IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.

**plmn-type** { **home** | **roaming** | **visiting** }

For GGSN, disconnects subscribers whose subscriber type matches the specified type.

**profile-id** *id*

Clears information for subscribers using the granted profile-id for the flow.

*id* must be an integer from 0 to 4294967295.

**profile-name** *name*

Clears information for subscribers using the specified policy profile name.

*name* must be name of an existing profile expressed as an alphanumeric string of 1 through 63 characters.

**qci** *number*

Disconnects subscribers based on their QCI identity.

*number* must be an integer from 0 to 9.

**rulebase** *rulebase\_name*

Clears information for subscribers using the specified rulebase.

*rulebase\_name* must be name of an existing rulebase expressed as an alphanumeric string of 1 through 63 characters.

**rulename rule\_name**

Displays subscribers associated with the specific rule name. The rule\_name options are: predefined, static, and dynamic rules..

**rx-data [ < | > | greater-than | less-than ] value**

Disconnects subscribers who have received the specified number of bytes of data.

<: Filters output so that only information less than the specified value is cleared.

>: Filters output so that only information greater than the specified value is cleared.

**greater-than**: Filters output so that only information greater than the specified value is cleared.

**less-than**: Filters output so that only information less than the specified value is cleared.

*value*: If no other filtering options are specified only output matching *value* is cleared. If *value* is not specified all data is cleared. *value* must be an integer from 0 through 18446744073709551615.

**s1u-state { active | idle | idle-active }**

Disconnects subscribers based on their S1-User Plane Protocol State.

**active**: Selects subscribers having S1-U state set to active.

**idle**: Selects subscribers having S1-U state set to idle.

**idle-active**: Selects subscribers having S1-U state set to idle-active.

**s5-proto { gtp | pmip }**

Disconnects subscribers based on their S5 interface protocol type.

**gtp**: Indicates that the GTP protocol is used on the S5 interface for the subscribers being disconnected.

**pmip**: Indicates that the PMIP protocol is used on the S5 interface for the subscribers being disconnected.

**saegw-only { all [ max-subscribers max\_count ] [ pace-out-interval interval\_in\_seconds ] | co-located | imsi id ebi id | pgw-anchored | saegw-service name | sgw-address ip\_addr | sgw-anchored }**

**all**: Disconnects all subscribers for all SAEGW services on this system.

**co-located**: Disconnects only co-located subscribers which have both S-GW and P-GW functions.

**imsi id**: Disconnects subscribers based on their International Mobile Subscriber Identification (IMSI). *id* must be the 3-digit MCC (Mobile Country Code), follow by the 2 or 3 digits of the MNC (Mobile Network Code) and the MSIN (Mobile Subscriber Identification Number).

*id* should not exceed 15 digits.

Example: 123-45-678910234 must be entered as 12345678910234

**ebi id**: The EBI (EPS Bearer Identity)

*id* must be a valid EBI and be an integer value from 5 to 15.

**pgw-anchored**: Disconnects only PGW-anchored subscribers.

**saegw-service name**: Disconnects all subscribers using this SAEGW service.

*name* must be an existing SAEGW service expressed as an alphanumeric string of 1 through 63 characters.

**sgw-address** *ip\_addr*: Disconnects all subscribers using this S-GW IP address.

*ip\_addr* must be an existing IP address entered using IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.

**sgw-anchored**: Disconnects only SGW-anchored subscribers.

#### **saegw-service** *name*

Disconnects all subscribers using this SAEGW service. *name* must be an existing SAEGW service expressed as an alphanumeric string of 1 through 63 characters.

#### **session-time-left** [ < | > | **greater-than** | **less-than** ] *value*

The amount of time left for the subscriber session.

<: Filters output so that only information less than the specified value is cleared.

>: Filters output so that only information greater than the specified value is cleared.

**greater-than**: Filters output so that only information greater than the specified value is cleared.

**less-than**: Filters output so that only information less than the specified value is cleared.

*value*: If no other filtering options are specified only output matching *value* is cleared. If *value* is not specified all data is cleared. *value* must be an integer from 0 through 4294967295.

#### **sgsn-address** *ip\_address*

Clears all PDP contexts currently being facilitated by a specific SGSN.

*ip\_address* is the IP address of the SGSN entered using IPv4 dotted-decimal notation.

#### **sgsn-only** *lai* *mcc* *mobile\_country\_code* *mnc* *mobile\_network\_code* *lac* *location\_area\_code*

Notes:

- **sgsn-only**: Specifies the clearing of SGSN 3G subscribers only.
- **lai**: Specifies location area identity.
- **mcc** *mobile\_country\_code*: Specifies mobile country code. *mobile\_country\_code* must be a string of size 3 to 3 ranging from 100 through 999.
- **mnc** *mobile\_network\_code*: Specifies mobile network code. *mobile\_network\_code* must be a string of size 2 to 3 ranging from 00 through 999.
- **lac** *location\_area\_code*: Specifies location area code. *location\_area\_code* must be an integer from 1 to 65535.

#### **sgsn-service** *name*

Clears all PDP contexts associated with SGSN. This keyword can be used with filtering keywords that are part of the **clear subscriber** command set.

Using this keyword can trigger a network-initiated service request (paging) procedure.

*name* identifies a specific SGSN-service configuration expressed as an alphanumeric string of 1 through 63 characters.

**sgw-address *ip\_address***

Disconnects subscribers using the Serving Gateway (S-GW) IP address.

*ip\_address* must be specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**sgw-only all [ max-subscribers *max\_count* [ uniform ] ] [ pace-out-interval *interval\_in\_seconds* ] [ verbose ]**

Disconnects all S-GW subscriber sessions on the system.

**sgw-service *name***

Disconnects subscribers using this Serving Gateway (S-GW) service configured on this system. *name* must be an existing S-GW service expressed as an alphanumeric string of 1 through 63 characters.

**smgr-instance *sessmgr\_instance\_number***

Disconnects subscribers on the specified sessmgr instance.

*sessmgr\_instance\_number* must be an integer from 1 to 4294967295.

**tpo { not-required | required }****Important**

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

**tx-data [ < | > | greater-than | less-than ] *value***

Disconnects subscribers who have transmitted the specified number of bytes of data.

<: Filters output so that only information less than the specified value is cleared.

>: Filters output so that only information greater than the specified value is cleared.

**greater-than:** Filters output so that only information greater than the specified value is cleared.

**less-than:** Filters output so that only information less than the specified value is cleared.

*value:* If no other filtering options are specified only output matching *value* is cleared. If *value* is not specified all data is cleared. *value* must be an integer from 0 through 18446744073709551615.

**username *name***

Disconnect the subscriber with the specified username

*name* is the username of the subscriber to be cleared. *name* must be a sequence of characters and/or wildcard characters ('\$ and '\*') from 1 to 127 characters. The \* wildcard matches multiple characters and the \$ wildcard matches a single character. If you do not want the wildcard characters interpreted as wildcard enclose them in single quotes ('). For example; '\$'.

**verbose**

Indicates the output should provide as much information as possible. If this option is not specified then the output is the standard level which is the concise mode.

**without-dynamic-rule**

Displays subscribers without any dynamic rule associated with them.

**without-override-control**

Displays subscribers without any override control rule associated with them.

**wsg-service name**

Disconnects subscribers using this WSG service configured on this ASR 9000 VSM. *name* must be an existing WSG (SecGW) service expressed as an alphanumeric string of 1 through 63 characters.

**grep grep\_options | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Clear subscribers sessions to aid in troubleshooting the system when no additional subscribers may connect or when a specific service or remote address may be having connection problems. This command may also be used to clear connections when preparing for maintenance activities.

Related commands to clear subscription data - *for SGSN use only*

- For a 2G SGSN, the **admin-disconnect-behavior clear-subscription** command in the GPRS Service Configuration mode enables the SGSN to clear subscription data after the administrative disconnect - **clear subscribers all** has been issued.
- For a 3G SGSN, the **admin-disconnect-behavior clear-subscription** command in the SGSN Service Configuration mode enables the SGSN to clear subscription data after the administrative disconnect - **clear subscribers all** has been issued.

**Example**

The following examples illustrate the basic command usage as well as the redirection of the command output. Not all options are exemplified as all options follow the same basic constructs.

The following are basic subscriber clearing examples.

```
clear subscribers username ser1
clear subscribers ha sampleService
clear subscribers ip-pool pool2 verbose
```

The following command disconnects users connected to the foreign agent with IP address *10.2.3.4*.

```
clear subscribers fa 10.2.3.4
```

# clear super-charger

Deletes the subscriber's backed-up subscription data with an SGSN supercharger subscription configuration (3GPP TS.23.116).



---

**Product** SGSN

---

**Privilege** Security Administrator, Administrator, Operator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **clear super-charger { imsi | all }**

**imsi**

Specifies a subscriber's international mobile subscriber identity (IMSI) number. This 15-digit number includes the MCC (mobile country code), the MNC (mobile network code) and the MSIN (mobile station identification number).

**all**

Instructs the SGSN to delete subscription data for all super charger subscribers.

---

**Usage Guidelines**

Use this command to clear (delete) the subscription data records for one or all subscribers within a supercharger subscription configuration.

**Example**

The following command deletes the backed up records for the subscriber identified by the IMSI 90121882144672.

```
clear super-charger imsi 90121882144672
```

## clear supplementary-service statistics

Clears the statistics for Supplementary Service Information.

---

**Product** SGSN

---

**Privilege** Security Administrator, Administrator, Operator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **clear supplementary-service statistics**

---

**Usage Guidelines** Use this command to clear the Supplementary Service Information.

**Example**

The following command clears the Supplementary Service Information:

```
clear supplementary-service statistics
```

# clear tacacs session

Clears TACACS+ sessions.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
clear tacacs session { all | session id session_id [ force ] }
```

**all**

Clears all TACACS+ sessions in idle state.

**session id *session\_id***

Will clear a specified TACACS+ session. *session\_id* must be an integer from 1 to 127.

The command will only be successfully executed if the session is in idle state; otherwise, it will fail.

**force**

Will clear a specified TACACS+ session whether or not the session is in idle state.

**Important**

This keyword should be used with caution.

If a TACACS+ session ends up in not completed login state, you may have to use this option to clear the session.

**Usage Guidelines**

Use this command to clear TACACS+ sessions.

**Example**

The following command clears all TACACS+ sessions in idle state.

```
clear tacacs session all
```

# clear task resources

Deletes the collected resource statistics for system tasks.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator, Operator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
clear task resources { card card_num { facility facility { all | instance id
max } | facility facility { all | instance id max } | max }
```

th e

**card** *card\_num*

Default: all powered on cards.

Specifies a single card for which task information is to be cleared where *card\_num* must be from 1 to 48 for the ASR 5000 and 1 through 20 for the ASR 5500.

**facility** *facility*{ **all** | **instance** *id* **max** }

Default: all facilities.

Specifies the list of facilities for which task information will be cleared. A specific instance of the facility may be cleared as specified by ID or all instances may be cleared. The value of *id* must be an integer from 0 through 10000000. *facility* must be one of:

- **a11mgr**: A11 Interface Manager facility
- **aaamgr**: AAA Manager Facility
- **aaaproxy**: AAA Proxy manager Facility
- **acsctrl**: Active Charging Service (ACS) Controller Facility [Release 11.0 and earlier versions only]
- **acsmgr**: Active Charging Service (ACS) Manager Facility
- **afctrl**: Fabric Manager [ASR 5500 only]
- **afmgr**: Fabric Manager [ASR 5500 only]
- **alcapmgr**: Access Link Control Application Part (ALCAP) Manager
- **asn gw mgr**: ASN Gateway Manager
- **asnpermgr**: ASN Paging/Location-Registry (ASN-PC) Manager
- **bfd**: Bidirectional Forwarding Detection
- **bgp**: Border Gateway Protocol (BGP) Facility

- **bngmgr**: Broadband Network Gateway (BNG) Manager
- **bulkstat**: Bulk Statistics Manager Facility
- **callhome**: Call Home Controller
- **cbsmgr**: Cell Broadcasting Service (CBS) Manager
- **cdfctrl**: Charging Data Function (CDF) Controller
- **cdfmgr**: CDF Manager
- **cdrmod**: Charging Detail Record (CDR) Module
- **cli**: Command Line Interface (CLI) Facility
- **connproxy**: Proxy for connections from same card/chassis
- **cspectrl**: Card Slot Port controller Facility
- **cssctrl**: Content Service Steering Controller
- **dcardctrl**: IPsec Daughter-card Controller Logging Facility
- **dcardmgr**: IPsec Daughter-card Manager Logging Facility
- **dgmbmgr**: Diameter Gmb Application Manager
- **dhmgr**: Distributed Host Manager
- **diamproxy**: Diameter Proxy
- **drvctrl**: Driver Controller Facility
- **egtpegmgr**: EGTP Egress Demux Manager
- **egtpinmgr**: EGTP Ingress Demux Manager
- **evlogd**: Event Log Daemon Facility
- **famgr**: Foreign Agent Manager Facility
- **gtpcmgr**: GTP-C Protocol Logging facility (GGSN product only)
- **gtpumgr**: GTP-U Demux Manager
- **h248prt**: H.248 Protocol Task [Release 11.0 and earlier versions only]
- **hamgr**: Home Agent Manager Facility
- **hatcpu**: High Availability Task CPU Facility
- **hatsystem**: High Availability Task Facility
- **hdctrl**: Hard Disk Controller
- **henbgwdemux**: Home eNodeB Gateway demux manager




---

**hpnt** In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

- **henbgwmgr**: Home eNodeB Gateway Manager




---

**hpnt** In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

- **hnbmgr**: HNBGW HNB Manager




---

**hpnt** In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

- **hwctrl**: Hardware Monitor Controller
- **hwmgr**: Hardware Monitor Manager
- **imsimgr**: SGSN IMSI Manager
- **ipsecctrl**: IP Security Controller Facility
- **ipsecmgr**: IP Security Manager Facility
- **ipsgmgr**: IP Services Gateway Facility
- **kvctrl**: KV Controller
- **kvmgr**: KV Manager
- **l2tpdemux**: L2TP Demultiplexor (LNS) Facility
- **l2tpmgr**: L2TP Manager Facility
- **lagmgr**: Link Aggregation Group (LAG) Manager
- **linkmgr**: SGSN/SS7 Link Manager
- **m3ap**: M3 Application Part Facility
- **m3ua**: M3UA Protocol Facility
- **magmgr**: Mobile Access Gateway (MAG) Manager
- **megadiammgr**: MegaDiameter Manager
- **mme-app**: Mobility Management Entity (MME) Application Facility
- **mme-embms**: MME evolved Multimedia Broadcast Multicast Service Facility

- **mme-misc**: MME miscellaneous logging facility
- **mmedemux**: MME Demux Manager logging facility
- **mmemgr**: MME Manager logging facility
- **mmgr**: SGSN/SS7 Master Manager
- **mpls\_sig**: Multiprotocol Label Switching
- **mpctest**: Migration Performance Test on Packet Accelerator Card
- **netwstrg**: Network Storage Manager [Release 11.0 and earlier versions only]
- **npuctrl**: Network Processor Unit Control Facility
- **npudrv**: Network Processor Unit Driver Facility [ASR 5500 only]
- **npumgr**: Network Processor Unit Manager Facility
- **npusim**: Network Processor Unit Simulator [ASR 5500 only]
- **nputst**: Network Processor Unit Tester
- **nsctrl**: Charging Service Controller [Release 11.0 and earlier versions only]
- **nsmgr**: Charging Service Process Manager [Release 11.0 and earlier versions only]
- **orbns**: Object Request Broker Notification Server Facility
- **orbs**: Object Request Broker System Facility
- **ospf**: Open Shortest Path First Facility
- **ospfv3**: Open Shortest Path First (OSPFv3)
- **pdgmgr**: Packet Data Gateway (PDG) Manager
- **phsgwmgr**: PHS Gateway manager
- **phspcmgr**: PHS Paging Controller manager
- **rct**: Recovery Control Task Facility
- **rdt**: Redirect Task Facility
- **rip**: Routing Information Protocol Facility
- **rmctrl**: Resource Manager Controller Facility
- **rmmgr**: Resource Manager Facility
- **sct**: Shared Configuration Task Facility
- **sessctrl**: Session Controller Facility
- **sessmgr**: Session Manager Facility
- **sesstrc**: Session Trace Collection task
- **sft**: Switch Fabric Monitoring Task
- **sgtpcmgr**: SGSN GTP-C Manager

- **sipcdprt**: SIP Call Distributor Task [Release 11.0 and earlier versions only]
- **sitmain**: System Initialization Task Main Facility
- **sitparent**: Card based system initialization facility that applies to MIO card.
- **snmp**: SNMP Protocol Facility
- **srdb**: Static Rating Database
- **testctrl**: Test Controller
- **testmgr**: Test Manager
- **threshold**: Threshold Server Facility
- **vpnctrl**: Virtual Private Network Controller Facility
- **vpnmgr**: VPN Manager Facility
- **zebos**: ZEBOS™ OSPF Message Facility

**all**: Clears information for all instances of the specified facility.

**instance *id***: Clears information for the facility instance specified as an integer from 0 through 10000000.

#### **max**

Default: current usage levels are cleared.

Clears just the maximum usage levels for tasks as opposed to all current usage levels.

#### **Usage Guidelines**

Use this command to clear (delete) the collected resource statistics for system tasks.

#### **Example**

The following command deletes the Switch Fabric Monitoring Task statistics for instance 100 running on card 2.

```
clear task resources card 2 facility sft instance 100 max
```

## **clear tcap statistics**

Deletes the collected statistics for traffic that has passed through the SS7 TCAP (Transaction Capabilities Application Part) layer.

#### **Product**

SGSN

#### **Privilege**

Security Administrator, Administrator, Operator

#### **Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `clear tcap statistics [ camel-service [ all | name camel_srvc ] | map-service [ all | name map_srvc ] ] [ | { grep grep_options | more } ]`

**camel-service [ all | name *camel\_srvc* ]**

Deletes TCAP statistics for either all CAMEL (Customized Applications for Mobile Network Enhanced Logic, GSM 09.78) services or only for the named CAMEL service.

**map-service [ all | name *mapl\_srvc* ]**

Deletes TCAP statistics for either all MAP services or only for the named MAP service.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines** Use this command to clear (delete) the collected TCAP statistics for MAP or CAMEL services.

#### Example

The following command deletes the collected statistics for a MAP service named *MAP-Tewk*.

```
clear tcap statistics map-service name MAP-Tewk
```

## clear wsg-service statistics

Deletes statistics collected for a Wireless Security Gateway (WSG) service.

**Privilege** Security Administrator, Administrator, Operator

**Product** SecGW (WSG)

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `clear wsg-service statistics [ name svrc_name ]`

**name *svrc\_name***

Specifies the name of a WSG service for which statistics will be deleted.

**Usage Guidelines** Deletes statistics for all WSG services or for a specified WSG service.



**Example**

The following command deletes statistics for all WSG services:

```
clear wsg-service
```

# cli

Specifies command line interface (CLI) session behavior.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
[ no ] cli { history | stop-on-first-error | test-commands [ encrypted ]
password password_string }
```

**no**

Disables the specified keyword functionality.

**history**

Enables command line history for the current command line session. Default: Enabled

**stop-on-first-error**

When enabled and a configuration file is loaded, the system stops loading the configuration file on the first syntax error. Default: Disabled

**test-commands [ encrypted ] password password\_string**

If you are logged in as a Security Administrator or Administrator enabling this command displays diagnostic commands and supplemental keywords to existing commands. The **cli hidden** command in Global Configuration mode must be enabled to grant access to this keyword. Default: Disabled

**Caution**

CLI test-commands are intended for diagnostic use only. Access to these commands is not required during normal system operation. These command are intended for use only by Cisco TAC personnel. Some of these commands can slow system performance, drop subscribers, and/or render the system inoperable

**[ encrypted ] password password\_string**: Password must be entered to access the CLI test-commands. This password must have been previously configured by a Security Administrator via the Global Configuration mode **tech-support test-commands password** command. The password is an alphanumeric string of 1 through 64 characters (plain text password) or 1 through 524 characters (encrypted password).

If the **password** keyword is not entered, the user is prompted (no-echo) to enter the password. If **tech-support test-commands password** has not been enabled, you will be unable to execute **cli test-commands**.



#### Important

An SNMP trap is generated whenever a user enables **cli test-commands (starTestModeEntered)**. Refer to the *SNMP MIB Reference* for additional information.

#### Usage Guidelines

This command controls CLI settings pertaining to the maintenance of a per-session command history and syntax error monitoring during configuration file loading.

By default, the system maintains a list of commands executed during each CLI session. This list is referred to as a history.

In addition, the system can be configured to stop loading a configuration if a syntax error is detected. By default, the system identifies the error but continues to process the configuration file.

#### Example

The following command disables the keeping of a CLI history for the current session:

```
no cli history
```

## clock set

Sets the system time.

#### Product

All

#### Privilege

Security Administrator, Administrator

#### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

#### Syntax Description

```
clock set date_time
```

#### *date\_time*

Specifies the date and time to set the system clock in the format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss. Where:

- YYYY = 4-digit year
- MM = 2-digit month in the range 01 through 12
- DD = 2-digit day in the range 01 through 31
- HH = 2-digit hour in the range 00 through 23
- mm = 2-digit minute in the range 00 through 59

- ss = 2-digit second in the range 00 through 59

### Usage Guidelines

Set the clock to adjust the system clock for such things as timing drift, day-light savings adjustment, etc. New settings are immediately applied to all CPUs in the system.



### Important

This command should only be used if there is no NTP server enabled for any context. If NTP is running on the system, this command returns a failure.

### Example

The following commands set the system clock where one sets the exact second as well.

```
clock set 2011:08:05:02:30
clock set 2011:08:05:02:31:30
```

## cmp enroll current-cert

Triggers a Certification Request (CR) after generating a public and private key pair, as well as an X.509 certificate to be included in the CR for a second certificate from the same Certificate Authority (CA). This is a Certificate Management Protocol v2 command.

### Product

All products supporting IPsec CMPv2 features



### Important

This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

### Privilege

Security Administrator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
cmp enroll current-cert old-cert-name modulus mod_type subject-name
"subject_string" cert-name name ca-root ca_name ca-url url
```

#### **current-cert** *old-cert-name*

Specifies a valid security gateway certificate as an alphanumeric string of 1 through 129 characters.

#### **modulus** *mod\_type*

Specifies the modulus of the generated certificate. *mod\_type* is one of the following integers: 1024, 2048, 4096 or 512.

**subject-name "subject\_string"**

Specifies the subject string of the certificate in double quotation marks. *subject\_string* is an alphanumeric string of 1 through 256 characters.

**cert-name name**

Specifies the name of the newly obtained certificate which also serves as the filename to be stored on /flash disk. *name* is an alphanumeric string of 1 through 129 characters.

**ca-root ca\_name**

Specifies the root certificate of the CA server. *ca\_name* is an alphanumeric string of 1 through 129 characters.

**ca-url url**

Specifies the URL to which the CA server listens. *url* is in the format:  
http://<host>[:<port>][/<directory>]/<filename>.

**Usage Guidelines**

Use this command to trigger a certification request for a second certificate from the same CA.

**Example**

The following command requests a second certificate from the same CA:

```
cmp enroll current-cert aqaw12345 modulus 1024 subject-name
"test_certificate" cert-name cert01 ca-root ca001 ca-url
http://excel:2033/certificates/aqaw12345
```

## cmp fetch cert-name

This command is only applicable for the ASR 9000 running VPC-SI on a Virtualized Services Module (VSM). CMPv2 operations are performed only on one VSM in the chassis. The certificates along with the private key file and the root certificate are stored on the supervisor card. When invoked on other VSMs in the chassis, this command reads the certificate, private key and the root certificate from the supervisor card.

**Product**

All products supporting IPsec CMPv2 features

**Important**

This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
cmp fetch current-cert old-cert-name ca-root ca_name
```

**current-cert *old-cert-name***

Specifies a valid security gateway certificate as an alphanumeric string of 1 through 129 characters.

**ca-root *ca\_name***

Specifies the root certificate of the CA server. *ca\_name* is an alphanumeric string of 1 through 129 characters.

**Usage Guidelines**

Use this command to read the certificate, private key and the root certificate from the supervisor card in an ASR 9000.

**Example**

The following command fetches a certificate from a specified CA:

```
cmp fetch current-cert aqaw12345 ca-root ca001
```

## cmp initialize

Triggers an Initial Certification Request (CR) after generating a public and private key pair, as well as an X.509 certificate to be included in the CR. This is a Certificate Management Protocol v2 command.

**Product**

All products supporting IPsec CMPv2 features

**Important**

This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
cmp initialize modulus mod_type cert-name name subject-name "subject_string"
ca-psk key ca-root ca_name ca-url url
```

**modulus *mod\_type***

Specifies the modulus of the generated certificate. *mod\_type* is one of the following integers: 1024, 2048, 4096 or 512.

**cert-name *name***

Specifies the name of the newly obtained certificate which also serves as the filename to be stored on /flash disk. *name* is an alphanumeric string of 1 through 129 characters.

**subject-name "subject\_string"**

Specifies the subject string of the certificate in double quotation marks. *subject\_string* is an alphanumeric string of 1 through 256 characters.

**ca-psk key**

Specifies the Pre-Shared Key provided by the CA server for CMPv2 operation. *key* is an alphanumeric string of 1 through 129 characters.

**ca-root ca\_name**

Specifies the root certificate of the CA server. *ca\_name* is an alphanumeric string of 1 through 129 characters.

**ca-url url**

Specifies the URL to which the CA server listens. *url* is in the format:  
http://<host>[:<port>][/<directory>]/<filename>.

**Usage Guidelines**

Use this command to trigger an initial certification request from the CA.

**Example**

The following command sends an Initial Certification Request to a specified CA:

```
cmp initialize modulus 1024 cert-name cert001 subject-name "test" ca-psk
AB33569 ca-root cert1 ca-url http://excel:2033/certificates/aqaw12345
```

# cmp poll

Triggers a pollReq for the specified certificate. This is a Certificate Management Protocol v2 command.

**Product**

All products supporting IPsec CMPv2 features

**Important**

This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
cmp poll current-cert old-cert-name
```

**current-cert old-cert-name**

Specifies a valid security gateway certificate as an alphanumeric string of 1 through 129 characters.

**Usage Guidelines**

Use this command to poll the current certificate.

**Example**

The following command polls the current certificate:

```
cmp poll current-cert aqaw12345
```

# cmp update

Triggers a Key Update Request after generating a public and private key pair, as well an X.509 certificate to be included in the Key Update Request for a certificate that is about to expire. This is a Certificate Management Protocol v2 command.

**Product**

All products supporting IPsec CMPv2 features

**Important**

This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
cmp update current-cert old-cert-name modulus mod_type ca-root ca_name ca-url  
url
```

**modulus** *mod\_type*

Specifies the modulus of the generated certificate. *mod\_type* is one of the following integers: 1024, 2048, 4096 or 512.

**current-cert** *old-cert-name*

Specifies a valid security gateway certificate as an alphanumeric string of 1 through 129 characters.

**ca-root** *ca\_name*

Specifies the root certificate of the CA server. *ca\_name* is an alphanumeric string of 1 through 129 characters.

**ca-root** *ca\_name*

Specifies the root certificate of the CA server. *ca\_name* is an alphanumeric string of 1 through 129 characters.

**ca-url url**

Specifies the URL to which the CA server listens. *url* is in the format: `http://<host>[:<port>][/<directory>]/<filename>`.

**Usage Guidelines**

Use this command to initiate a manual update of the current certificate.

**Example**

The following command requests a second certificate from the same CA:

```
cmp update modulus 1024 current-cert aqaw12345 ca-root ca001 ca-url
http://excel:2033/certificates/aqaw12345
```

## commandguard

Enable / disable Commandguard feature to prevent operators from accidentally entering configuration modes by presenting yes/no confirmation prompts.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
commandguard
[ default | no ] commandguard
```

```
[ default | no ]
```

Restores the default behavior for confirmation prompting and disables the Commandguard feature.

**Usage Guidelines**

When **commandguard** is enabled it affects the **configure** and **autoconfirm** CLI commands by causing them to prompt (Y/N) for confirmation. This feature protects operators from accidentally entering configuration mode via CLI or file replay.

**Important**

When **autoconfirm** is enabled, **commandguard** has no affect.

**Example**

The following command enables the Commandguard feature:

```
commandguard
```

The following command restores system default confirmation prompts:



**default commandguard**

The following command instructs the SGSN to ignore Commandguard when enabled:

```
autoconfirm
```

## configure

Moves to the Global Configuration mode to modify the running configuration. May also be used to pre-load a configuration file specified by its URL for modification in the Global Configuration mode.

You can also use this command to update the ConfD Configuration Database (CDB) that supports the NETCONF protocol. Another option locks access to the configuration mode.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
configure [ confd ] [ encrypted ] [ url ] [ lock [ force | warn ] ] [ -noconfirm ]
```

**configure**

Moves from Exec mode to the Global Configuration mode for modifying the configuration.

**confd**

This keyword is always used in conjunction with a URL and is not supported on the ASR 5000. The **configure confd url** command applies the configuration at the URL to the ConfD configuration database (CDB) if no errors exist in the file as specified by the URL. The operator remains in the Exec mode. The CDB supports NETCONF protocol.

**encrypted**

Allows a Lawful Intercept (LI) administrator to execute only encrypted LI contexts from a saved configuration file. This keyword is only visible to an LI Administrator.

**Note**

For additional information on the use of this command, refer to the *Lawful Intercept Configuration Guide*.

**url**

Specifies the location of a configuration file to pre-load for modification. If no URL is specified, modifications are made to the running configuration.

*url* may refer to a local or a remote file. *url* must be entered using one of the following formats:

For the ASR 5000 (not supported with the **confd** keyword):

- [ **file:** ] { /flash | /pcmcia1 | /hd-raid | /sftp } [ /directory ] /file\_name
- **tftp:** // { host [ :port# ] } [ /directory ] /file\_name
- [ **http:** | **ftp:** | **sftp:** ] // [ username [ :password ] @ ] { host } [ :port# ] [ /directory ] /file\_name

For the ASR 5500:

- [ **file:** ] { /flash | /usb1 | /hd-raid / sftp } [ /directory ] /file\_name
- **tftp:** // { host [ :port# ] } [ /directory ] /file\_name
- [ **http:** | **ftp:** | **sftp:** ] // [ username [ :password ] @ ] { host } [ :port# ] [ /directory ] /file\_name



### Important

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

*directory* is the directory name.

*filename* is the actual file of interest.

*username* is the user to be authenticated.

*password* is the password to use for authentication.

*host* is the IP address or host name of the server.

*port#* is the logical port number that the communication protocol is to use.

### **lock [ force | warn ]**

Locks the configuration mode for exclusive access by this administrator. This option prevents multiple administrators from simultaneously modifying the configuration.

The **force** option forces all other administrators to exit to Exec mode, including anyone currently holding the exclusive lock.

The **warn** option warns all other administrators to exit to Exec mode. This administrator will be taking the exclusive lock soon. You may want to use this option before actually forcing administrators out of configuration mode.

### **-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

### Usage Guidelines

If no URL is specified, executing this command causes the CLI to enter the Global Configuration Mode and modify the running configuration.

If a URL is specified, executing this command loads the specified configuration file for modification in Global Configuration mode.

Use the **confd url** option to apply the contents of a configuration script specified by the URL to the CDB. This option does not send you to Global Configuration mode.

The **encrypted** option can only be executed by an administrator with **li-administration** privilege enabled. For additional information see the *Lawful Intercept Configuration Guide*.

By default, configuration (config) mode is shared among all administrative users. You have the option of requesting an exclusive lock of the config mode to assure that no other user is modifying the configuration at the same time. When an administrator holds the exclusive lock, no other administrators are allowed to enter into config mode or load a config file. Any other administrators attempting to enter into config mode or load a config file will see the following message:

```
Failure: User <username> has the exclusive lock
- please enter 'show administrators' for more information
```

If another administrator attempts to enter config mode with the exclusive lock when it is already enabled, the following message appears:

```
Failure: Another administrator is still in configuration mode
- please enter 'show administrators' for more information
```

Administrators who have been forced to exit from config mode will see the following message:

```
Warning: Administrator <username> has forced you to exit from configuration mode
```



### Important

For additional information about config mode locking mechanisms, refer to the *System Administration Guide*.

### Examples

The following command sends you to the Global Configuration mode and allows you to modify the currently running configuration:

```
configure
```

The following command loads a configuration file via FTP from the specified pathname:

```
configure ftp://sampleNode/pub/glob.cfg
```

For the ASR 5000 the following command loads a configuration file from a PCMCIA card:

```
configure /pcmcia1/pub/glob.cfg verbose
```

For the ASR 5500 the following command loads a configuration file from a USB flash drive:

```
configure /usb1/pub/glob.cfg verbose
```

For NETCONF-ConfD, the following command copies the script from the flash drive pathname to the CDB:

```
configure confd /flash/confd/cdb.cfg
```

The following command warns other administrators that you are seeking an exclusive lock on the config mode:

```
configure lock warn
```

## context

Sets the current context to the context specified.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<b>context</b> <i>name</i>  <b>name</b> Specifies the context of interest as an alphanumeric string of 1 through 79 characters. Must be a previously defined context.
<b>Usage Guidelines</b>	Change the current context when it is desired to configure and/or manage a specific context.

**Example**

The following sets the current context to the *sampleContext* context.

```
context sampleContext
```

## copy

Copies files from one location to another. Allows files to be copied to/from locally, as well as from one remote location to another.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<b>copy</b> <i>from_url to_url</i> [ <b>passive</b> ] [ <b>-noconfirm</b> ]  <b>from_url</b> Specifies the source of the copy. <i>url</i> may refer to a local or a remote file. <i>url</i> must be entered using the following format: For the ASR 5000: <ul style="list-style-type: none"> <li>• [ <b>file:</b> ] { <b>/flash</b>   <b>/pcmcia1</b>   <b>/hd-raid</b> } [ <i>/directory</i> ] <i>/file_name</i></li> <li>• <b>tftp:</b> // { <i>host</i> [ <i>:port#</i> ] } [ <i>/directory</i> ] <i>/file_name</i></li> <li>• [ <b>http:</b>   <b>ftp:</b>   <b>sftp:</b> ] // [ <i>username</i> [ <i>:password</i> ] @ ] { <i>host</i> } [ <i>:port#</i> ] [ <i>/directory</i> ] <i>/file_name</i></li> </ul>

For the ASR 5500:

- [ **file:** ] { /flash | /usb1 | /hd-raid } [ /directory ] /file\_name
- **tftp://** { host [ :port# ] } [ /directory ] /file\_name
- [ **http:** | **ftp:** | **sftp:** ] // [ username [ :password ] @ ] { host } [ :port# ] [ /directory ] /file\_name

For VPC:

- [ **file:** ] { /flash | /hd-raid | /usb1 | /usb2 | /cdrom1 } [ /directory ] /file\_name




---

**Important** The USB ports and CD-ROM must be configured via the hypervisor to be accessible.

---

- **tftp://** { host [ :port# ] } [ /directory ] /file\_name
- [ **http:** | **ftp:** | **sftp:** ] // [ username [ :password ] @ ] { host } [ :port# ] [ /directory ] /file\_name




---

**Important** Use of the ASR 5000 SMC hard drive is not supported in this release.

---




---

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

---

*directory* is the directory name.

*filename* is the actual file of interest.

*username* is the user to be authenticated.

*password* is the password to use for authentication.

*host* is the IP address or host name of the server.

*port#* is the logical port number that the communication protocol is to use.

#### **to\_url**

Specifies the destination of the copy. *url* may refer to a local or a remote file. *url* must be entered using the following format:

For the ASR 5000:

- [ **file:** ] { /flash | /pcmcia1 | /hd-raid } [ /directory ] /file\_name
- **tftp://** { host [ :port# ] } [ /directory ] /file\_name
- [ **ftp:** | **sftp:** ] // [ username [ :password ] @ ] { host } [ :port# ] [ /directory ] /file\_name

For the ASR 5500:

- [ **file:** ] { /flash | /usb1 | /hd-raid } [ /directory ] /file\_name

- **tftp://**{ *host* [ *:port#* ] } [ */directory* ] */file\_name*
- [ **ftp** | **sftp** ] **://** [ *username* [ *:password* ] @ ] { *host* } [ *:port#* ] [ */directory* ] */file\_name*

For VPC:

- [ **file:** ] { **/flash** | **/hd-raid** | **/usb1** | **/usb2** | **/cdrom1** } [ */directory* ] */file\_name*




---

**Important** The USB ports and CD-ROM must be configured via the hypervisor to be accessible.

---

- **tftp://**{ *host* [ *:port#* ] } [ */directory* ] */file\_name*
- [ **http** | **ftp** | **sftp** ] **://** [ *username* [ *:password* ] @ ] { *host* } [ *:port#* ] [ */directory* ] */file\_name*




---

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

---

*directory* is the directory name.

*filename* is the actual file of interest.

*username* is the user to be authenticated.

*password* is the password to use for authentication.

*host* is the IP address or host name of the server.

*port#* is the logical port number that the communication protocol is to use.

#### **passive**

Indicates the file copy is to use the passive mode FTP.

#### **-noconfirm**

Executes the command without any additional prompt and confirmation from the user.




---

**Important** Use of the **-noconfirm** option allows the overwriting of an existing file if the destination file already exists.

---

### **Usage Guidelines**

Copy configuration files, log files, etc., to provide backups of data through the network.

#### **Example**

For the ASR 5000, the following copies files from the local */flash/pub* directory to remote node *remoteABC*'s */pcmcia2/pub* directory with and without confirmation respectively.

```
copy http://remoteABC/pub/june.cfg /flash/pub/june.cfg
copy tftp://remoteABC/pub/june.cfg /pcmcia2/pub/june.cfg -noconfirm
```

For the ASR 5500, the following copies files from the local */flash/pub* directory to remote node *remoteABC*'s */flash/pub* directory with and without confirmation respectively.

```
copy http://remoteABC/pub/june.cfg /flash/pub/june.cfg
copy tftp://remoteABC/pub/june.cfg /flash/pub/june.cfg -noconfirm
```

The following copies files from remote node *remoteABC* to remote node *remote123*.

```
copy ftp://remoteABC/pub/may.cfg ftp://remote123/pub/may.cfg
```

## crash copy

Copies individual crash files (one-at-a-time) and optionally the core dump file from the stored crash records on the chassis to a user-specified location.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<b>crash copy number</b> <i>number</i> <b>url</b> <i>to_url</i> [ <b>core</b> ]

### **number** *number*

Specifies the identification number of the crash record as an integer representing a valid record number from 1 through 120. To determine the numeric identity of a specific crash file, use the **show crash list** command in Exec mode.

### **url** *to\_url*

Specifies the destination of the copy. *url* may refer to a local or a remote file and must be entered using the following format:

For the ST16:

- [ **file:** ] { **/flash** | **/pcmcia1** | **/pcmcia2** } [ */directory* ] /
- **tftp://** { *host* [ *:port#* ] } [ */directory* ] /
- [ **ftp:** | **sftp:** ]/[ *username* [ *:password* ] @ ] { *host* } [ *:port#* ] [ */directory* ] /

For the ASR 5000:

- [ **file:** ] { **/flash** | **/pcmcia1** | **/hd** } [ */directory* ] /
- **tftp://**{ *host*[ *:port#* ] } [ */directory* ] /
- [ **ftp:** | **sftp:** ]/[ *username* [ *:password* ] @ ] { *host* } [ *:port#* ] [ */directory* ] /

For the ASR 5500:

- [ **file:** ] { /flash | /usb1 | /hd } [ /directory ] /
- **tftp:**//{ host[ :port# ] } [ /directory ] /
- [ **ftp:** | **sftp:** ]//[ username [ :password ] @ ] { host } [ :port# ] [ /directory ] /

For VPC:

- [ **file:** ] { /flash | /hd-raid | /usb1 | /usb2 | /cdrom1 } [ /directory ] /file\_name




---

**Important** The USB ports and CD-ROM must be configured via the hypervisor to be accessible.

---

- **tftp:**//{ host[ :port# ] } [ /directory ] /file\_name
- [ **http:** | **ftp:** | **sftp:** ]//[ username [ :password ] @ ] { host } [ :port# ] [ /directory ] /file\_name




---

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

---

*directory:* the name of the target directory.

*username:* the username to be authenticated to provide access to targeted server.

*password:* the username's password to be authenticated.

*host:* the IP address or host name of the targeted server.

*port#:* the number of the target server's logical port used for the selected communication protocol.




---

**Important** Do **not** specify a target filename as this will prevent the file from writing to the target server. The system generates and provides a timestamp-based filename that appears at the destination when the **copy** command completes.

---

### **core**

Copies the core dump to the targeted storage server. The core cannot be copied alone; it must be part of a **crash copy** action included when copying a crash file.

---

### **Usage Guidelines**

Copy crash files of core dump to another location for backup or analysis.

### **Example**

The following uses FTP to copy stored record number 5 and the core dump from the crash record list to a targeted remote node directory called *crasharchive* through port 22 of the targeted server *remoteABC* with access through user *homeboy* whose password is *secret.7.word*.

```
crash copy number 5 url ftp://homeboy:secret.7.word@
remoteABC:22/crasharchive/ core
```



# crypto blockedlistfile update

Updates the blacklist / blockedlist (access denied) file using the path specified when the / blockedlist was enabled.

---

**Product**

All products supporting IPsec crypto blockedlisting



---

**Important**

This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

---

**Privilege**

Security Administrator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

In releases prior to StarOS 21.26:

```
crypto blacklist file update
```

From StarOS 21.26 and later releases:

```
crypto blockedlist file update
```

---

**Usage Guidelines**

Update the / blockedlist file. For additional information on blockedlisting, refer to the *System Administration Guide*.

**Example**

In releases prior to StarOS 21.26:

The following command updates the / blockedlist file:

```
crypto blacklist file update
```

From StarOS 21.26 and later releases:

The following command updates the / blockedlist file:

```
crypto blockedlist file update
```

# crypto rsa-keygen modulus

Generates an RSA key pair and Certificate Signing Request (CSR) using information to authenticate the site.

---

**Product**

All products that support IPsec

**Important**

This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
crypto rsa-keygen modulus { 1024 | 2048 | 4096 | 512 }
```

**Usage Guidelines**

Generate an RSA key pair and Certificate Signing Request (CSR) using information to authenticate the site. You can specify the modulus (key size of the generated certificate) as 512, 1024, 2048 or 4096 bits.

A CSR is a message sent to a Certification Authority (CA) to request a public key certificate for an entity, where the entity is the subject of the certificate. The software creating the CSR must first generate an RSA key pair; the key pair comprises a public and private key. The public key is bundled with the subject's name, and other information to form the CSR.

**Example**

The following command generates a CSR for a certificate with a modulus of 2048 bits:

```
crypto rsa-keygen modulus 2048
```

## crypto permitlistfile update

Updates the permitlist(access granted) file using the path specified when the permitlist was enabled.

**Product**

All products supporting IPSec crypto permitlisting

**Important**

This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

In releases prior to StarOS 21.26:

```
crypto whitelist file update
```

From StarOS 21.26 and later releases:

**crypto permitlist file update****Usage Guidelines**

Update the permitlist file. For additional information on permitlisting, refer to the *System Administration Guide*.

**Example**

In releases prior to StarOS 21.26:

The following command updates the whitelist file:

```
crypto whitelist file update
```

From StarOS 21.26 and later releases:

The following command updates the whitelist file:

```
crypto permitlist file update
```

## crypto-group

Allows the manual switchover of redundant IPSec tunnels belonging to a specific crypto group.

**Product**

PDSN

GGSN

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
crypto-group name group_name activate { primary | secondary }
```

**name** *group\_name*

Specifies the name of an existing crypto group with which the tunnels to be switched are associated.

**activate { primary | secondary }**

Allows you to specify which tunnel to activate:

- **primary**: Switches traffic to the primary tunnel in the group.
- **secondary**: Switches traffic to the secondary tunnel in the group.

**Usage Guidelines**

This command is used in conjunction with the Redundant IPSec Tunnel Fail-over feature.

Use this command to manually switch traffic to a specific tunnel in a crypto group if the automatic switchover options have been disabled. Refer to the **switchover** command in the Crypto Group configuration mode for more information.

**Example**

The following command manually switches user traffic to the secondary tunnel in the crypto group called *group1*:

```
crypto-group group1 activate secondary
```



# CHAPTER 17

## Exec Mode Commands (D-S)

The Exec Mode is the initial entry point into the command line interface system. Exec mode commands are useful in troubleshooting and basic system monitoring.

### Command Modes

This chapter contains the commands in the Exec Mode from **debug** to **system**.

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```



### Important

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

- [debug bfd, on page 378](#)
- [debug ip, on page 379](#)
- [debug ip bgp, on page 380](#)
- [debug ip ospf all, on page 381](#)
- [debug ip ospf event, on page 382](#)
- [debug ip ospf ism, on page 383](#)
- [debug ip ospf lsa, on page 384](#)
- [debug ip ospf nsm, on page 385](#)
- [debug ip ospf packet, on page 386](#)
- [debug ip ospf route, on page 387](#)
- [debug ip ospf router, on page 388](#)
- [debug ipv6 ospf all, on page 389](#)
- [debug ipv6 ospf event, on page 390](#)
- [debug ipv6 ospf ifsm, on page 391](#)
- [debug ipv6 ospf lsa, on page 392](#)
- [debug ipv6 ospf nsm, on page 393](#)
- [debug ipv6 ospf packet, on page 394](#)
- [debug ipv6 ospf route, on page 395](#)
- [default terminal, on page 396](#)
- [delete, on page 397](#)
- [delete support record, on page 398](#)

- `dhcp force`, on page 399
- `dhcp test`, on page 400
- `diameter disable endpoint`, on page 401
- `diameter enable endpoint`, on page 401
- `diameter-proxy conn-audit`, on page 402
- `diameter reset connection`, on page 403
- `diameter reset route failure`, on page 404
- `directory`, on page 405
- `disable radius`, on page 406
- `dns-client`, on page 407
- `egtpc test echo`, on page 408
- `enable radius`, on page 410
- `exit`, on page 411
- `filesystem`, on page 411
- `filesystem synchronize`, on page 412
- `gtpc test echo`, on page 414
- `gtpm interim now`, on page 415
- `gtpm interim now active-charging egcdr`, on page 417
- `gtpm storage-server commit`, on page 419
- `gtpm storage-server streaming start`, on page 419
- `gtpm test`, on page 420
- `gtpu test echo`, on page 422
- `gtpv0 test echo`, on page 424
- `hd raid`, on page 425
- `host`, on page 430
- `install plugin`, on page 430
- `interface`, on page 431
- `lawful-intercept`, on page 431
- `lawful-intercept packet-cable`, on page 432
- `lawful-intercept ssdf`, on page 432
- `license`, on page 432
- `link-aggregation port switch to`, on page 433
- `logging active`, on page 434
- `logging filter`, on page 435
- `logging trace`, on page 446
- `logging session fp-flow-state-change`, on page 448
- `logs checkpoint`, on page 449
- `lsp-ping`, on page 450
- `lsp-traceroute`, on page 451
- `mkdir`, on page 452
- `mme-mmedemux`, on page 453
- `mme disconnect`, on page 454
- `mme imsimgr`, on page 455
- `mme offload`, on page 456
- `mme paging cache clear`, on page 458
- `mme relocate-ue imsi`, on page 458

- mme reset, on page 459
- monitor interface, on page 460
- monitor protocol, on page 461
- monitor subscriber, on page 465
- newcall policy, on page 469
- password change, on page 475
- patch plugin, on page 476
- ping, on page 478
- ping6, on page 480
- port disable, port enable, on page 481
- port switch to, on page 482
- ppp echo-test, on page 483
- push ssh-key, on page 484
- radius interim accounting now, on page 485
- radius test, on page 486
- reload, on page 488
- rename, on page 489
- reset active-charging, on page 490
- reset alcap-service, on page 491
- reset diameter, on page 492
- reset ims-authorization, on page 492
- reveal disabled commands, on page 493
- rlogin, on page 494
- rmdir, on page 495
- rollback module, on page 496
- rotate-hd-file, on page 496
- save configuration, on page 497
- save logs, on page 500
- session trace, on page 513
- session trace random, on page 517
- session trace signaling, on page 519
- setup, on page 520
- sgs offload, on page 521
- sgs vlr-failure, on page 523
- sgs vlr-recover, on page 524
- sgsn clear-congestion, on page 526
- sgsn clear-detached-subscriptions, on page 526
- sgsn imsimgr, on page 527
- sgsn offload, on page 528
- sgsn op, on page 531
- sgsn retry-unavailable-ggsn, on page 535
- sgsn trigger-congestion, on page 535
- sgtpc test echo sgsn-address, on page 536
- shutdown, on page 537
- sleep, on page 538
- srp disable, on page 539

- [srp enable](#), on page 539
- [srp initiate-audit](#), on page 540
- [srp initiate-switchover](#), on page 541
- [srp reset-auth-probe-fail](#), on page 542
- [srp reset-diameter-fail](#), on page 542
- [srp reset-sx-fail](#), on page 543
- [srp terminate-post-process](#), on page 543
- [srp validate-configuration](#), on page 544
- [srp validate-switchover](#), on page 544
- [ssh](#), on page 545
- [start crypto security-association](#), on page 545
- [statistics-collection](#), on page 546
- [system packet-dump](#), on page 547
- [system ping](#), on page 548
- [system ssh](#), on page 549

## debug bfd

Enables or disables the debug options for Bidirectional Forwarding Detection (BFD) debugging. If logging is enabled, results are sent to the logging system.

**Product** All

**Privilege** Security Administrator, Administrator, Operator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `[ no ] debug bfd { all | events ipc-error | ipc-events | nsm | packet | session }`

**no**

Indicates the IP debugging is to be disabled for the IP interfaces/function specified.

**bfd | interface *name* | route**

Specifies which IP interfaces/function to debug.

**all**: enables debug for all BFD items.

**events**: enables debug for BFD events.

**ipc-error**: enables debug for BFD Inter-process communication (IPC) errors.

**ipc-events**: enables debug for BFD Inter-process communication (IPC) events.

**nsm**: enables debug for BFD Network Service Manager messages.

**packet**: enables debug for BFD packets.



**session:** enables debug for BFD sessions.

---

### Usage Guidelines

The `debug bfd` command is valuable when troubleshooting network problems with BFD-enabled BGP routers. The debugging is stopped by using the **no** keyword.




---

### Caution

Issuing this command could negatively impact system performance depending on system configuration and/or loading.

---

### Example

The following commands enable/disable debugging for BFD.

```
debug bfd
```

```
no debug bfd
```

# debug ip

Enables or disables the debug options for IP debugging. If logging is enabled, results are sent to the logging system.

---

### Product

All

---

### Privilege

Security Administrator, Administrator, Operator

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

```
[ no ] debug ip { arp | interface | route }
```

**no**

Indicates the IP debugging is to be disabled for the IP interfaces/function specified.

**arp | interface *name* | route**

Specifies which IP interfaces/function to debug.

**arp:** indicates debug is to be enabled for the address resolution protocol.

**interface:** indicates debug is to be enabled for the IP interfaces.

**route:** indicates debug is to be enabled for the route selection and updates.

---

### Usage Guidelines

The debug IP command is valuable when troubleshooting network problems between nodes. The debugging is stopped by using the **no** keyword.

**Caution**

Issuing this command could negatively impact system performance depending on system configuration and/or loading.

**Example**

The following commands enable/disable debugging for ARP.

```
debug ip arp
no debug ip arp
```

The following enables/disables debugging for IP interfaces.

```
debug ip interface
no debug ip interface
```

The following enables/disables debugging for routing.

```
debug ip route
no debug ip route
```

## debug ip bgp

Enables or disables BGP (Border Gateway Protocol) debug flags. If logging is enabled, results are sent to the logging system.

**Product**

HA

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
[ no ] debug ip bgp { all | event | filters | fsm | keepalives | updates
  { inbound | outbound } }
```

**no**

Disables the specified BGP debug flags.

**all**

Enables all BGP debug flags.

**event**

Enables debugging of all BGP protocol events.

**filters**

Enables debugging of all BGP filters.

**fsm**

Enables debugging of BGP Finite State Machine

**keepalives**

Enables debugging of all BGP keepalives.

**updates {inbound | outbound}**

Enables debugging of BGP updates.

**inbound:** Debug all BGP inbound updates.

**outbound:** Debug all BGP outbound updates.

**Usage Guidelines**

Use this command to enable or disable BGP debug flags.

**Example**

The following command disables all BGP debug flags enabled by any of the **debug ip bgp** commands:

```
no debug ip bgp all
```

The following command enables all BGP debug flags:

```
debug ip bgp all
```

## debug ip ospf all

Enables or disables all OSPF (Open Shortest Path First) debug flags. If logging is enabled, results are sent to the logging system.

**Product**

PDSN

HA

GGSN

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
[ no ] debug ip ospf all
```

**no**

Disable all OSPF debug flags.

**Usage Guidelines**

Use this command to enable or disable all OSPF debug flags.

**Example**

The following command disables all OPSF debug flags enabled by any of the **debug ip ospf** commands:

```
no debug ip ospf all
```

The following command enables all OSPF debug flags:

```
debug ip ospf all
```

## debug ip ospf event

Enables or disables debugging of OSPF protocol events. If logging is enabled, results are sent to the logging system. If no keywords are specified, all events are enabled for debugging.

**Product**

PDSN  
HA  
GGSN

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
[ no ] debug ip ospf event [ abr | asbr | vl | lsa | os | router ]
```

**no**

Disables debugging the specified OSPF event. If no keywords are specified, all events are disabled.

**abr**

Enables debugging of Area Border Router (ABR) events.

**asbr**

Enables debugging of Autonomous System Boundary Router (ASBR) events.

**vl**

Enables debugging of Virtual Link (VL) events.

**lsa**

Enables debugging of link state advertisement (LSA) events.

**os**

Enables debugging of operating system (OS) events.

**router**

Enables debugging of router events.

**Usage Guidelines**

Use this command to output debug information for OSPF events.

**Example**

To enable all event debug information, enter the following command;

```
debug ip ospf event
```

To disable all event debug information, enter the following command;

```
no debug ip ospf event
```

## debug ip ospf ism

Enables or disables OSPF Interface State Machine (ISM) troubleshooting, based on ISM information type. If no keywords are specified all ISM information types are enabled. If logging is enabled, results are sent to the logging system.

**Product**

PDSN  
HA  
GGSN

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
[ no ] debug ip ospf ism [ events | status | timers ]
```

**no**

Disables debugging the specified ISM information. If no keywords are specified, all information is disabled.

**events**

Enables debugging ISM event information.

**status**

Enables debugging ISM status information.

**timers**

Enables debugging ISM timer information.

**Usage Guidelines**

Use this command to output ISM debug information.

**Example**

To enable all ISM debug information, enter the following command;

```
debug ip ospf ism
```

To disable all ISM debug information, enter the following command;

```
no debug ip ospf ism
```

## debug ip ospf lsa

Enables or disables troubleshooting on OSPF Link State Advertisements (LSAs), based on the specific LSA option. If no keywords are specified, all options are enabled. If logging is enabled, results are sent to the logging system.

**Product**

PDSN  
HA  
GGSN

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
[ no ] debug ip ospf lsa [ flooding | generate | install | refresh |  
maxage | refresh ]
```

**no**

Disables the specified LSA debug information. If no keyword is specified, all LSA debug information is disabled.

**flooding**

Enables LSA flooding information.

**generate**

Enables LSA generation information.

**install**

Enables LSA install information.

**maxage**

Enables LSA maximum age information in seconds. The maximum age is 3600 seconds.

**refresh**

Enables LSA refresh information.

**Usage Guidelines**

Use this command to output debug information for LSAs.

**Example**

To enable all LSA debug information, enter the following command;

```
debug ip ospf lsa
```

To disable all LSA debug information, enter the following command;

```
no debug ip ospf lsa
```

## debug ip ospf nsm

Enables or disables troubleshooting OSPF Neighbor State Machines (NSMs), based on the specific NSM information type. If no keyword is specified, all NSM information types are enabled. If logging is enabled, results are sent to the logging system.

**Product**

PDSN  
HA  
GGSN

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
[ no ] debug ip ospf nsm [ status | events | timers ]
```

**no**

Disables the debugging the specified NSM information type. If no keyword is specified, all information types are disabled.

**events**

Enables debugging NSM event information.

**status**

Enables debugging NSM status information.

**timers**

Enables debugging NSM timer information.

**Usage Guidelines**

Use this command to output debug information for OSPF NSMs

**Example**

To enable all NSM debug information, enter the following command;

```
debug ip ospf nsm
```

To disable all NSM debug information, enter the following command;

```
no debug ip ospf nsm
```

## debug ip ospf packet

Enables or disables troubleshooting of specific OSPF packet information. If logging is enabled, results are sent to the logging system.

**Product**

PDSN

HA

GGSN

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
[ no ] debug ip ospf packet { all | dd | hello | ls-ack | ls-request |
ls-update } [ send | rcv ] [ detail ]
```

**no**

Disable debugging of the specified packet information.

**all**

Enables debugging all OSPF packet information.



**dd**

Enables debugging database descriptions.

**hello**

Enables debugging hello packets.

**ls-ack**

Enables debugging link state acknowledgements.

**ls-request**

Enables debugging link state requests.

**ls-update**

Enables debugging link state updates.

**send**

Enables debugging only on sent packets.

**recv**

Enables debugging only on received packets.

**detail**

Enables detailed information in the debug output.

---

**Usage Guidelines**

Use this command to output specific OSPF packet information.

**Example**

To enable all packet debug information, enter the following command;

```
debug ip ospf packet all
```

To disable all route debug information, enter the following command;

```
no debug ip ospf packet all
```

## debug ip ospf route

Sets the route calculation method to use in debugging OSPF routes. If no route calculation method is specified, all methods are enabled. If logging is enabled, results are sent to the logging system.

---

**Product**

PDSN

HA

GGSN

---

**Privilege** Security Administrator, Administrator, Operator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `[ no ] debug ip ospf route [ ase | ia | install | spf ]`

**no**

Disables debugging of route information. If no keyword is specified all information types are disabled.

**ase**

Enables debugging information on autonomous system external (ASE) route calculations.

**ia**

Enables debugging information on Inter-Area route calculations.

**install**

Enables debugging information on route installation.

**spf**

Enables debugging information on Shortest Path First (SPF) route calculations.

---

**Usage Guidelines** Use this command to output debug information for OSPF routes.

**Example**

To enable all route debug information, enter the following command;

```
debug ip ospf route
```

To disable all route debug information, enter the following command;

```
no debug ip ospf route
```

## debug ip ospf router

Sets the debug option for OSPF router information. If no keyword is specified, all router information is enabled. If logging is enabled, results are sent to the logging system.

---

**Product** PDSN

HA

GGSN

---

**Privilege** Security Administrator, Administrator, Operator

<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<code>[ no ] debug ip ospf router [ interface   redistribute ]</code>  <b>no</b> Disables the specified router debug information. If no keyword is specified, all router information is disabled.  <b>interface</b> Enables router interface information.  <b>redistribute</b> Enables router redistribute information.
<b>Usage Guidelines</b>	Use this command to output debug information for the OSPF router.  <b>Example</b> To enable all router debug information, enter the following command; <b>debug ip ospf router</b> To disable all router debug information, enter the following command; <b>no debug ip ospf router</b>

## debug ipv6 ospf all

Enables or disables all OSPFv3 (Open Shortest Path First Version 3) debug flags. If logging is enabled, results are sent to the logging system.

<b>Product</b>	PDSN HA GGSN
<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<code>[ no ] debug ipv6 ospf all</code>

**no**

Disable all OSPFv3 debug flags.

**Usage Guidelines**

Use this command to enable or disable all OSPFv3 debug flags.

**Example**

The following command disables all OPSFv3 debug flags enabled by any of the **debug ip ospf** commands:

```
no debug ipv6 ospf all
```

The following command enables all OSPFv3 debug flags:

```
debug ipv6 ospf all
```

## debug ipv6 ospf event

Enables or disables debugging of OSPFv3 protocol events. If logging is enabled, results are sent to the logging system. If no keywords are specified, all events are enabled for debugging.

**Product**

PDSN  
HA  
GGSN

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
[ no ] debug ipv6 ospf event [ abr | asbr | os | router ]
```

**no**

Disables debugging the specified OSPFv3 event. If no keywords are specified, all events are disabled.

**abr**

Enables debugging of Area Border Router (ABR) events.

**asbr**

Enables debugging of Autonomous System BOUNDary Router (ASBR) events.

**os**

Enables debugging of operating system (OS) events.

**router**

Enables debugging of router events.

**Usage Guidelines**

Use this command to output debug information for OSPFv3 events.

**Example**

To enable all event debug information, enter the following command;

```
debug ipv6 ospf event
```

To disable all event debug information, enter the following command;

```
no debug ipv6 ospf event
```

## debug ipv6 ospf ifsm

Enables or disables OSPFv3 Interface State Machine (ISM) troubleshooting, based on ISM information type. If no keywords are specified all ISM information types are enabled. If logging is enabled, results are sent to the logging system.

**Product**

PDSN

HA

GGSN

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
[ no ] debug ipv6 ospf ism [ events | status | timers ]
```

**no**

Disables debugging the specified ISM information. If no keywords are specified, all information is disabled.

**events**

Enables debugging ISM event information.

**status**

Enables debugging ISM status information.

**timers**

Enables debugging ISM timer information.

**Usage Guidelines** Use this command to output ISM debug information.

### Example

To enable all ISM debug information, enter the following command;

```
debug ipv6 ospf ism
```

To disable all ISM debug information, enter the following command;

```
no debug ipv6 ospf ism
```

## debug ipv6 ospf lsa

Enables or disables troubleshooting on OSPFv3 Link State Advertisements (LSAs), based on the specific LSA option. If no keywords are specified, all options are enabled. If logging is enabled, results are sent to the logging system.

**Product** PDSN  
HA  
GGSN

**Privilege** Security Administrator, Administrator, Operator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** [ no ] debug ip ospf lsa [ flooding | generate | install | maxage | refresh ]

### no

Disables the specified LSA debug information. If no keyword is specified, all LSA debug information is disabled.

### flooding

Enables LSA flooding information.

### generate

Enables LSA generation information.

### install

Enables LSA install information.

**maxage**

Enables LSA maximum age information in seconds. The maximum age is 3600 seconds.

**refresh**

Enables LSA refresh information.

**Usage Guidelines**

Use this command to output debug information for LSAs.

**Example**

To enable all LSA debug information, enter the following command;

```
debug ipv6 ospf lsa
```

To disable all LSA debug information, enter the following command;

```
no debug ipv6 ospf lsa
```

## debug ipv6 ospf nsm

Enables or disables troubleshooting OSPFv3 Neighbor State Machines (NSMs), based on the specific NSM information type. If no keyword is specified, all NSM information types are enabled. If logging is enabled, results are sent to the logging system.

**Product**

PDSN

HA

GGSN

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
[ no ] debug ipv6 ospf nsm [ interface | redistribute ]
```

**no**

Disables the debugging the specified NSM information type. If no keyword is specified, all information types are disabled.

**interface**

Enables debugging NSM on this interface.

**redistribute**

Enables debugging NSM redistribution information.

**Usage Guidelines** Use this command to output debug information for OSPFv3 NSMs

### Example

To enable all NSM debug information, enter the following command;

```
debug ipv6 ospf nsm
```

To disable all NSM debug information, enter the following command;

```
no debug ipv6 ospf nsm
```

## debug ipv6 ospf packet

Enables or disables troubleshooting of specific OSPFv3 packet information. If logging is enabled, results are sent to the logging system.

**Product** PDSN  
HA  
GGSN

**Privilege** Security Administrator, Administrator, Operator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** [ no ] debug ipv6 ospf packet { dd | hello | ls-ack | ls-request | ls-update } [ recv | send ] [ detail ]

### no

Disable debugging of the specified packet information.

### dd

Enables debugging database descriptions.

### hello

Enables debugging hello packets.

### ls-ack

Enables debugging link state acknowledgements.

### ls-request

Enables debugging link state requests.



**ls-update**

Enables debugging link state updates.

**recv**

Enables debugging only on received packets.

**send**

Enables debugging only on sent packets.

**detail**

Enables detailed information in the debug output.

**Usage Guidelines**

Use this command to output specific OSPFv3 packet information.

**Example**

To enable all packet debug information, enter the following command;

```
debug ipv6 ospf packet all
```

To disable all route debug information, enter the following command;

```
no debug ipv6 ospf packet all
```

## debug ipv6 ospf route

Sets the route calculation method to use in debugging OSPFv3 routes. If no route calculation method is specified, all methods are enabled. If logging is enabled, results are sent to the logging system.

**Product**

PDSN  
HA  
GGSN

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
[ no ] debug ipv6 ospf route [ ase | ia | install | spf ]
```

**no**

Disables debugging of route information. If no keyword is specified all information types are disabled.

**ase**

Enables debugging information on autonomous system external (ASE) route calculations.

**ia**

Enables debugging information on Inter-Area route calculations.

**install**

Enables debugging information on route installation.

**spf**

Enables debugging information on Shortest Path First (SPF) route calculations.

**Usage Guidelines**

Use this command to output debug information for OSPF routes.

**Example**

To enable all route debug information, enter the following command;

```
debug ipv6 ospf route
```

To disable all route debug information, enter the following command;

```
no debug ipv6 ospf route
```

## default terminal

Restores the system default value for the terminal options.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
default terminal { length | width }
```

**length | width**

**length:** Resets the terminal length to the system default.

**width:** Resets the system default terminal width.

**Usage Guidelines**

Restore the default terminal settings when the current paging and display wraps inappropriately or pages to soon.

**Example**

The following sets the default length then width in two commands.

```
default terminal length
```

```
default terminal width
```

# delete

Removes the specified file(s) permanently from the local.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
delete filepath [ -noconfirm ]
```

***filepath***

Specifies the location of the file to rename. The path must be formatted as follows:

For the ASR 5000:

```
[ file: ]{ /flash | /pcmcial | /hd-raid }[ /directory ]/file_name
```

**Important**

Use of the ASR 5000 SMC hard drive is not supported in this release.

For the ASR 5500:

```
[ file: ]{ /flash | /usb1 | /hd-raid }[ /directory ]/file_name
```

For VPC:

```
[ file: ]{ /flash | /hd-raid / usb1 | usb2 | /cdrom1 }[ /directory ]/file_name
```

**Important**

The USB ports and CD-ROM must be configured via the hypervisor to be accessible.

**Important**

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

*directory* is the directory name

*filename* is the actual file of interest

### **-noconfirm**

Executes the command without any additional prompt and confirmation from the user.



### **Important**

Use of the **-noconfirm** option should be done with extra care to ensure the file is specified accurately as there is no method of recovering a file that has been deleted.

### **Usage Guidelines**

Deleting files is a maintenance activity which may be part of periodic routine procedures to reduce system space utilization.

### **Example**

The following removes files from the local */flash/pub* directory.

```
delete /flash/pub/june03.cfg
```

## delete support record

Removes a Support Data Record (SDR) with a specified record-id or all SDRs in the specified range of record-ids.

### **Product**

All

### **Privilege**

Security Administrator, Administrator

### **Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### **Syntax Description**

```
delete support record <record-id> [ to <record-id> ]
```

#### ***record-id***

Specifies a single SDR as an integer from 0 to 65536.

Each SDR is identified by a time index called the record-id. For example, the most recent record is always record-id 0 (filename = sdr.0.gz). The next older record is record-id 1 (filename = sdr.1.gz), and so on.

#### ***to record-id***

Specifies the endpoint record-id when deleting a range of SDRs.

### **Usage Guidelines**

Use this command to delete one or more SDRs stored on the system. For additional information on the Support Data Collector feature, refer to the *System Administration Guide*.

**Example**

The following command deletes the SDR with a record-id of 5 (filename = sdr.5.gz):

```
delete support record 5
```

## dhcp force

Tests the lease-renewal for DHCP-assigned IP addresses for a particular subscriber.

**Product**

GGSN  
ASN-GW  
P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
dhcp force lease-renewal { callid id | imsi imsi [ nsapi nsapi ] | msid msid }
```

**callid *id***

Clears the call ID specified as a 4-byte hexadecimal number.

**imsi *msid***

Disconnects the subscriber with the specified msid. The IMSI (International Mobile Subscriber Identity) ID is a 50-bit field which identifies the subscriber's home country and carrier. Wildcard characters \$ and \* are allowed. The \* wildcard matches multiple characters and the \$ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes ( ' ). For example; '\$'.

**nsapi *nsapi***

Specifies a Network Service Access Point Identifier (NSAPI) an integer from 5 to 15.

**msid *id***

Disconnects the mobile user identified by *ms\_id*. *ms\_id* must be from 7 to 16 digits specified as an IMSI, MIN, or RMI. Wildcard characters \$ and \* are allowed. The \* wildcard matches multiple characters and the \$ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes ( ' ). For example; '\$'.

**Usage Guidelines**

Use this command tests a forced IP address lease renewal for a specific subscriber.

**Example**

The following command tests DHCP lease renewal for a subscriber with an MSID of *1234567*:

```
dhcp force lease-renewal msid 1234567
```

# dhcp test

Tests DHCP (Dynamic Host Configuration Protocol) functions for a particular DHCP service.

**Product**

GGSN  
ASN-GW  
P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
dhcp test dhcp-service svc_name [ all | server ip_address ]
```

**dhcp-service *svc\_name***

Specifies the name of the DHCP service as an alphanumeric string of 1 through 63 characters that is case sensitive.

**all**

Tests DHCP functionality for all servers.

**server *ip\_address***

Tests DHCP functionality for the server specified by an IP address entered using IPv4 dotted-decimal notation.

**Usage Guidelines**

Once DHCP functionality is configured on the system, this command can be used to verify that it is configured properly and that it can successfully communicate with the DHCP server.

Executing this command causes the system to request and allocate an IP address and then release it.

If a specific DHCP server is not specified, then each server configured in the service is tested.

**Example**

The following command tests the systems ability to get an IP address from all servers a DHCP service called *DHCP-Gi* is configured to communicate with:

```
dhcp test dhcp-service DHCP-Gi all
```

# diameter disable endpoint

Disables a Diameter endpoint without removing the peer's configuration.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **diameter disable endpoint** *endpoint\_name* **peer** *peer\_id*

***endpoint\_name***

Specifies the endpoint in which the peer is configured as an alphanumeric string of 1 through 63 characters.

**peer *peer\_id***

Specifies the Diameter peer host name to be disabled as an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to administratively disable a Diameter peer without removing the peer configuration. This command will tear down all connections on the specified peer (by sending a DPR if the configuration demands the same at peer level configuration). The peer will remain in disabled state until it is enabled again. Also see the **diameter enable endpoint** command.

**Example**

This command disables the Diameter peer *peer12*:

```
diameter disable endpoint endpoint1 peer peer12
```

# diameter enable endpoint

Enables a Diameter endpoint that is disabled.

**Product** All

**Privilege** Security Administrator, Administrator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **diameter enable endpoint** *endpoint\_name* **peer** *peer\_id*

**endpoint\_name**

Specifies the endpoint in which the peer is configured as an alphanumeric string of 1 through 63 characters.

**peer peer\_id**

Specifies the Diameter peer host name to be enabled as an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to administratively enable a Diameter peer. Also see the **diameter disable endpoint** command.

**Example**

This command enables the Diameter peer *peer12*:

```
diameter enable endpoint endpoint1 peer peer12
```

## diameter-proxy conn-audit

This command enables the Diameter proxy Peer Connection Status Audit with Diabase clients.

**Product**

P-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
diameter-proxy conn-audit interval 1-10
default diameter-proxy conn-audit
```

**default**

Configures the default setting.

By default, Diameter proxy Peer Connection Status Audit with Diabase clients is disabled.

**diameter-proxy**

Specifies the Diameter proxy related configurations.

**conn-audit**

Specifies the periodic connection status audit processes. Disabled by default.

**interval 1-10**

Specifies the connection status audit interval in minutes, in the range of 1 through 10. Recommended value is 2 minutes.



**Usage Guidelines**

Enabling Diamproxy Peer Connection Status Audit with Diabase clients might affect performance of the services using Diameter interface. Service is impacted only when auto-correction happens (due to mismatch) and the cases are:

1. When Diabase state is IDLE and Diameter proxy is OPEN.
2. When Diabase state is OPEN and Diameter proxy is IDLE.

In both these cases, Diabase corrects the connection status based on information received in audit message. Diameter messaging failures is avoided once Diabase corrects the connection status.

**Example**

The following command specifies that the connection status audit interval is 2minutes:

```
diameter-proxy conn-audit interval 2
```

## diameter reset connection

Resets individual TCP/SCTP connections for a specified Diameter endpoint.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
diameter reset connection { endpoint endpoint_name peer peer_id }
```

**endpoint *endpoint\_name***

Resets connection to the endpoint specified as an alphanumeric string of 1 through 63 characters.

**peer *peer\_id***

Resets connection to the Diameter peer host name specified as an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to reset the TCP/SCTP connections for the specified endpoint/peer. With this command, the connection will be closed temporarily after DPR/DPA. If there is any traffic to be sent to the particular peer, then the connection will be re-established.

This command overrides the endpoint configured in any other configuration mode.

This command is applicable only when the specified peer is enabled.

**Example**

This command resets connection to the endpoint named *test123*:

```
diameter reset connection endpoint test123
```

## diameter reset route failure

Resets the failed route status of a Diameter destination-host combination via peer to AVAILABLE status.

---

**Product** All

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **diameter reset route failure** [ **endpoint** *endpoint\_name* ] [ **host** *host\_name* ] [ **peer** *peer\_id* ]

**endpoint** *endpoint\_name*

Resets paths to the endpoint specified as an alphanumeric string of 1 through 63 characters.

**host** *host\_name*

Resets the FAILED status of all Diameter destination-host combination routes via peer for every Diameter client within the chassis having a specific host name to AVAILABLE.

Specifies the Diameter host name as an alphanumeric string of 1 through 63 characters.

**peer** *peer\_id*

Resets the FAILED status of all Diameter destination-host combination routes via a peer having specific peer-Id for every Diameter client within the chassis to AVAILABLE.

Specifies the Diameter peer host name as an alphanumeric string of 1 through 63 characters.

---

**Usage Guidelines**

Use this command to reset the FAILED status of all Diameter destination-host combination routes via peer for every Diameter client within the chassis to AVAILABLE status.

This command also resets the failure counts used to determine the AVAILABLE/FAILED status of a destination-host combination.

When executed from local context, this command matches all contexts. If an optional keyword is not supplied, a wildcard is used for the value.

The status of every matching combination of destination-host via peer for every matching Diameter client within the chassis will be reset to AVAILABLE. The failure counts that are used to determine AVAILABLE/FAILED status will also be reset.

Also see the **route-entry** and **route-failure** commands in the *Diameter Endpoint Configuration Mode Commands* chapter.

Default value: N/A

**Example**

The following command resets the FAILED status of all Diameter destination-host combination routes via peer for every Diameter client within the chassis for specified endpoint name to AVAILABLE.

```
diameter reset route failure endpoint endpoint123
```

# directory

Lists the files in a specified location.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
directory filepath [ -size ] [ -reverse ] [ -time ]
```

***filepath***

Specifies the directory path to list the contained files using the following format:

For the ASR 5000:

```
[ file: ]{ /flash | /pcmcia1 | /hd }[ /directory ]/file_name
```

**Important**

Use of the ASR 5000 SMC hard drive is not supported in this release.

For the ASR 5500:

```
[ file: ]{ /flash | /usb1 | /hd }[ /directory ]/file_name
```

For VPC:

```
[ file: ]{ /flash | /hd-raid | /usb1 | /usb2 | cdrom1 }[ /directory ]/file_name
```

**Important**

The USB ports and CD-ROM must be configured via the hypervisor to be accessible.

**Important**

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

*directory* is the directory name

*filename* is the actual file of interest

**-size**

Indicates the size of each file should be displayed in the output.

**-reverse**

Indicates the order of files listed should be in descending order (z-aZ-A9-0). Default is to sort in ascending order (0-9A-Za-z).

**-time**

Indicates the last modification timestamp of each file should be displayed in the output.

**Usage Guidelines**

Lists such things as log and crash files from multiple nodes within the network.

The optional arguments may be specified individually or in any combination.

**Example**

The following command will list the files in the local */flash/pub* directory sorted in reverse order.

```
directory /flash/pub -reverse
```

## disable radius

Prevents the system from making requests of a selected RADIUS server.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
disable radius { [ charging ] [ accounting ] server ipv4/ipv6_address [ group group_name | port port_number + ] }
```

**[ charging ] [ accounting ]**

Specifies the type of RADIUS server to disable.

- **accounting**: Specifies accounting servers
- **charging**: Specifies charging servers
- **charging accounting**: Specifies charging accounting servers

**server *ipv4/ipv6\_address***

Specifies the RADIUS server by IP address entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**port *port\_number***

Specifies the port number of the RADIUS server being disabled an integer from 0 through 65535. Default: 1812 (authentication) 1813 (accounting)

**group *group\_name***

Specifies the RADIUS group to which the server belongs as an alphanumeric string of 1 through 63 characters. Use this option in the event that the RADIUS server belongs to multiple groups and you only want to disable the server within the specific group. Default: **default**

**Usage Guidelines**

Use this command to gracefully stop the system from making requests of a specific RADIUS server.

**Example**

The following command disables a RADIUS accounting server with an IP address of *10.2.3.4*, the default accounting server port number, and that resides in the *Group5* server group:

```
disable radius accounting server 10.2.3.4 group Group5
```

## dns-client

Performs DNS (Domain Name System) query on the basis of specified DNS client name, DNS query domain name, and type of query criteria.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
dns-client dns_client_name [ query-type { A | AAAA | NAPTR | SRV } ]  
query-name query_domain_name
```

**dns-client *dns\_client\_name***

Specifies the name of the DNS client whose cache and/or statistics are to be queried. It must be an existing DNS client expressed as an alphanumeric string of 1 through 64 characters.

**query-type { **A** | **NAPTR** | **SRV** }**

Specifies that the type of query to perform for the defined DNS client is to be displayed.

- **A**: Filters DNS results based on domain IPv4 address records (A records). This is the default query type.

- **AAAA**: Filters DNS results based on domain IPv6 address records (AAAA records).
- **NAPTR**: Filters DNS results based on Naming Authority Pointer records (NAPTR).
- **SRV**: Filters DNS results based on service host records (SRV records).

#### **query-name *query\_domain\_name***

Filters the DNS results based on the query domain name expressed as an alphanumeric string of 1 through 255 characters.

*query\_domain\_name* is the domain name used to perform the DNS query and is different from the actual domain name which is resolved. For example, to resolve the SIP server for *service.com*, the query name is *\_sip.\_udp.service.com* and the query type is **SRV**.

#### **Usage Guidelines**

Use this command to perform DNS query on the basis of DNS Client name and filters the query results based on query type and query name. This command also populates the result into DNS Cache. This command used the current context to DNS request.

#### **Example**

The following command displays statistics for a DNS client named *test\_dns* with query type for IP address as *A* and query name as *domain1.com*:

```
dns-client test_dns query-type A query-name domain1.com
```

## egtpc test echo

Tests the ability of a GGSN/P-GW service to exchange GTP-C echo request messages with specified peer(s).

#### **Product**

GGSN  
P-GW  
SAEGW

#### **Privilege**

Operator, Config-Administrator, Administrator

#### **Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

#### **Syntax Description**

```
egtpc test echo gtp-version version src-address ip_address { all | peer-address ip_address }
```

#### **gtp-version *version***

Specifies version number for sending Echo request message.

*version* must be an integer from 0 through 2.




---

**Important** If peer is not a new peer for service bind to **src-address**, then echo request is sent with the last known highest version of the peer.

---

**src-address *ip\_address***

Specifies the IP address of a Gn interface configured on the system.

*ip\_address* must be entered using IPv4 dotted-decimal notation or IPV6 colon-separated-hexadecimal notation.




---

**Important** The IP address of the system's Gn interface must be bound to a configured GGSN/P-GW service prior to executing this command.

---

**all**

Sends GTP-C echo requests to first 100 peers that currently have sessions with the GGSN/P-GW service.




---

**Important** If this keyword is selected, additional confirmation is required after the following message, "Warning: Due to possibility of huge number of connected peers, considering system performance impacts, issue echo request to only 100 peers".

---

**peer-address *ip\_address***

Specifies that GTP-C echo requests will be sent to a specific peer.

*ip\_address* must be entered using IPv4 dotted-decimal notation or IPV6 colon-separated-hexadecimal notation.

---

**Usage Guidelines**

This command tests the GGSN's or P-GW's ability to exchange GPRS Tunneling Protocol control plane (GTP-C) packets with the specified peer. This command is useful for troubleshooting and/or monitoring.

This command must be executed from within the context in which the GGSN/P-GW service is configured.




---

**Important** In StarOS v14.0 and later, this command replaces the **gtpv0 test echo** and **gtpc test echo** commands.

---

**Example**

The following command issues GTP-C echo packets from a GGSN service bound to address *192.168.157.43* to an SGSN with an address of *192.168.1.52*:

```
egtpc test echo gtp-version 1 src-address 192.168.157.43 peer-address
192.168.1.52
```

# enable radius

Enables the system to start making requests of a specific RADIUS server.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
enable radius { [ charging ] [ accounting ] server ipv4/ipv6_address [ group
group_name | port port_number + ] }
```

**[ charging ] [ accounting ]**

Specifies the type of RADIUS server to enable.

- **accounting**: Specifies accounting servers
- **charging**: Specifies charging servers
- **charging accounting**: Specifies charging accounting servers

**server *ipv4/ipv6\_address***

Specifies the RADIUS server by an IP address entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**port *port\_number***

Specifies the port number of the RADIUS server being enabled as an integer from 0 through 65535. Default: 1812 (authentication) 1813 (accounting)

**group *group\_name***

Specifies the RADIUS group to which the server belongs as an alphanumeric string of 1 through 63 characters. Use this option in the event that the RADIUS server belongs to multiple groups and you only want to disable the server within the specific group. Default: **default**

---

**Usage Guidelines**

Use this command to allow the system to start making requests of a specific RADIUS server.

**Example**

The following command enables a RADIUS accounting server with the IP address *10.2.3.4*, the default accounting server port number, and in the *Group5* server group:

```
enable radius accounting server 10.2.3.4 group Group5
```



## exit

Terminates the current CLI session.

---

**Product** All

---

**Privilege** Any

---

**Syntax Description** **exit**

---

**Usage Guidelines** Use this command to terminate the current CLI session.

## filesystem

Use this command to check, format or repair the filesystem on internal and external storage devices.

---

**Product** All

---

**Privilege** Security Administrator, Administrator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** For the ASR 5000:

```
filesystem { check | format | repair | synchronize } { /flash | /pcmcia1
  | /hd-raid } [ card slot_num ]
```

For the ASR 5500:

```
filesystem { check | format | repair | synchronize } { /flash | /usb1 |
  /hd-raid } [ card slot_num ]
```

For VPC:

```
filesystem { check | format | repair | synchronize | update } { /flash |
  /hd-raid | /usb1 | /usb2 | cdrom1 }
```

The following devices are supported based on platform type:

- **/flash** – ASR 5x00, VPC
- **/hd-raid** – ASR 5x00, VPC
- **/pcmcia1** – ASR 5000 only
- **/usb1** – ASR 5500, VPC (if configured via hypervisor)
- **/usb2** – VPC (if configured via hypervisor)
- **/cdrom1** – VPC (if configured via hypervisor)

**Important**

For VPC, the USB ports and CD-ROM must be configured via the hypervisor to be accessible by the Control Function (CF) virtual machine.

**check**

Checks for filesystem corruption.

**format**

Reformats file system.

**Caution**

This keyword erases all data on the device.

Formatting /flash will remove all boot configurations and the ASR 5x00 chassis-ID. Before running **format**, be sure to review or save the output of the **show boot** command. After running **format**, be sure to restore boot entries as needed, generate a new chassis-ID, and execute **save configuration** to save the running configuration.

**repair**

Repairs file system corruption.

**synchronize**

See the description of the **filesystem synchronize** command for detailed information. **Not supported on VPC-SI.**

**update**

Updates the boot code on the file system. **Supported on VPC-SI only.**

**Usage Guidelines**

Check, format, or repair all directories and files from on an internal or external storage device and re-establish the file system.

**Example**

The following command formats the PCMCIA card located in slot 1 on the SMC (ASR 5000):

```
filesystem format /pcmcial
```

## filesystem synchronize

Use this command to synchronize the file systems of active and standby storage devices on MIO card or VPC-DI Control Function (CF) virtual machines.

**Product**

All

<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<p>For the ASR 5500:</p> <pre><b>filesystem synchronize</b> [ /flash   /usb1   all ] [ checkonly ] [ from card_num   to card_num ] [-noconfirm]</pre> <p>For VPC:</p> <pre><b>filesystem synchronize</b> [ /flash   /usb1   /usb2   cdrom1   all ] [ checkonly ] [ from card_num   to card_num ] [-noconfirm]</pre> <p>The following devices are supported based on platform type:</p> <ul style="list-style-type: none"> <li>• <b>/flash</b> – ASR 5x00, VPC</li> <li>• <b>/hd-raid</b> – ASR 5x00, VPC</li> <li>• <b>/usb1</b> – ASR 5500, VPC (if configured via hypervisor)</li> <li>• <b>/usb2</b> – VPC (if configured via hypervisor)</li> <li>• <b>/cdrom1</b> – VPC (if configured via hypervisor)</li> <li>• <b>all</b> – Selects all file systems</li> </ul> <p><b>checkonly</b> Checks for file system corruption; does not modify file systems.</p> <p><b>[ from card_num   to card_num ]</b> Copies files from a source card to a destination card specified by slot numbers.</p> <p><b>-noconfirm</b> Executes the command without displaying "are you sure" prompts.</p>
<b>Usage Guidelines</b>	Synchronize the file systems between active and standby storage devices.

**Example**

The following command all file systems on the management card:

```
filesystem synchronize all
```

The following command sequence appears when **filesystem synchronize /flash** is run after **save configuration /flash/filename -redundant** is executed and a change has been made to the configuration:

```
filesystem synchronize /flash
2 to be updated on card 2
  /flash/oam.cfg
  /flash/service.cfg
0 to be updated (but are newer) on card 2
```

```
0 to be deleted on card 2
Are you sure? [Yes|No] :
```

You must confirm the synchronization before it will be initiated.

If "No files to update" appears, you are returned to the CLI prompt.

## gtpc test echo

Tests the ability of a GGSN service to exchange GTP-C echo request messages with the specified SGSN(s).

<b>Product</b>	GGSN
<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `gtpc test echo src-address gn_address { all | sgsn-address ip_address }`

### **src-address gn\_address**

Specifies the IP address of a Gn interface configured on the system in IPv4 dotted-decimal notation.



#### **Important**

The IP address of the system's Gn interface must be bound to a configured GGSN service prior to executing this command.

### **all**

Specifies that GTP-C echo requests will be sent to all SGSNs that currently have sessions with the GGSN service.

### **sgsn-address ip\_address**

Specifies that GTP-C echo requests will be sent to a SGSN specified by an IP address in IPv4 dotted-decimal notation.

#### **Usage Guidelines**

This command tests the GGSN's ability to exchange GPRS Tunneling Protocol control plane (GTP-C) packets with the specified SGSNs. This command is useful for troubleshooting and/or monitoring.

This command must be executed from within the context in which the GGSN service is configured.

Refer also to the **gtpu test** command.



#### **Important**

In StarOS v14.0 and later, this command has been replaced by the **egtpc test echo** command.

**Example**

The following command issues GTP-C echo packets from a GGSN service bound to address *192.168.157.32* to an SGSN with an address of *192.168.157.2*:

```
gtpc test echo src-address 192.168.157.32 sgsn-address 192.168.157.2
```

## gtp interm now

Check points current GTPP accounting messages and identifies which types of interim CDRs are to be generated and sent to the external charging/storage servers (for example, a CFG or a GSS). The impact of this command is immediate.

<b>Product</b>	GGSN SGSN SGW
<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

<b>Syntax Description</b>	<pre>gtp interm now [ active-charging egcdr   apn apn_name   callid call_id   cdr-types { gcdr   mcdr   scdr }   dhcp-server ip_address   gprs-service svc_name   ggsn-address ggsn_ip_addr   ggsn-service svc_name   imsi imsi [ ip-address sub_address [ username name ] ]   ip-addresssub-address   nsapi nsapi [ ip-address sub-address [ username name ] ]   ip-pool pool_name   mcc mcc_number mnc mnc_number   msisdn msisdn_num   sgsn-address ip_address   sgsn-service svc_name   username name ] +</pre>
---------------------------	---

**active-charging**

This feature is specific to the GGSN and is documented separately. .

**apn apn\_name**

Initiates GTPP interim accounting for all PDP contexts accessing the APN specified as an alphanumeric string of 1 through 62 characters that is case sensitive.

**callid call\_id**

Identifies a specific call id as an 8-digit hexadecimal number.

**cdr-types { mcdr | scdr }**

Specifies the CDR types to be generated by the SGSN:

**gcdr** - Instructs the GGSN to only generate G-CDRs.

**mcd** - Instructs the SGSN to only generate M-CDRs

**scd** - Instructs the SGSN to only generate S-CDRs.

This keyword is specific to the SGSN.

#### **dhcp-server ip\_address**

Identifies the DHCP server where the IP address (defined with the **ip address** keyword) was allocated by the IP address of the DHCP server entered using IPv4 dotted-decimal notation.

#### **ggsn-address ggsn\_ip\_addr**

Specifies the IP address of the interface to the GGSN using IPv4 dotted-decimal notation. This keyword is specific to the GGSN.

#### **ggsn-service svc\_name**

Initiates GTPP interim accounting for all PDP contexts currently being facilitated by the GGSN service specified as an alphanumeric string of 1 through 63 characters that is case sensitive. This keyword is specific to the GGSN.

#### **gprs-service svc\_name**

Initiates GTPP interim accounting for all PDP contexts currently being facilitated by an existing GPRS service specified as an alphanumeric string of 1 through 63 characters that is case sensitive. This keyword is specific to the SGSN.

#### **imsi imsi [ ip-address sub\_address [ username name ] | nsapi nsapi [ ip-address sub-address [ username name ] | username name ] ]**

Initiates GTPP interim accounting for a specific International Mobile Subscriber Identity (IMSI) number. The request could be further filtered using any of the following keywords:

- **ip-address**: Interim accounting will be performed for the IP address specified by *sub\_address*. The command can be further filtered by specifying a specific username with that address.
- **nsapi**: Interim accounting will be performed for a Network Service Access Point Identifier (NSAPI) specified as an integer from 5 to 15. The command can be further filtered by specifying a specific ip address and/or a username with that address, or just a specific username.

#### **ip-address sub\_address [ username name ]**

Initiates GTPP interim accounting for the IP address of the subscriber specified in IPv4 dotted-decimal notation.

The command can be further filtered by specifying a username with that address. The name is the subscriber's name and can be a sequence of characters and/or wildcard characters ('\$' and '\*') from 1 to 127 characters. The \* wildcard matches multiple characters and the \$ wildcard matches a single character. If you do not want the wildcard characters interpreted as wildcard enclose them in single quotes ('). For example; '\$'.

#### **ip-pool pool\_name**

Initiates GTPP interim accounting for all PDP contexts that were allocated IP addresses from an existing pool specified as an alphanumeric string of 1 through 31 characters that is case sensitive. This keyword is applicable to the GGSN only.

**mcc *mcc\_number* mnc *mnc\_number***

*mcc\_number*: Specifies the mobile country code (MCC) portion of the PLMN identifier and can be configured to any 3-digit integer value between 100 and 999.

*mnc\_number*: Specifies the mobile network code (MNC) portion of the PLMN identifier and can be configured to any 2- or 3-digit integer between 00 and 999.

**msisdn *msisdn\_num***

Configures the SGSN to include the Mobile Subscribers Integrated Services Digital Network identifier in generated CDRs (M-CDRs and/or the S-CDRs). This keyword is applicable for SGSN only.

*msisdn\_number* must be followed by a valid MSISDN number, consisting of 1 to 15 digits.

**sgsn-address *ip\_address***

Initiates GTPM interim accounting for all PDP contexts currently being facilitated by the SGSN specified by an IP address in IPv4 dotted-decimal notation. This keyword is specific to the GGSN.

**sgsn-service *svc\_name***

Initiates GTPM interim accounting for all PDP contexts currently being facilitated by an existing SGSN service specified an alphanumeric string of 1 through 63 characters that is case sensitive. This keyword is specific to the SGSN.

**username *name***

Initiates GTPM interim accounting for all PDP contexts for the subscriber name specified as an alphanumeric string of 1 through 127 characters that is case sensitive.

+

More than one of the above keywords can be entered within a single command.

---

**Usage Guidelines**

This command causes GTPM accounting CDRs to immediately be generated for all active sessions that are in the current context. If executed within the local context, CDRs will be generated for all active sessions regardless of context. This command generates only certain types of CDRs including GCDRs, SGWCDRs, and SCDRs.

The sending of the CDRs is paced so as not to overload the accounting server.

**Example**

The following command causes CDRs to immediately be generated:

```
gtpm interim now
```

## gtpm interim now active-charging egcdr

Check points current GTPM accounting messages for active charging immediately.

---

**Product**

GGSN

---

**Privilege** Security Administrator, Administrator, Operator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **gtpc interim now active-charging egcdr** [ **callid** *call\_id* | **imsi** *imsi* | **msid** *msid* | **rulebase** *rbase\_name* | **session-id** *sess\_id* | **username** *name* ]

**callid** *call\_id*

Initiates GTPC interim accounting for a session for the call ID specified as an 8-digit hexadecimal number.

**imsi** *imsi*

Initiates GTPC interim accounting for a International Mobile Subscriber Identity (IMSI) number. specified as a sequence of hexadecimal digits and wildcard characters - \$ matches a single character and \* matches multiple characters

**msid** *msid*

Initiates GTPC interim accounting for a Mobile Station Identifier (MSID) number specified as a sequence of up to 24 digits and wildcard characters - \$ matches a single character and \* matches multiple characters

**rulebase** *rbase\_name*

Initiates GTPC interim accounting for sessions that use the named active charging rulebase specified as an alphanumeric string of 1 through 24 characters.

**session-id** *sess\_id*

Initiates GTPC interim accounting for a current active charging session.

---

**Usage Guidelines**

This command causes GTPC accounting eG-CDRs to immediately be generated for active charging sessions that meet the specified criteria.

The sending of the CDRs is paced so as not to overload the accounting server.

**username** *name*

Initiates GTPC interim accounting for all PDP contexts for the subscriber name specified as an alphanumeric string of 1 through 127 characters that is case sensitive.

**Example**

The following command causes eG-CDRs to immediately be generated for active charging sessions using the rulebase named rulbase1:

```
gtpc interim now active-charging egcdr rulebase rulbase1
```



## gtp storage-server commit

Causes the GTPP storage server to archive all buffered packets.

---

### Product

GGSN  
P-GW  
SAEGW

---

### Privilege

Security Administrator, Administrator, Operator

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

**gtp storage-server commit now [ group name *group\_name* ]**

#### **group name *group\_name***

Commits Storage Server for an existing group name expressed as an alphanumeric string of 1 through 63 characters.

---

### Usage Guidelines

This command sends a request to the GTPP Storage Server to archive all buffered packets. It also deletes all CDRs that have been acknowledged by the charging gateway function (CGF). The deleted CDRs are saved in a separate file.

Note that this command must be executed from within the context in which the GTPP Storage Server is configured.

Refer to the **gtp storage-server** command in the *Context Configuration Mode Commands* chapter for more information.

## gtp storage-server streaming start

This command enables to start streaming of the copied CDR files from active chassis when the ICSR switchover occurs.

---

### Product




---

#### Important

This command is obsolete in release 16.0. In 16.0 and later releases, use the "**gtp push-to-active url**" CLI command in global configuration mode to enable the automatic transfer of stranded CDRs to active chassis.

---

GGSN  
P-GW  
S-GW  
SGSN

<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<b>gtpptest storage-server streaming start [ group name group_name ]</b>  <b>group name group_name</b> Specifies the name of a GTPP group configured in the current context as an alphanumeric string of 1 through 63 characters. Note that, if the group name is not specified, then all the GTPP groups in the current context will be considered. If the group name is specified, then only the group provided in this CLI command will be considered.
<b>Usage Guidelines</b>	This command is used to resynchronize the CDRs left on local HDD with the active GTPP' streaming feed to transfer the CDRs from active chassis to IT mediation device during ICSR switchover. Note that this CLI command must be executed from within the context in which the GTPP Storage Server is configured. In the event of ICSR switchover, to transfer the copied CDRs from active chassis to IT mediation device, follows these steps: <ol style="list-style-type: none"> <li>1. Manually copy files from old active chassis to new active chassis.</li> <li>2. Issue this CLI command "<b>gtpptest storage-server streaming start</b>" to start streaming of the copied files from active chassis.</li> <li>3. If the streaming is in progress, then wait till the current file is fully streamed out. After the current file is fully streamed out, then rebuild the file list (to get the copied CDR files) and start streaming based on the timestamp.</li> <li>4. If the streaming is not in progress then rebuild the file list (to get the copied CDR files) and start streaming.</li> </ol>

## gtpptest

Tests communication with configured Charging Gateway Function (CGF) servers or a GTPP Storage-Server.

<b>Product</b>	ePDG GGSN P-GW SAEGW SGSN
<b>Privilege</b>	Operator, Config-Administrator, Administrator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#

**Syntax Description**

```
gtp test { accounting { all | cgf-server ipv4/ipv6_address [ port port_num ]
| group name group_name } | storage-server [ address ipv4/ipv6_address port
udp-port | group name group_name ] }
```

**all**

Tests all CGFs configured within the given context.

**cgf-server *ipv4/ipv6\_address* [ port *port\_num* ]**

Tests a CGF configured within the given context and specified by the IP address of the CGF entered using IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.

**port *port\_num***: Specifies the port number of CGF server. The port number must be an integer ranging from 1 to 65535.

This optional keyword is introduced to ease the identification of product specific CDRs. This configuration provides the flexibility to send ePDG, SaMOG and P-GW LBO CDRs to the same CGF server on different ports.

When the port is specified, this command displays the status of CGF server with the specified IP address and port. If port is not provided then it will show the status of all CGF servers with the specified IP address.

**group name *group\_name***

Tests the storage server for an existing group name specified as an alphanumeric string of 1 through 63 characters.

**storage-server [ address *ipv4/ipv6\_address* port *udp-port* ]**

Tests the connectivity and provides round trip time for the echo request sent to the GTPP Storage-Server configured in the requested context. The IP address of the GSS is entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation and the UDP port is the one defined for the GTPP Storage Server.

**Usage Guidelines**

This command is used to verify the configuration of and test the system's ability to communicate with one or all configured GSS/CGFs for monitoring or troubleshooting purposes.

When executed, this command causes the system to send GTPP echo packets to the specified GSS/CGF(s). The command's response will display whether the GSS/CGF is active or unreachable.

**Example**

The following command tests communication with a CGF server having an IP address of *192.168.1.5*:

```
gtp test accounting cgf-server 192.168.1.5
```

The following command tests communication with a GSS configured in requested context:

```
gtp test storage-server
```

The following command verifies the communication with a GSS having an IP address of *192.156.12.10* and port *50000*, without configuring it in a context:

```
gtp test storage-server address 192.156.12.10 port 50000
```

# gtpu test echo

Tests the ability of a GGSN/P-GW/SAEGW/SGSN/S-GW service to exchange GTP-U echo request messages with specified peer(s).

<b>Product</b>	GGSN P-GW SAEGW SGSN S-GW
----------------	---------------------------------------

<b>Privilege</b>	Operator, Config-Administrator, Administrator
------------------	---

<b>Command Modes</b>	Exec  The following prompt is displayed in the Exec mode:  [local]host_name#
----------------------	--

<b>Syntax Description</b>	StarOS v12.x and earlier:  <b>gtpu test echo src-address</b> <i>gn_address</i> { <b>all</b>   <b>sgsn-address</b> <i>ip_address</i> }  StarOS v14.0 and later:  <b>gtpu test echo gtpu-service</b> <i>service_name</i> { <b>all</b>   <b>peer-address</b> <i>ip_address</i> } [ <b>gtpu-version</b> { 0   1 } ]
---------------------------	---

### **src-address** *gn\_address*

Specifies the IP address of a Gn interface configured on the system using IPv4 dotted-decimal notation.



<b>Important</b>	The IP address of the system's Gn interface must be bound to a configured GGSN service prior to executing this command.
------------------	---

### **all**

Sends GTP-U echo requests to all SGSNs that currently have sessions with the GGSN service.

### **sgsn-address** *ip\_address*

Sends GTP-U echo requests to an SGSN specified by its IP address in IPv4 dotted-decimal notation.

### **gtpu-service** *service\_name*

Specifies an existing GTP-U service.

*service\_name* is an alphanumeric string of 1 through 63 characters.

**all**

Sends GTP-U echo requests to first 100 peers that currently have sessions with the GTP-U service.

**Important**

If this keyword is selected, additional confirmation is required after the following message, "Warning: Due to possibility of huge number of connected peers, considering system performance impacts, issue echo request to only 100 peers".

**peer-address *ip\_address***

Specifies that GTP-U echo requests will be sent to a specific peer.

*ip\_address* must be entered using IPv4 dotted-decimal notation or IPV6 colon-separated-hexadecimal notation.

**gtpu-version { 0 | 1 }**

Optional. Specifies the GTP-U version in which the test echo will be sent. **0** Specifies GTP-U version 0, and **1** specifies GTP-U version 1.

- If the GTP-U version of the peer is unknown, the GGSN/P-GW/SAEGW/SGSN/S-GW will use the user-configured GTP-U version.
- If the GTPU version of peer node is already known, the test echo is sent in the known GTP-U version.
- If the GTP-U version is not configured, and the peer version is unknown, the test echo is sent in GTP-U version 0.

**Usage Guidelines**

This command tests the GGSN/P-GW/SAEGW/SGSN/S-GW's ability to exchange GPRS Tunneling Protocol user plane (GTP-U) packets with the specified SGSNs/peer(s). This command is useful for troubleshooting and/or monitoring.

**Important**

This command returns statistics on the number of packets transmitted and received; however, statistics are displayed right after transmitting the "echo" packet, but before receiving the response. Therefore, received statistics are always off by one. For more information, the same command should be run twice.

For example:

```
[ingress]asr5000# gtpu test echo gtpu-service sgw_ingress_gtpu peer-address 192.45.1.6
gtpu-version 1
GTPU test echo
-----
PEER: 192.45.1.6 Tx/Rx: 1/0 RTT(ms): 0 Recovery

[ingress]asr5000#
[ingress]asr5000# gtpu test echo gtpu-service sgw_ingress_gtpu peer-address 192.45.1.6
gtpu-version 1
GTPU test echo
-----
PEER: 192.45.1.6 Tx/Rx: 2/1 RTT(ms): 4285432 (COMPLETE)
```

Refer also to the **gtpc test** command.

**Example**

The following command issues GTP-U echo packets from a GGSN service bound to address *192.168.157.43* to an SGSN with an address of *192.168.1.52*:

```
gtpu test echo src-address 192.168.157.43 sgsn-address 192.168.1.52
```

The following command issues GTP-U echo packets from a GTP-U service named *gtpu\_1* to the first 100 connected peers:

```
gtpu test echo gtpu-service gtpu_1 all
```

## gtpv0 test echo

Tests the ability of a GGSN service to exchange GTPv0 echo request messages with the specified SGSN(s).

**Product**

GGSN

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
gtpv0 test echo src-address gn_address { all | sgsn-address ip_address }
```

**src-address gn\_address**

Specifies the IP address of a Gn interface configured on the system using IPv4 dotted-decimal notation.

**Important**

The IP address of the system's Gn interface must be bound to a configured GGSN service prior to executing this command.

**all**

Sends GTPv0 echo requests to all SGSNs that currently have sessions with the GGSN service.

**sgsn-address ip\_address**

Sends GTPv0 echo requests to an SGSN specified by its IP address in IPv4 dotted-decimal notation.

**Usage Guidelines**

This command tests the GGSN's ability to exchange GPRS Tunneling Protocol version 0 (GTPv0) packets with the specified SGSNs which can be useful troubleshooting and/or monitoring.

This command must be executed from within the context in which the GGSN service is configured.

Refer also to the **gtpc test** and **gtpu test** commands.

**Important**

In StarOS v14.0 and later, this command has been replaced by the **egtpc test echo** command.

**Example**

The following command issues GTPv0 echo packets from a GGSN service bound to address *192.168.1.33* to an SGSN with an address of *192.168.1.42*:

```
gtpv0 test echo src-address 192.168.1.33 sgsn-address 192.168.1.42
```

## hd raid

Performs RAID management operations on the platform's hard disk drives.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

For the ASR 5000:

```
hd raid { check | create { local1 | remote1 } | insert { local1 | remote1
} | overwrite { local1 | remote1 } | directory pathname | limit number_files
| mtime minutes } | remove { local1 | remote1 } | select { local1 | remote1
} } [ -force ] [ -noconfirm ]
```

For the ASR 5500:

```
hd raid { check | create { hd13 | hd14 | hd15 | hd16 | hd17 | hd18 } |
insert { hd13 | hd14 | hd15 | hd16 | hd17 | hd18 } | overwrite { hd13 |
hd14 | hd15 | hd16 | hd17 | hd18 } | quarantine { directory pathname | limit
number_file | mtime minutes } | remove { hd13 | hd14 | hd15 | hd16 | hd17 |
hd18 } } [ -force ] [ -noconfirm ]
```

For VPC:

```
hd raid { check | create | insert | overwrite | quarantine { directory
pathname | limit number_files | mtime minutes } | remove | select } { local1 |
local2 } [ -force ] [ -noconfirm ]
```

**check**

Starts a background check on RAID disks unless the RAID is running in degraded mode.

**create { local1 | remote1 }**

On the ASR 5000, creates a new RAID that could run in degraded mode on the specified drive:

- **local1** specifies the RAID is to be established on the primary SMC.
- **remote1** specifies the RAID is to be established on the backup SMC.

### **create *hd\_num***

On the ASR 5500, creates a new RAID that could run in degraded mode on the hard drive array of a specific FSC.

*hd\_num* specifies the RAID is to be established. *hd\_num* corresponds to the FSC in slot numbers as shown below:

- hd13 = disk in slot 13
- hd14 = disk in slot 14
- hd15 = disk in slot 15
- hd16 = disk in slot 16
- hd17 = disk in slot 17
- hd18 = disk in slot 18

### **create { *local1* | *local2* }**

On VPC, creates a new virtual RAID as vHD Local1 or vHD Local2.

### **insert { *local1* | *remote1* }**

On the ASR 5000, inserts the specified disk to the running RAID causing it to recover from degraded mode.

- **local1** specifies the primary SMC is to be inserted into the RAID.
- **remote1** specifies the backup SMC is to be inserted into the RAID.

### **insert *hd\_num***

On the ASR 5500, inserts the specified FSC disk array into the running RAID causing it to recover from degraded mode.

*hd\_num* specifies the RAID is to be established. *hd\_num* corresponds to the FSC in slot numbers as shown below:

- hd13 = disk in slot 13
- hd14 = disk in slot 14
- hd15 = disk in slot 15
- hd16 = disk in slot 16
- hd17 = disk in slot 17
- hd18 = disk in slot 18



**insert { local1 | local2 }**

On VPC, inserts the specified vHD into the running RAID causing it to recover from degraded mode.

**overwrite { local1 | remote1 }**

On the ASR 5000, overwrites the specified disk and adds it to the current running RAID to construct a fully mirrored array.

- **local1** specifies the primary SMC is to be inserted into the RAID.
- **remote1** specifies the backup SMC is to be inserted into the RAID.

**overwrite *hd\_num***

On the ASR 5500, overwrites the specified FSC disk array and adds it to the current running RAID to reconstruct the RAID 5 array.

*hd\_num* specifies the RAID is to be established. *hd\_num* corresponds to the FSC in slot numbers as shown below:

- hd13 = disk in slot 13
- hd14 = disk in slot 14
- hd15 = disk in slot 15
- hd16 = disk in slot 16
- hd17 = disk in slot 17
- hd18 = disk in slot 18

**overwrite { local1 | local2 }**

On VPC, overwrites the specified vHD and adds it to the current running RAID to construct a fully mirrored array.

**quarantine [ *directory pathname* | *limit number\_files* | *mtime minutes***

Recovers and quarantines dirty-degraded RAID files.

- **directory** specifies the directory to which files are to be moved. *pathname* is expressed as an alphanumeric string of 1 through 29 characters. Default = "lost+found"
- **limit** sets the maximum number of files to quarantine. *number\_files* is an integer from 0 to 1000000; 0 is unlimited. Default = 3000 (10 files per second within 5 minutes).
- **mtime** specifies within how many minutes the file is modified to be considered suspects for quarantine. *minutes* is an integer from 0 through 1440; 0 means no files would be quarantined. Default = 5

**remove { local1 | remote1 }**

On the ASR 5000, removes the specified disk from the running RAID causing it to run in degraded mode or to fail.

- **local1** specifies the primary SMC is to be inserted into the RAID.

- **remote1** specifies the backup SMC is to be inserted into the RAID.

### **remove *hd\_num***

On the ASR 5500, removes the specified FSC disk array from the running RAID causing it to run in degraded mode or to fail.

*hd\_num* specifies the RAID is to be established. *hd\_num* corresponds to the FSC in slot numbers as shown below:

- hd13 = disk in slot 13
- hd14 = disk in slot 14
- hd15 = disk in slot 15
- hd16 = disk in slot 16
- hd17 = disk in slot 17
- hd18 = disk in slot 18

### **remove { *local1* | *local2* }**

On the VPC-SI, removes the specified vHD from the running RAID causing it to run in degraded mode or to fail.

- **local1** specifies the primary vHD to be removed from the RAID.
- **local2** specifies the backup vHD to be removed from the RAID.

### **remove { *local1* | *remote1* }**

On the VPC-DI, removes the specified vHD from the running RAID causing it to run in degraded mode or to fail.

- **local1** specifies the disk on the active Control Function (CF) to be removed from the RAID.
- **remote1** specifies the disk on the backup CF to be removed from the RAID.

### **select { *local1* | *remote1* }**

On the ASR 5000, selects the specified disk to assemble a RAID when two unrelated RAID disks are present in the system. The resulting RAID runs in degraded mode.

- **local1** specifies the primary SMC is to be inserted into the RAID.
- **remote1** specifies the backup SMC is to be inserted into the RAID.

### **select { | *local1* | *local2* }**

On VPC-SI, selects the specified vHD to assemble a RAID when two or more unrelated RAID disks are present in the system. The resulting RAID runs in degraded mode.

- **local1** specifies the primary vHD to be inserted into the RAID.

- **local2** specifies the backup vHD to be inserted into the RAID.

### **select { | local1 | remote1 }**

On VPC-DI, selects the specified vHD to assemble a RAID when two or more unrelated RAID disks are present in the system. The resulting RAID runs in degraded mode.

- **local1** specifies the disk on the active Control Function (CF) to be inserted into the RAID.
- **remote1** specifies the disk on the backup CF to be inserted into the RAID.

### **-noconfirm**

Executes the command without displaying "Are you sure" prompt.

### **-force**

Executes the command and overrides warnings.

## Usage Guidelines

All commands need confirmation unless the **-noconfirm** is included in the command. If the result will bring down a running RAID, you have to force the command using **-force**.

RAID commands are needed to intervene in the following situations:

- The hard disk controller task can not determine the correct operation.
- Administrative action is required by policy.
- The administrator wants to wipe out an unused disk.

In an automated system, the policies created with this CLI address the possibility of a manually partitioned disk, a disk resulting from a different version of software, a partially constructed disk, or the case of two unrelated disks in the system.

To reduce administrator intervention, a set of policies can be configured to set the default action using the commands in the HD RAID configuration mode. These commands are described in the *HD Storage Policy Configuration Mode Commands* chapter of this guide.



### Caution

Use of the **hd raid** commands and keywords has the potential for deleting the contents of hard disk drives without the possibility of recovery. You should only use these commands under guidance from the Cisco Technical Assistance Center (TAC).



### Important

For release 19.2 and higher on the ASR 5500, only those hd<slot> arrays having an FSC in the slot number with available disks can be specified.

### Example

The following instructs the system to setup a RAID on the primary ASR 5000 SMC hard drive.

```
hd raid create local1 -force
```

# host

Used to resolve the IP address or logical host name information via a DNS query.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator, Operator

<b>Command Modes</b>	Exec
----------------------	------

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

<b>Syntax Description</b>	<b>host</b> { <i>host_name</i>   <i>host_ip_address</i> }
---------------------------	---

### ***host\_name* | *host\_ip\_address***

Specifies the host for which IP information is to be displayed.

*host\_name*: Specifies the logical host name for which the IP address is to be displayed (via DNS lookup). This is an alphanumeric string of 1 through 127 characters.

*host\_ip\_address*: Specifies the IP address for which the associated logical host name(s) are to be displayed (via reverse DNS lookup) using IPv4 dotted-decimal notation.

<b>Usage Guidelines</b>	Verify DNS information which affects connections and packet routing.
-------------------------	--

### **Example**

The following commands will resolve the host information for *remoteABC* and *10.2.3.4* respectively.

```
host remoteABC
```

```
host 10.2.3.4
```

# install plugin

Unpacks the contents of a patch kit for a specific plugin module. This function is associated with the patch process for accommodating dynamic software upgrades.

<b>Product</b>	ADC
<b>Privilege</b>	Security Administrator, Administrator

<b>Command Modes</b>	Exec
----------------------	------

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

<b>Syntax Description</b>	<b>install plugin</b> <i>plugin_name</i> <i>patch_file_name</i>
---------------------------	---

***plugin\_name***

Specifies the name of a plugin that has been already copied onto the system as an alphanumeric string of 1 through 16 characters.

***patch\_file\_name***

Specifies the file name of the patch (.tgz extension) that was copied onto the system. Ensure that the full file path is copied.

**Usage Guidelines**

Unpacks the contents of a patch kit intended for a specific plugin module. After unpacking the patch you must configure the plugin using the **plugin** command in the Global Configuration mode.

For additional information, refer to the *Plugin Configuration Mode Commands* chapter.

**Example**

To unpack the plugin module named *p2p* with the patch file name *libp2p-1.2.0.tgz* onto the system enter the following command:

```
install plugin p2p libp2p-1.2.0.tgz
```

## interface

Configures the system to generate gratuitous ARP (G-ARP) requests in case of a failure during an inter-node online upgrade. If the chassis is not active, an error message displays.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, or Inspector with li-administrator permissions

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
interface name send gratuitous-arp ip-address
```

**Usage Guidelines**

This command generates a G-ARP for the IP address specified and sends it over the interface.

**Example**

The following generate a G-ARP for IP address *192.168.100.10*.

```
interface interface_1 send gratuitous-arp 192.168.100.10
```

## lawful-intercept

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

## lawful-intercept packet-cable

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

## lawful-intercept ssdf

Refer to the *Lawful Intercept Guide* for a description of this command.

## license

Registers and deregisters the system with Cisco as part of the Cisco Smart Licensing functionality. This command also can be used to manually refresh the Smart Licensing registration information and license information.

---

### Privilege

Administrator

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

```
license smart { deregister | register idtoken id | renew { auth | id } }
```

#### **deregister**

This command contacts the Cisco Smart Software Manager (CSSM) to revoke any previous registration. All Smart Licensing entitlements and certificates on the platform will be removed. All certificates and registration information will be removed from the trusted store. This is true even if the agent is unable to communicate with Cisco to deregister.

If the customer wishes to use Smart Licensing again they will need to run the **license smart register idtoken** command again.

#### **register idtoken *id***

Using the specified ID token the customer received from Cisco Smart Software Manager (CSSM), this command registers this product with Cisco and receives back an identity certificate. This certificate is saved and automatically used for all future communications with Cisco. After registration it will send the current license usage information to Cisco. Every 180 days the agent will automatically renew the registration information with Cisco. The ID token is not saved on the device. By default, the system/product is not registered with the the Cisco Smart Software Manager (CSSM).

*id* is a string from 1 to 512 characters.

#### **renew { auth | id }**

- **auth:** Manually renews authorization of Smart Licenses in use. Since the license authorization is renewed automatically by the system every 6 months, you do not typically need to issue this command.

- **id:** Manually renews the id certificate and registration with CSSM. Since the registration renewal is automatically performed by the system every 6 months, you do not typically need to issue this command.

---

**Usage Guidelines**

Before issuing these commands, you must enable Smart Licensing using the **license smart enable** Global Config Mode command.

For additional information, refer to the *Licensing* chapter in the *System Administration Guide*.

**Example**

To register the system with Cisco Smart Software Manager (CSSM) for Smart Licensing, enter the following command:

```
license smart register
```

## link-aggregation port switch to

When a link aggregation group (LAG) contains two sets of ports with each connecting to a different Ethernet switch, this command allows you to change the status of the active distributing ports. (ASR 5x00 only)

Default: none.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator, Operator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

**link-aggregation port switch to** *slot# / port#*

**slot#**

Identifies the physical chassis slot where the line card or MIO card is installed.

**port#**

Identifies the physical port on the line card or MIO card to automatically switch to.

---

**Usage Guidelines**

This command is subject to the following restrictions:

- *slot#/port#* must support LAG.
- *slot#/port#* must be configured with LAG.
- *slot#/port#* must not be actively distributing.
- *slot#/port#* must have negotiated a partner while in standard mode.
- *slot#/port#*'s partner must have a priority equal to or greater than itself.

- *slot#/port#*'s partner bundle must have bandwidth in standard mode equal to or greater than itself.
- Switching to *slot#/port#* must not violate preference within hold-time in standard mode.

### Example

```
link-aggregation port switch to 17/2
link-aggregation port switch to 5/12
```

## logging active

Enables or disables logging for active internal log files.

### Product

All

### Privilege

Security Administrator, Administrator, Operator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
logging active [ copy runtime filters ] [ event-verbosity event_level ] [ pdu-data format ] [ pdu-verbosity pdu_level ] [ no logging active
```

### no

Indicates the internal logging is to be disabled.

### copy runtime filters

Copies the runtime filters and uses that copy to filter the current logging session.

### event-verbosity *event\_level*

Specifies the level of verbosity to use in logging of events as one of:

- *min*: Displays minimal information about the event. Information includes event name, facility, event ID, severity level, date, and time.
- *concise*: Displays detailed information about the event, but does not provide the event source within the system.
- *full*: Displays detailed information about event, including source information, identifying where within the system the event was generated.

### pdu-data *format*

Specifies output format for packet data units when logged as one of:



- *none*: raw format (unformatted).
- *hex*: hexadecimal format.
- *hex-ascii*: hexadecimal and ASCII similar to a main-frame dump.

### **pdu-verbosity pdu\_level**

Specifies the level of verbosity to use in logging of packet data units as an integer from 1 through 5, where 5 is the most detailed.

#### **Usage Guidelines**

Adjust the active logging levels when excessive log file sizes are being generated or, conversely, not enough information is being sent to the active log files for adequate troubleshooting support. The **no** keyword is used to disable internal logging.



#### **Important**

A maximum of 50,000 events may be stored in each log. Enabling more events for logging may cause the log to be filled in a much shorter time period. This may reduce the effectiveness of the log data as a shorter time period of event data may make troubleshooting more difficult.



#### **Important**

Once a log has reached the 50,000 event limit the oldest events will be discarded as new log entries are created.

#### **Example**

The following sets the active logging for events to the maximum.

```
logging active event-verbosity full
```

The following command sets the active logging for packet data units to level 3 and sets the output format to the main-frame style *hex-ascii*.

```
logging active pdu-data hex-ascii pdu-verbosity 3
```

The following disables internal logging.

```
no logging active
```

## logging filter

Sets the logging filtering options for all or individual facilities.

#### **Product**

All

#### **Privilege**

Security Administrator, Administrator, Operator

#### **Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `logging filter active facility facility level severity_level [ critical-info | no-critical-info ]`

`logging filter { disable | enable } facility facility { all | instance instance_number }`

#### active

Indicates only active processes are to have logging options set.

#### disable

Disables logging for a specific instance or all instances. This keyword is only supported for aaamgr, hamgr and sessmgr facilities.

#### enable

Enables logging for a specific instance or all instances. This keyword is only supported for aaamgr, hamgr and sessmgr facilities.



#### Important

By default logging is enabled for all instances of aaamgr, hamgr and sessmgr.

#### facility *facility*

Specifies the facility to modify the filtering of logged information. Valid facilities for this command are:

- **a10**: A10 interface facility
- **a11**: A11 interface facility
- **a11mgr**: A11 Manager facility
- **aaa-client**: Authentication, Authorization and Accounting (AAA) client facility
- **aaamgr**: AAA manager logging facility
- **aaaproxy**: AAA Proxy facility
- **aal2**: ATM Adaptation Layer 2 (AAL2) protocol logging facility
- **acl-log**: Access Control List (ACL) logging facility
- **acsctrl**: Active Charging Service (ACS) Controller facility
- **acsmgr**: ACS Manager facility
- **afctrl**: Fabric Controller facility [ASR 5500 only]
- **afmgr**: Fabric Manager logging facility [ASR 5500 only]
- **alarmctrl**: Alarm Controller facility
- **alcap**: Access Link Control Application Part (ALCAP) protocol logging facility
- **alcapmgr**: ALCAP manager logging facility
- **all**: All facilities

- **bfd**: Bidirectional Forwarding Detection (BFD) protocol logging facility
- **bgp**: Border Gateway Protocol (BGP) facility
- **bindmux**: IPCF BindMux-Demux Manager logging facility
- **bngmgr**: Broadband Network Gateway (BNG) Demux Manager logging facility
- **bssap+**: Base Station Sub-system Application Part+ protocol facility for the login interface between the SGSN and the MSC/VLR (2.5G and 3G)
- **bssgp**: Base Station Sub-system GPRS Protocol logging facility handles exchange information between the SGSN and the BSS (2.5G only)
- **bulkstat**: Statistics logging facility
- **callhome**: Call Home application logging facility
- **cap**: CAMEL Application Part (CAP) logging facility for protocol used in prepaid applications (2.5G and 3G)
- **cbsmgr**: Cell Broadcasting Service (CBS) logging facility [HNBGW]
- **cdf**: Charging Data Function (CDF) logging facility
- **cgw**: Converged Access Gateway (CGW) logging facility
- **cli**: Command Line Interface (CLI) logging facility
- **cmp**: Certificate Management Protocol (IPSec) logging facility
- **confdmgr**: ConfD Manager proctet (NETCONF) logging facility
- **connectedapps**: SecGW ASR 9000 oneP communication proctol
- **connproxy**: Controller Proxy logging facility
- **credit-control**: Credit Control (CC) facility
- **csp**: Card/Slot/Port controller facility
- **css**: Content Service Selection (CSS) facility
- **css-sig**: CSS RADIUS Signaling facility
- **cx-diameter**: Cx Diameter Messages facility [CSCF <--> HSS]
- **data-mgr**: Data Manager Framework logging facility
- **dcardctrl**: IPsec Daughter Card Controller logging facility
- **dcardmgr**: IPsec Daughter Card Manager logging facility
- **demuxmgr**: Demux Manager API facility
- **dgbmbr**: Diameter Gmb Application Manager logging facility
- **dhcp**: Dynamic Host Configuration Protocol (DHCP) logging facility
- **dhcpx6**: DHCPv6
- **dhost**: Distributed Host logging facility

- **diabase**: Diabase messages facility
- **diactrl**: Diameter Controller procelet logging facility
- **diameter**: Diameter endpoint logging facility
- **diameter-acct**: Diameter Accounting
- **diameter-auth**: Diameter Authentication
- **diameter-dns**: Diameter DNS subsystem
- **diameter-ecs**: ACS Diameter signaling facility
- **diameter-engine**: Diameter version2 engine logging facility
- **diameter-hdd**: Diameter Horizontal Directional Drilling (HDD) Interface facility
- **diameter-svc**: Diameter Service
- **diamproxy**: DiamProxy logging facility
- **dpath**: IPSec Data Path facility
- **drvctrl**: Driver Controller facility
- **dpath**: IPSec Data Path logging facility
- **drvctrl**: Driver Controller logging facility
- **doulosuemgr**: Doulos (IMS-IPSec-Tool) user equipment manager
- **eap-diameter**: Extensible Authentication Protocol (EAP) IP Sec urity facility
- **eap-ipsec**: Extensible Authentication Protocol (EAP) IPSec facility
- **eap-sta-s6a-s13-s6b-diameter**: EAP/STA/S6A/S13/S6B Diameter messages facility
- **ecs-css**: ACSMGR <-> Session Manager Signalling Interface facility
- **egtpc**: eGTP-C logging facility
- **egtpmgr**: enhanced GPRS Tunneling Protocol (eGTP) manager logging facility
- **egtpu**: eGTP-U logging facility
- **embms**: evolved Multimedia Broadcast Multicast Services Gateway facility
- **embms**: eMBMS Gateway Demux facility
- **epdg**: evolved Packet Data (ePDG) gateway logging facility
- **event-notif**: Event Notification Interface logging facility
- **evlog**: Event log facility
- **famgr**: Foreign Agent manager logging facility
- **firewall**: Firewall logging facility
- **fng**: Femto Network Gateway (FNG) logging facility
- **gbmgr**: SGSN Gb Interface Manager facility

- **gmm**:
  - For 2.5G: Logs the GPRS Mobility Management (GMM) layer (above LLC layer)
  - For 3G: Logs the access application layer (above the RANAP layer)
- **gprs-app**: GPRS Application logging facility
- **gprs-ns**: GPRS Network Service Protocol (layer between SGSN and the BSS) logging facility
- **gq-rx-tx-diameter**: Gq/Rx/Tx Diameter messages facility
- **gss-gcdr**: GTP Storage Server GCDR facility
- **gtpc**: GTP-C protocol logging facility
- **gtpcmgr**: GTP-C protocol manager logging facility
- **gtp**: GTP-prime protocol logging facility
- **gtpu**: GTP-U protocol logging facility
- **gtpumgr**: GTP-U Demux manager
- **gx-ty-diameter**: Gx/Ty Diameter messages facility
- **gy-diameter**: Gy Diameter messages facility
- **h248prt**: H.248 port manager facility
- **hamgr**: Home Agent manager logging facility
- **hat**: High Availability Task (HAT) process facility
- **hdctrl**: HD Controller logging facility
- **henbapp**: Home Evolved NodeB (HNB) App facility (Do not use this keyword for HeNB-GW in Release 20, 21.0 and 21.1.)
- **henbgw**: HNB-GW facility (Do not use this keyword for HeNB-GW in Release 20, 21.0 and 21.1.)
- **henbgw-pws**: HNB-GW Public Warning System logging facility (Do not use this keyword for HeNB-GW in Release 20, 21.0 and 21.1.)
- **henbgw-sctp-acs**: HNB-GW access Stream Control Transmission Protocol (SCTP) facility (Do not use this keyword for HeNB-GW in Release 20, 21.0 and 21.1.)
- **henbgw-sctp-nw**: HNB-GW network SCTP facility (Do not use this keyword for HNB-GW in Release 20 and later.)
- **henbgwdemux**: HNB-GW Demux facility (Do not use this keyword for HeNB-GW in Release 20, 21.0 and 21.1.)
- **henbgwmgr**: HNB-GW Manager facility (Do not use this keyword for HeNB-GW in Release 20, 21.0 and 21.1.)
- **hnb-gw**: HNB-GW (3G Femto GW) logging facility (Do not use this keyword for HNB-GW in Release 20 and later)
- **hnbmgr**: HNB-GW Demux Manager logging facility (Do not use this keyword for HNB-GW in Release 20 and later)

- **hss-peer-service**: Home Subscriber Server (HSS) Peer Service facility
- **igmp**: Internet Group Management Protocol (IGMP)
- **ikev2**: Internet Key Exchange version 2 (IKEv2)
- **ims-authorization**: IP Multimedia Subsystem (IMS) Authorization Service facility
- **ims-sh**: HSS Diameter Sh Interface Service facility
- **imsimgr**: SGSN IMSI Manager facility
- **imsue**: IMS User Equipment (IMSUE) facility
- **ip-arp**: IP Address Resolution Protocol facility
- **ip-interface**: IP interface facility
- **ip-route**: IP route facility
- **ipms**: Intelligent Packet Monitoring System (IPMS) logging facility
- **ipne**: IP Network Enabler (IPNE) facility
- **ipsec**: IP Security logging facility
- **ipsecdemux**: IPSec demux logging facility
- **ipsg**: IP Service Gateway interface logging facility
- **ipsgmgr**: IP Services Gateway facility
- **ipsp**: IP Pool Sharing Protocol logging facility
- **kvstore**: Key/Value Store (KVSTORE) Store facility
- **l2tp-control**: Layer 2 Tunneling Protocol (L2TP) control logging facility
- **l2tp-data**: L2TP data logging facility
- **l2tpdemux**: L2TP Demux Manager logging facility
- **l2tpmgr**: L2TP Manager logging facility
- **lagmgr**: Link Aggregation Group (LAG) manager logging facility
- **lcs**: Location Services (LCS) logging facility
- **ldap**: Lightweight Directory Access Protocol (LDAP) messages logging facility
- **li**: Refer to the *Lawful Intercept Configuration Guide* for a description of this command.
- **linkmgr**: SGSN/BSS SS7 Link Manager logging facility (2.5G only)
- **llc**: Logical Link Control (LLC) Protocol logging facility; for SGSN: logs the LLC layer between the GMM and the BSSGP layers for logical links between the MS and the SGSN
- **local-policy**: Local Policy Service facility
- **location-service**: Location Services facility
- **m3ap**: M3 Application Protocol facility

- **m3ua**: M3UA Protocol logging facility
- **magmgr**: Mobile Access Gateway manager logging facility
- **map**: Mobile Application Part (MAP) protocol logging facility
- **megadiammgr**: MegaDiameter Manager (SLF Service) logging facility
- **mme-app**: Mobility Management Entity (MME) Application logging facility
- **mme-embms**: MME evolved Multimedia Broadcast Multicast Service facility
- **mme-misc**: MME miscellaneous logging facility
- **mmedemux**: MME Demux Manager logging facility
- **mmemgr**: MME Manager facility
- **mmgr**: Master Manager logging facility
- **mobile-ip**: Mobile IP processes
- **mobile-ip-data**: Mobile IP data facility
- **mobile-ipv6**: Mobile IPv6 logging facility
- **mpls**: Multiprotocol Label Switching (MPLS) protocol logging facility
- **mrme**: Multi Radio Mobility Entity (MRME) logging facility
- **mseg-app**: Mobile Services Edge Gateway (MSEG) application logging facility (This option is not supported in this release.)
- **mseg-gtpc**: MSEG GTP-C application logging facility (This option is not supported in this release.)
- **mseg-gtpu**: MSEG GTP-U application logging facility (This option is not supported in this release.)
- **msegmgr**: MSEG Demux Manager logging facility (This option is not supported in this release.)
- **mtp2**: Message Transfer Part 2 (MTP2) Service logging facility
- **mtp3**: Message Transfer Part 3 (MTP3) Protocol logging facility
- **multicast-proxy**: Multicast Proxy logging facility
- **nas**: Non-Access Stratum (NAS) protocol logging facility [MME 4G]
- **netwstrg**: Network Storage facility
- **npuctrl**: Network Processor Unit Control facility
- **npudrv**: Network Processor Unit Driver facility [ASR 5500 only]
- **npumgr**: Network Processor Unit Manager facility
- **npumgr-acl**: NPUMGR ACL logging facility
- **npumgr-drv**: NPUMGR DRV logging facility
- **npumgr-flow**: NPUMGR FLOW logging facility
- **npumgr-fwd**: NPUMGR FWD logging facility

- **npumgr-init**: NPUMGR INIT logging facility
- **npumgr-lc**: NPUMGR LC logging facility
- **npumgr-port**: NPUMGR PORT logging facility
- **npumgr-recovery**: NPUMGR RECOVERY logging facility
- **npumgr-rri**: NPUMGR RRI (Reverse Route Injection) logging facility
- **npumgr-vpn**: NPUMGR VPN logging facility
- **npusim**: NPUSIM logging facility [ASR 5500 only]
- **ntfy-intf**: Notification Interface logging facility [Release 12.0 and earlier versions only]
- **ocsp**: Online Certificate Status Protocol logging facility.
- **orbs**: Object Request Broker System logging facility
- **ospf**: OSPF protocol logging facility
- **ospfv3**: OSPFv3 protocol logging facility
- **p2p**: Peer-to-Peer Detection logging facility
- **pagingmgr**: PAGINGMGR logging facility
- **pccmgr**: Intelligent Policy Control Function (IPCF) Policy Charging and Control (PCC) Manager library
- **pdg**: Packet Data Gateway (PDG) logging facility
- **pdgdmgr**: PDG Demux Manager logging facility
- **pdif**: Packet Data Interworking Function (PDIF) logging facility
- **pgw**: Packet Data Network Gateway (PGW) logging facility
- **pmm-app**: Packet Mobility Management (PMM) application logging facility
- **ppp**: Point-To-Point Protocol (PPP) link and packet facilities
- **pppoe**: PPP over Ethernet logging facility
- **proklet-map-frwk**: Proklet mapping framework logging facility
- **push**: VPNMGR CDR push logging facility
- **radius-acct**: RADIUS accounting logging facility
- **radius-auth**: RADIUS authentication logging facility
- **radius-coa**: RADIUS change of authorization and radius disconnect
- **ranap**: Radio Access Network Application Part (RANAP) Protocol facility logging info flow between SGSN and RNS (3G)
- **rcf**: Recovery Control Task logging facility
- **rdt**: Redirect Task logging facility
- **resmgr**: Resource Manager logging facility
- **rf-diameter**: Diameter Rf interface messages facility



- **rip**: Routing Information Protocol (RIP) logging facility [RIP is not supported at this time.]
- **rlf**: Rate Limiting Function (RLF) logging facility
- **rohc**: Robust Header Compression (RoHC) facility
- **rsvp**: Reservation Protocol logging facility
- **rua**: RANAP User Adaptation (RUA) [3G Femto GW - RUA messages] logging facility
- **s102**: S102 protocol logging facility
- **s102mgr**: S102Mgr logging facility
- **s1ap**: S1 Application Protocol (S1AP) Protocol logging facility
- **sabp**: Service Area Broadcast Protocol (SABP) logging facility
- **saegw**: System Architecture Evolution (SAE) Gateway facility
- **sbc**: SBc protocol logging facility
- **sccp**: Signalling Connection Control Part (SCCP) Protocol logging (connection-oriented messages between RANAP and TCAP layers).
- **sct**: Shared Configuration Task logging facility
- **sctp**: Stream Control Transmission Protocol (SCTP) Protocol logging facility
- **sef\_ecs**: Severely Errored Frames (SEF) APIs printing facility
- **sess-gr**: SM GR facility
- **sessctrl**: Session Controller logging facility
- **sessmgr**: Session Manager logging facility
- **sesstrc**: session trace logging facility
- **sft**: Switch Fabric Task logging facility
- **sgs**: SGs interface protocol logging facility
- **sgsn-app**: SGSN-APP logging various SGSN "glue" interfaces (for example, between PMM, MAP, GPRS-FSM, SMS).
- **sgsn-failures**: SGSN call failures (attach/activate rejects) logging facility (2.5G)
- **sgsn-gtpc**: SGSN GTP-C Protocol logging control messages between the SGSN and the GGSN
- **sgsn-gtpu**: SGSN GTP-U Protocol logging user data messages between the SGSN and GGSN
- **sgsn-mbms-bearer**: SGSN Multimedia Broadcast/Multicast Service (MBMS) Bearer app (SMGR) logging facility
- **sgsn-misc**: Used by stack manager to log binding and removing between layers
- **sgsn-system**: SGSN System Components logging facility (used infrequently)
- **sgsn-test**: SGSN Tests logging facility; used infrequently
- **sgtpcmgr**: SGSN GTP-C Manager logging information exchange through SGTPC and the GGSN

- **sgw**: Serving Gateway facility
- **sh-diameter**: Sh Diameter messages facility
- **sitmain**: System Initialization Task main logging facility
- **sls**: Service Level Specification (SLS) protocol logging facility
- **sm-app**: SM Protocol logging facility
- **sms**: Short Message Service (SMS) logging messages between the MS and the SMSC
- **sndcp**: Sub Network Dependent Convergence Protocol (SNDCP) logging facility
- **snmp**: SNMP logging facility
- **sprmgr**: IPCF Subscriber Policy Register (SPR) manager logging facility
- **srdp**: Static Rating Database
- **srp**: Service Redundancy Protocol (SRP) logging facility
- **sscfnni**: Service-Specific Coordination Function for Signaling at the Network Node Interface (SSCF-NNI) logging facility
- **sscop**: Service-Specific Connection-Oriented Protocol (SSCOP) logging facility
- **ssh-ipsec**: Secure Shell (SSH) IP Security logging facility
- **ssl**: Secure Socket Layer (SSL) message logging facility
- **stat**: Statistics logging facility




---

**important** The keyword **bulkstat** was added in StarOS release 21.1 to provide consistency with other CLI commands. Both keywords are supported for statistics logging facility.

---

- **supserv**: Supplementary Services logging facility [H.323]
- **system**: System logging facility
- **tacacsplus**: TACACS+ Protocol logging facility
- **tcap**: TCAP Protocol logging facility
- **testctrl**: Test Controller logging facility
- **testmgr**: Test Manager logging facility
- **threshold**: threshold logging facility
- **ttg**: Tunnel Termination Gateway (TTG) logging facility
- **tucl**: TCP/UDP Convergence Layer (TUCL) logging facility
- **udr**: User Data Record (UDR) facility (used with the Charging Service)
- **user-data**: User data logging facility

- **user-l3tunnel**: User Layer 3 tunnel logging facility
- **usertcp-stack**: User TCP Stack
- **vim**: Voice Instant Messaging (VIM) logging facility
- **vinfo**: VINFO logging facility
- **vmgctrl**: Virtual Media Gateway (VMG) controller facility
- **vmgctrl**: VMG Content Manager facility
- **vpn**: Virtual Private Network logging facility
- **wimax-data**: WiMAX DATA
- **wimax-r6**: WiMAX R6
- **wsg**: Wireless Security Gateway (ASR 9000 Security Gateway)
- **x2gw-app**: X2GW (X2 proxy Gateway, eNodeB) application logging facility
- **x2gw-demux**: X2GW demux task logging facility

#### **all | instance *instance\_number***

Specifies whether logging will be disabled or enabled for all instances or a specific instance of aaamgr, hamgr or sessmgr. See additional information in the Usage Guidelines section.

These keywords are only supported for the **disable** and **enable** keywords.

#### **level *severity\_level***

This keyword is only supported in conjunction with the **active** keyword.

Specifies the level of information to be logged from the following list which is ordered from highest to lowest:

- **critical** - display critical events
- **error** - display error events and all events with a higher severity level
- **warning** - display warning events and all events with a higher severity level
- **unusual** - display unusual events and all events with a higher severity level
- **info** - display info events and all events with a higher severity level
- **trace** - display trace events and all events with a higher severity level
- **debug** - display all events

#### **critical-info | no-critical-info**

These keywords are only supported in conjunction with the **active** keyword.

**critical-info**: Specifies that events with a category attribute of critical information are to be displayed. Examples of these types of events can be seen at bootup when system processes and tasks are being initiated. This is the default setting.

**no-critical-info**: Specifies that events with a category attribute of critical information are not to be displayed.

#### **Usage Guidelines**

Apply filters for logged data to collect only that data which is of interest.

To enable logging of a single instance of a facility, you must first disable all instances of the facility (**logging filter disable facility *facility* all**) and then enable logging of the specific instance (**logging filter enable facility *facility* instance *instance\_number***). To restore default behavior you must re-enable logging of all instances (**logging filter enable facility *facility* all**).

**Important**

A maximum of 50,000 events may be stored in each log. Enabling more events for logging may cause the log to be filled in a much shorter time period. This may reduce the effectiveness of the log data as a shorter time period of event data may make troubleshooting more difficult.

**Important**

Once a log has reached the 50,000 event limit the oldest events will be discarded as new log entries are created.

**Caution**

Issuing this command could negatively impact system performance depending on the amount of system activity at the time of execution and/or the type of facility(ies) being logged.

**Example**

The following are selected examples used to illustrate the various options. Not all facilities will be explicitly shown as each follows the same syntax for options.

The following sets the level to log only *warning* information for *all* facilities.

```
logging filter active facility all level warning
```

The following enables the logging of critical information for the SNMP facility while setting the level to *error*.

```
logging filter active facility snmp level error critical-info
```

The following command disables logging of all *aaamgr* instances.

```
logging filter disable facility aaamgr all
```

## logging trace

Enables or disables the logging of trace information for specific calls, mobiles, or network addresses.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `[ no ] logging trace { callid call_id | ipaddr ip_address | msid ms_id | username user_name }`

**no**

Indicates the logging of trace information is to be disabled.

**callid *call\_id* | ipaddr *ip\_address* | msid *ms\_id* | username *user\_name***

**callid *call\_id*:** Specifies the exact call instance ID which is to have trace data logged.as a 4-byte hexadecimal number.

**ipaddr *ip\_address*:** Specifies the IP address in IPv4 dotted-decimal notation for which trace information is to be logged.

**msid *ms\_id*:** Specifies the mobile subscriber ID for which trace information is to be logged as 7 to 16 digits of an IMSI, MIN, or RMI.

**username *user\_name*:** Specifies a previously configured user who is to have trace information logged.

### Usage Guidelines

A trace log is useful in troubleshooting subscriber problems as well as for system verification by using a test subscriber. The **no** keyword is used to stop the logging of trace information.



#### Important

A maximum of 50,000 events may be stored in each log. Enabling more events for logging may cause the log to be filled in a much shorter time period. This may reduce the effectiveness of the log data as a shorter time period of event data may make troubleshooting more difficult.



#### Important

Once a log has reached the 50,000 event limit the oldest events will be discarded as new log entries are created.



#### Caution

Issuing this command could negatively impact system performance depending on the number of subscribers connected and the amount of data being passed.

### Example

The following commands enables/disables trace information for user *user1*.

```
logging trace username user1
```

```
no logging trace username user1
```

The following commands will enable/disable trace information logging for the user assigned IP address *10.2.3.4*.

```
logging trace ipaddr 10.2.3.4
```

```
no logging trace ipaddr 10.2.3.4
```

The following enables/disables logging of trace information for call ID *fe80AA12*.

```
logging trace callid fe80AA12
```

```
no logging trace callid fe80AA12
```

## logging session fp-flow-state-change

Enables logging for flow offload and onload state change between VPP and sessmgr.

<b>Product</b>	P-GW
<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
logging session fp-flow-state-change facility sessmgr instance  
instance_number number-of-events value
```

```
logging session fp-flow-state-change facility sessmgr instance  
instance_number duration value
```

```
[ no ] logging session fp-flow-state-change facility sessmgr instance  
instance number number-of-events value
```

```
[ no ] logging session fp-flow-state-change facility sessmgr instance  
instance number duration value
```

Event count range is 1–144000, Timer value is 1–120 seconds, and the Integer value is 1-1152.

#### **no**

Indicates that the logging information is to be disabled.

#### **facility**

Specifies the name of the facility.

#### **all**

Specifies all the instances of the facility.

#### **instance**

specifies the instance of the facility.

#### **duration**

specifies the total duration in seconds to log the events.

#### **number-of-events**

Specifies the total number of events to log.

**Usage Guidelines**

Use this command to enable logging for flow offload and onload state change between VPP and sessmgr. Logs are available on `/hd-raid/fpflowchangelog/fpflowchangelog_timestamp#.csv`. Example for timestamp is `2021-11-16_05h04m02sEST` since the flow state change logging may have performance impact, this feature must be used with discretion.

**Important**

By default, the monitoring is disabled.

**Example**

The following command enables logging for flow offload and onload state change between VPP and sessmgr:

```
logging session fp-flow-state-change facility sessmgr instance 8 duration
10
```

## logs checkpoint

Performs checkpointing operations on log data. Checkpointing identifies logged data as previously viewed or marked. Checkpointing results in only the log information since the last checkpoint being displayed; checkpointed log data is not available for viewing.

Individual logs may have up to 50,000 events in the active log. Checkpointing the logs results in at most 50,000 events being in the inactive log files. This gives a maximum of 100,000 events in total which are available for each facility logged.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

**logs checkpoint**

**Usage Guidelines**

Check point log data to set the log contents to a well-known point prior to special activities taking place. This command may also be a part of periodic regular maintenance to manage log data.

Checkpointing logs moves the current log data to the inactive logs. Only the most recently check pointed data is retained in the inactive logs. A subsequent check pointing of the logs results in the prior check pointed inactive log data being cleared and replaced with the newly check pointed data.

Checkpointing log data marks the active log data to be retained as the inactive log data. This results in the active log data, if displayed, having no data earlier than the point in time when the checkpointing occurred.




---

**Important** Checkpointing logs should be done periodically to prevent the log files becoming full. Logs which have 50,000 events logged will discard the oldest events first as new events are logged.

---




---

**Important** An Inspector-level administrative user cannot execute this command.

---

### Example

The following command immediately sets a checkpoint for event logs and moves the current log data to inactive logs:

```
logs checkpoint
```

## lsp-ping

Checks Multi Protocol Label Switching (MPLS) label switch path (LSP) connectivity for the specified IPv4 forwarding equivalence class (FEC). It must be followed by an IPv4 FEC prefix.

---

**Product** All

---

**Privilege** Security Administrator, Administrator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `lsp-ping ip_prefix_FEC [ count ping_packets ] [ | verbose ] [ | grep grep_options ]`

### *ip\_prefix\_FEC*

Specifies an IP prefix FEC with or without subnet mask entered using IPv4 dotted-decimal CIDR notation.

### *count ping\_packets*

Sets the number of ping packets to be sent as an integer from 1 through 16. Default: 4.




---

**Important** The timeout interval for the packets is 5 seconds by default.

---

### **verbose**

Sets the verbose (detailed) output mode.



**grep***grep\_options*

Pipes (sends) the output of this command to the **grep** command.

**Usage Guidelines**

This command is used to verify the MPLS LSP connectivity for the specified FEC.

**Example**

Following are the examples for using this command with all possible options for IPv4 address *13.13.13.1* and mask *32* (CIDR notation):

```
lsp-ping 13.13.13.1/32
```

```
lsp-ping 13.13.13.1/32 count 15
```

```
lsp-ping 13.13.13.1/32 verbose
```

## lsp-traceroute

Discovers MPLS LSP routes that packets actually take when traveling to their destinations. It must be followed by an IPv4 or IPv6 FEC prefix.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
lsp-traceroute ip_prefix_FEC [ maxttl time_to_live ] [ | verbose ] [ | grep grep_options ]
```

***ip\_prefix\_FEC***

Specifies the destination IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal with or without mask (CIDR notation).

**maxttl** *time\_to\_live*

Sets the maximum time to live in hops. TTL is an integer from 1 through 255. Default: 30.

**verbose**

Sets the verbose (detailed) output mode.

**grep***grep\_options*

Pipes (sends) the output of this command to the **grep** command.

**Usage Guidelines**

This command is used on the router to discover the MPLS LSP routes through which the packets will travel to their IPv4 or IPv6 destinations.

**Example**

The following command specifies the destination IP address *13.13.13.13* for which the MPLS routes will be discovered for packets to traverse:

```
lsp-traceroute 13.13.13.13/32
```

# mkdir

Creates a new directory in the local file system or in remote locations as specified.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
mkdir filepath
```

***filepath***

Specifies the directory path to create. The path must be formatted as follows:

For the ASR 5000:

```
[ file: ]{ /flash | /pcmcia1 | /hd-raid }[ /directory ]/file_name
```

**Important**

Use of the ASR 5000 SMC hard drive is not supported in this release.

For the ASR 5500:

```
[ file: ]{ /flash | /usb1 | /hd-raid }[ /directory ]/file_name
```

For VPC:

```
[ file: ]{ /flash | /hd-raid | /usb1 | /usb2 | /cdrom1 }[ /directory ]/file_name
```

**Important**

The USB ports and CDROM must be configured via the hypervisor to be accessible.



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

*directory* is the directory name

*filename* is the actual file of interest

**Usage Guidelines** Create new directories as part of periodic maintenance activities to better organize stored files.

### Example

The following creates the directory */flash/pub* in the local flash storage.

```
mkdir /flash/pub
```

## mme-mmedemux

Configures the MME Manager related commands.

**Product** MME

**Privilege** Security Administrator, Administrator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **mme mmedemux { audit-with | slap-sync } mmemgr { all | instance *value* }**

### mme

Configures the MME exec commands.

### mmedemux

Configures the MME Manager related commands.

### audit-with

Performs audit with MME Manager.

### slap-sync

Synchronizes with slap association count with MME Manager-Archive with all instances of MME Manager.

### mmemgr

Synchronizes up with MME Manager on eNodeB list.

**all**

Synchronizes up with MME Manager on eNodeB list with all instances.

**instance *value***

Synchronizes with MME Manager on eNodeB list with specific instance. *value* Must be an integer from 1 to 48.

## mme disconnect

Performs a graceful/ungraceful disconnection of an SCTP peer.

**Product**

MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
mme disconnect { s1-peer peer_ID [ graceful ] [ -noconfirm ] | sgs-peer
  peer_ID [ -noconfirm | perform-imsi-detach [ -noconfirm | detach-rate
    detach_rate [ -noconfirm ] ] ] }
```

**s1-peer *peer-ID***

Specifies the eNodeB peer ID which has to be disconnected. *peer-ID* is an integer from 1 through 4294967295.

**graceful**

Specifies that the SCTP connection to the S1 peer will be terminated with a complete handshake. By default (without this keyword), SCTP connections are aborted.

**sgs-peer *peer-ID***

Specifies the SGs peer ID which has to be disconnected. *peer-ID* must be an integer from 1 through 4294967295.

**perform-imsi-detach**

Performs IMSI detach.

**detach-rate *detach-rate***

Detaches per cycle. *detach-rate* must be an integer from 1 to 100.

**-noconfirm**

Executes the command without any additional prompts or confirmation from the user.

**Usage Guidelines**

Use this command to disconnect the SCTP connection to the specified peer eNodeB. This command can be used to remove stale eNodeB connections from the MME, even when no active SCTP connection exists.

**Example**

The following gracefully disconnects the SCTP connection with the eNodeB with a peer ID of 22315734:

```
mme disconnect s1-peer 22315734 graceful -noconfirm
```

## mme imsimgr

Triggers an MME IMSIMgr audit for IMSI, IMEI, MSISDN information for a specific SessMgr instance associated with a specific IMSIMgr instance.

**Product**

MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
mme imsimgr instance instance_id audit-with sessmgr { all | instance  
instance_id }
```

**imsimgr instance *instance\_id***

Specifies the IMSI manager instance for which the audit is initiated. The audit is initiated for only one specified instance of IMSI manager at a time.

*instance\_id*: Enter an integer from 1 through 4.

**audit-with sessmgr { all | instance *instance\_id* }**

Initiates an IMSIMgr for either all associated session managers or for a specific session manager (SessMgr) instance.

**all | instance *instance\_id***: Select **all** to initiate the audit for all SessMgr instances or select **instance** and for *instance\_id* enter an integer from 1 to 1152 to identify a specific SessMgr for the audit.

**Usage Guidelines**

Use this command to manage the IMSIMgr's IMSI table, and to initiate an audit of one or more SessMgrs associated with the specific IMSIMgr. This is useful when the MME has been configured to support more than one MME IMSIMgr. The audit assists you to ensure that the IMSI table has the correct IMSI-SessMgr association. triggers as the audit checks for IMSI, IMEI, MSISDN information for a specific SessMgr instance.

**Example**

Use a command similar to the following to trigger an audit of SessMgr 243 associated with IMSIMgr 2:

```
mme imsimgr instance 2 audit-with sessmgr instance 243
```

## mme offload

Initiates or stops the offload of UEs associated with a specified MME service.

---

### Product

MME

---

### Privilege

Security Administrator, Administrator

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

The following command syntax is available in Release 12.2 and earlier.

```
mme offload mme-service mme_svc_name { start mme-init-release-timeout seconds
paging-init-timeout seconds | stop }
```

The following command syntax is available in Release 14.0 and higher.

```
mme offload mme-service mme_svc_name { time-duration minutes offload-percentage
percent [ disable-implicit-detach | preserve-volte-subscribers ] ] | stop
} [- noconfirm ]
```

#### **mme-service** *name*

Specifies the name of an existing MME service from which UEs will be offloaded as an alphanumeric string of 1 through 63 characters.

#### **start mme-init-release-timeout** *seconds* **paging-init-timeout** *seconds*

These keywords are available in Release 12.2 and earlier.

Sets the timeout for the initial release procedure and the paging procedure.

**start mme-init-release-timeout** *seconds*: Configures the timeout (in seconds) for triggering the IDLE MODE ENTRY procedure for UEs that are in the ECM\_CONNECTED state as an integer from 1 to 120. The cause of the IDLE MODE ENTRY will be "Load balancing TAU required".

**paging-init-timeout** *seconds*: Configures the timeout (in seconds) for triggering the PAGING procedure for UEs in the ECM\_IDLE state as an integer from 1 to 120. After returning the UEs to the ECM\_CONNECTED state, the IDLE MODE ENTRY procedure is triggered with the "Load balancing TAU required" cause.

#### **time-duration** *minutes* **offload-percentage** *percent*

**time-duration** specifies the maximum allowed time for the UE offload procedure to complete.

*minutes* can be any value 1 through 1000 minutes.

**offload-percentage** specifies the percentage of total subscribers on this mme-service to offload.

*percent* can be any value 0 through 100.

**disable-implicit-detach**

By default, if the UE context is not transferred to another MME within 5 minutes, the UE will be implicitly detached. This option disables this implicit detach timer.

**stop**

Ends the offload process.

**-noconfirm**

Executes the command without any additional prompts or confirmation from the user.

**preserve-volte-subscribers**

This keyword is used to configure preservation of VoLTE subscribers from offloading during active calls (QCI=1). By default, the subscribers with voice bearer with QCI = 1 will not be preserved during MME offloading. Configuring the keyword **preserve-volte-subscribers** enables preservation of subscribers with voice bearer.

**Usage Guidelines**

Use this command to initiate or stop the offloading of UEs associated with a specified MME service.

Prior to initiating this command, you can set the **relative-capacity** command in the MME Service Configuration Mode to zero (0). This prevents this MME from accepting any new calls, and redirects them to other MMEs in the pool while existing UEs on this MME are removed.

**Important**

Emergency attached UEs in Connected or Idle mode are not considered for offloading.

**Example**

This example applies to Release 12.2 and earlier.

The following command sets the trigger to start off-loading UEs from a service named *mme3* at 60 seconds and the paging trigger at 90 seconds:

```
mme offload mme-service mme3 start mme-init-release-timeout 60
paging-init-timeout 90
```

**Example**

This example applies to Release 14.0 and higher.

The following example command rebalances (offloads) 30 percent of all UEs from the specified *mme-service* (to other *mme-services* in the MME pool) over the course of 10 minutes.

```
mme offload mme-service mme_svc time-duration 10 offload-percentage 30
-noconfirm
```

**Example**

The following example command re-balances(offloads) 30 percent of Non-VoLTE subscribers from the specified mme-service (to other mme-services in the MME pool) over the course of 30 minutes with VoLTE preservation.

```
mme offload mme-service mmesvc time-duration 30 offload-percentage 30
preserve-volte-subscribers
```

## mme paging cache clear

Enables the operator to clear the paging cache for either a specific SessMgr instance or for all SessMgrs.

**Product**

MME.

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
mme paging cache clear { all | instance sessmgr_instance }
```

**all**

Instructs the MME to clear the paging cache for all Session Managers.

**instance sessmgr\_instance**

Enter an integer from 0 to 4294967295 to specify a single Session Manager.

**Usage Guidelines**

This command clears the cache. It is important to clear the cache after the **mme paging cache size** is set to zero (0) to stop caching. This clear command needs to be used to reset the cache after caching is stopped.

**Example**

Use the following command to clear the paging cache for all SessMgrs:

```
mme paging cache clear all
```

## mme relocate-ue imsi

This command enables the operator to detach a UE from the current MME and cause it to reattach to another MME in the pool.

**Product**

MME



<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<p><b>mme relocate-ue</b> <b>imsi</b> <i>imsi</i> <b>new-guti</b> <b>mme-group-id</b> <i>grp_id</i> <b>mme-code</b> <i>mme_code</i> <b>m-tmsi</b> <i>mtmsi</i></p> <p><b>imsi</b> <i>imsi</i></p> <p>Specifies the Mobile Station Identifier of the UE to be relocated. This UE must be registered or connected to this MME.</p> <p><b>new-guti mme-group-id</b> <i>group_id</i></p> <p>The group to which the target MME belongs.</p> <p><i>grp_id</i> :</p> <ul style="list-style-type: none"> <li>Beginning with Releases 16.5, 17.4, and 18.2 and forward, the valid range for mme group id is an integer from 0 through 65536.</li> <li>Previous releases, the valid range for mme group id is an integer from 32768 through 65536.</li> </ul> <p><b>mme-code</b> <i>mme_code</i></p> <p>The target MME to which this UE should be attached.</p> <p><i>mme_code</i> : The unique identifier for the target MME; must be an integer from 0 through 255.</p> <p><b>m-tmsi</b> <i>mtmsi</i></p> <p>The new GUTI MME-TMSI for this UE.</p> <p><i>mtmsi</i> : An integer from 0 through 4294967295.</p>
<b>Usage Guidelines</b>	MME uses this configuration to relocate UEs to a different MME using IMSI, mme-group-id, mme-code and m-tmsi.

## mme reset

Sends an S1 RESET message to a designated eNodeB to reset all UE-associated S1 connections.

<b>Product</b>	MME
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>

**Syntax Description** `mme reset s1-peer peer_ID`

**s1-peer *peer-ID***

Specifies an existing eNodeB peer ID to which the REST message is to be sent as an integer from 1 through 4294967295.

**Usage Guidelines** Use this command to send an S1 RESET message to a designated eNodeB to reset all UE-associated S1 connections.

The S1 peer ID for an eNodeB can be identified by executing the **show mme-service enodeb-association** command available in this mode. The peer ID is presented in the "Peerid" field.

**Example**

The following command initiates the sending of an S1-peer reset message to an eNodeB with a peer ID of 22315734:

```
mme reset s1-peer 22315734
```

## monitor interface

Enables monitoring of traffic on a particular interface.

**Product** All

**Privilege** Security Administrator, Administrator, Operator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `monitor interface if_name`

***if\_name***

Specifies the name of the interface to be monitored as an alphanumeric string of 1 through 79 characters.

**Usage Guidelines** Use this command to monitor the traffic on a specified interface.

**Example**

This command monitors the traffic on the interface named *if1001*:

```
monitor interface if1001
```

# monitor protocol

Enters the system's protocol monitoring utility.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator, Operator

<b>Command Modes</b>	Exec
----------------------	------

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

<b>Syntax Description</b>	<b>monitor protocol</b>
---------------------------	-------------------------

<b>Usage Guidelines</b>	Useful for troubleshooting, this command provides a tool for monitoring protocol transactions between the system and other network nodes including the mobile station(s).
-------------------------	---

The following protocols can be monitored:

- SNMP
- RADIUS Authentication
- RADIUS Accounting
- A11 (R-P Interface) (PDSN only)
- Mobile IPv4
- A11MGR
- PPP
- A10
- User L3 (User Layer 3 protocols)
- USERTCP STACK
- L2TP
- L2TPMGR
- L2TP Data
- GTPC
- GTPCMGR
- GTPU
- GTPP



---

**important** If the hard disk drive (HDD) is used for CDR storage, the CDR option must be used and not the GTPP option (27).

---

- DHCP (GGSN only)
- CDR
- DHCPV6
- RADIUS COA
- MIP Tunnel
- L3 Tunnel (Layer 3 Tunnel Protocols)
- CSS Data
- CSS Signaling



---

**important** In StarOS 9.0 and later releases the CSS Data Signaling option is not supported.

---

- EC Diameter (Diameter Enhanced Charging)
- SIP (IMS)
- IPSec IKE Inter-Node
- IPSec IKE Subscriber
- IPSG RADIUS Signal
- ROHC (Robust Header Compression)
- WiMAX R6
- WiMAX Data
- SRP
- BCMCS SERV AUTH
- RSVP
- Mobile IPv6
- ASNGWMGR
- STUN
- SCTP: Enabling this option will display the SCTP protocol message packets on HNB-GW node.



---

**Important** In Release 20 and later, HNBDGW is not supported. For more information, contact your Cisco account representative.

---

- M3UA
- SCCP
- TCAP
- MAP
- RANAP
- GMM
- GPRS-NS
- BSSGP
- CAP
- SSCOP
- SSCFNFI
- MTP3
- LLC
- SNDCCP
- BSSAP+
- SMS
- PHS-Control (Payload Header Compression)
- PHS-Data
- DNS Client
- MTP2
- HNBAP: Enabling this option will display the HNB Application Part (HNBAP) protocol packets.



---

**Important** In Release 20 and later, HNBDGW is not supported. For more information, contact your Cisco account representative.

---

- RUA: Enabling this option will display the RANAP User Adaptation (RUA) protocol packets.
- EGTPC
- App Specific Diameter: Enabling this option will display the following sub-options —
  - 1 - DIABASE (OFF )

- 2 - DIAMETER Gy (OFF )
- 3 - DIAMETER Gx/Ty/Gxx (OFF )
- 4 - DIAMETER Gq/Rx/Tx (OFF )
- 5 - DIAMETER Cx (OFF )
- 6 - DIAMETER Sh (OFF )
- 7 - DIAMETER Rf (OFF )
- 8 - DIAMETER EAP/STa/S6a/S6d/S6b/S13/SWm (OFF )
- 9 - DIAMETER HDD (OFF )

- PHS-EAPOL
- ICAP
- Micro-Tunnel
- ALCAP: Enabling this option will display the Access Link Control Application Part (ALCAP) protocol message packets on HNB-GW node.




---

**important** In Release 20 and later, HNBNW is not supported. For more information, contact your Cisco account representative.

---

- SSL
- S1-AP
- NAS
- LDAP
- SGS
- AAL2: Enabling this option will display the ATM Adaptation Layer 2 (AAL2) protocol message packets on HNB-GW node.




---

**important** In Release 20 and later, HNBNW is not supported. For more information, contact your Cisco account representative.

---

- PHS (Payload Header Suppression)
- PPPOE
- RTP (IMS)
- RTCP (IMS)
- LMI
- NPDB (IMS)

- SABP (Femto-UMTS)
- OCSP (X.509)

Once the protocol has been selected by entering its associated number, the utility monitors and displays every relative protocol message transaction.

Protocol monitoring is performed on a context-by-context-basis. Therefore, the messages displayed are only those that are transmitted/received within the system context from which the utility was executed.

For additional information on using the monitor utility, refer to the *System Administration Guide*.



**Caution** Protocol monitoring can be intrusive to subscriber sessions and could impact system performance. Therefore, it should only be used as a troubleshooting tool.

### Example

The following command opens the protocol monitoring utility for SIP (IMS) = 37:

```
monitor protocol 37
```

## monitor subscriber

Enables the system's subscriber monitoring utility. Available keywords vary based on the licenses installed on the system.

**Product** All

**Privilege** Security Administrator, Administrator, Operator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
monitor subscriber [ asn-peer-address bs_peer_address | callid call_id
fng-peer-address ipv4_address | global-enb-id global-enb-id | imei imei_value
| imsi imsi_value | ipaddr ip_address | ipv6addr ipv6_address | ipsg-peer-address
ipsg_peer_address | msid ms_id | msisdn msisdn | next-call | pcf pcf_address |
pdif-peer-address pdif_peer_address | peer-fa peer_fa_address | peer-lac
lac_peer_address | sgsn-address sgsn_address | type { lxrft | asngw | asnpc |
closedrp | evdorev0 | evdoreva | interrogating-cscf | ggsn [ Next-Call By
APN ] | ha | ipsg | lns | mme | pdif | proxy-cscf | rfc3261-proxy |
serving-cscf } next-call | type bcmcs { next-call | next-service-request
} | username user_name | Next-Call By APN ]
```

**asn-peer-address** *bs\_peer\_address*

Specifies the peer ASN Base Station IP address in IPv4 address in dotted-decimal notation.

**callid *call\_id***

Specifies the call identification number assigned to the subscriber session by the system to be monitored as a 4-byte hexadecimal number.

**fng-peer-address *ipv4\_address***

Specifies the specific FNG WLAN IP address in IPv4 dotted-decimal notation.

**global-enb-id *global-enb-id***

Specifies the Global eNodeB ID. This must be followed by MCC-MNC-eNBType-eNBID.

MCC consists of 3 digits.

MNC consists of 2 or 3 digits.

eNBType is 0 for Macro and 1 for Home.

eNBID has max 1048575 for MACRO eNB and max 268435456 for Home eNB.

**imei *imei\_value***

International Mobile Equipment Identification (IMEI). Must be followed by 8 digits of TAC (Type Allocation Code) and 6 digits of SNR (Serial Number). Only the first 14 digit of IMEI/IMEISV is used to find the equipment ID.

**imsi *imsi\_value***

Specifies the International Mobile Subscriber Identity (IMSI) of the subscriber session to be monitored an integer from 1 though 15 characters.

**ipaddr *ip\_address***

Specifies the IP address of the subscriber session to be monitored in IPv4 dotted-decimal notation.

**ipv6addr *ipv6\_address***

Specifies the IPv6 address of the subscriber session to be monitored in IPv6 colon-separated-hexadecimal notation.

**ipsg-peer-address *ipsg\_peer\_address***

Specifies the peer IPSG IP address. Must be followed by an IPv4 address in dotted -decimal notation.

**msid *ms\_id***

Specifies the mobile subscriber identification number to be monitored as 7 to 16 digits of an IMSI, MIN, or RMI.

**msisdn *msisdn***

Specifies the Mobile Subscriber ISDN number to be monitored as 7 to 16 digits of an IMSI, MIN, or RMI.



**next-call**

Specifies that the system will monitor the next incoming subscriber session.

Entering this keyword will display the available options of protocols to select. For a list of supported protocols with this keyword, refer to the **monitor protocol** command.

**pcf pcf\_address**

Specifies the PCF IP address in IPv4 dotted-decimal notation.

**pdif-peer-address pdif\_peer\_address**

Specifies the peer PDIF IP address in IPV4 dotted-decimal notation.

**peer-fa peer\_fa\_address**

Specifies the peer FA IP address in IPv4 dotted-decimal notation.

**peer-lac lac\_peer\_address**

Specifies the peer LAC IP address in IPv4 dotted-decimal notation.

**sgsn-address sgsn\_address**

Specifies the SGSN IP address in IPv4 dotted-decimal notation.

**type { 1xrtt | asngw | asnpc | bcmcs { next-call | next-service-request } closedrp | evdorev0 | evdoreva | | fng | interrogating-cscf | ggsn [ Next-Call By APN ] | ha | ipsg | lns | mme | openrp | pdif | pgw | proxy-cscf | rfc3261-proxy | saegw | serving-cscf } next-call [ apn apn ]**

Allows monitoring for specific subscriber types established in the system when next call occurs.

- **1xrtt**: Displays logs for cdma2000 1xRTT call session subscriber
- **asngw**: Displays logs for ASN-GW call session subscriber
- **asnpc**: Displays logs for ASN PC/LR call session subscriber
- **bcmcs**: Displays logs for Broadcast and Multicast Service
- **closedrp**: Displays logs for cdma2000 Closed-RP call session subscriber
- **evdorev0**: Displays logs for cdma2000 EVDO Rev0 call session subscriber
- **evdoreva**: Displays logs for cdma2000 EVDO RevA call session subscriber
- **fng**: Displays logs for the FNG session subscriber
- **interrogating-cscf**: Displays logs for Interrogating CSCF subscriber
- **ggsn**: Displays logs for UMTS GGSN call session subscriber
- **Next-Call By APN**: Display logs for next call on APN basis, where APN name can be any Gi or Gn APN.
- **ha**: Displays logs for Home Agent call session subscriber
- **ipsg**: Displays logs for IPSP call session subscriber

- **lms**: Displays logs for LMS call session subscriber
- **mme**: Displays logs for MME session subscribers.
- **openrp**: Displays logs for OpenRP subscriber
- **pgw**: Displays logs for P-GW call session subscriber
- **pdif**: Displays logs for PDIF call session subscriber
- **proxy-cscf**: Displays logs for Proxy CSCF subscriber
- **rfc3261-proxy-cscf**: Displays logs for non-ims-proxy (RFC-3261 proxy) subscriber
- **saegw**: Displays logs for SAEGW call session subscriber
- **servicing-cscf**: Displays logs for Serving CSCF subscriber

**username** *user\_name*

Specifies the username of an existing subscriber to be monitored.

---

### Usage Guidelines

The `monitor subscriber` utility provides a useful tool for monitoring information about and the activity of either a single subscriber or all subscribers with active sessions within a given context.



#### Caution

The **monitor subscriber** command is intended for *system debugging only*. This command is complementary to external tracing systems and not meant as a replacement for ongoing external system monitoring.

The following items can be monitored:

- Control events
- Data events
- Event ID information
- Inbound events
- Outbound events
- Protocols (identical to those monitored by command)

Once the criteria has been selected, the utility will monitor and display every relative piece of information on the subscriber(s).

For additional information on using the monitor utility, refer to the *System Administration Guide*.



#### Important

Option Y for performing multi-call traces is only supported for use with the GGSN. This option is available when monitoring is performed using the "Next-Call" option. It allows you monitor up to 11 primary PDP contexts for a single subscriber.

Subscriber monitoring is performed on a context-by-context-basis. Therefore, the information displayed will be only that which is collected within the system context from which the utility was executed.

**Caution**

Subscriber monitoring can be intrusive to subscriber sessions and could impact system performance; therefore, it should only be used as a troubleshooting tool.

**Example**

The following command enables monitoring for user *user1*.

```
monitor subscriber username user1
```

The following command will enable monitoring for the user assigned IP address *10.2.3.4*.

```
monitor subscriber ip-address 10.2.3.4
```

The following enables monitoring for call ID *FE80AA12*.

```
monitor subscriber callid fe80aa12
```

## newcall policy

Configures new call policies for busy-out conditions.

**Product**

ASN-GW

ASN PC/LR

ePDG

GGSN

HA

HNB-GW

IPCF

LNS

MME

PDSN

P-GW

S-GW

SAEGW

SaMOG

SGSN

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
newcall policy { asngw-service | asnpc-service | ePDG-service |
sgsn-service } { all | name service_name } reject

newcall policy { fa-service | lma-service | lns-service | mipv6ha-service
} { all | name service_name } reject
newcall policy ggsn-service { apn name apn_name | all | name service_name }
reject [ release-existing-session ]
newcall policy { ha-service | pdsn-service | pdsnclosedrpservice } {
all | name service_name } { redirect target_ip_address [ weight weight_num ] [
target_ipaddress2 [ weight weight_num ] ... target_ip_address16 [ weight weight_num
] | reject }
newcall policy hnbgw-service { all | name service_name } reject
newcall policy mme-service { all | name service_name } reject
newcall policy { pcc-af-service | pcc-policy-service } { all | name
service_name } reject
newcall policy pgw-service { all | apn name apn_name | name service_name }
reject [ release-existing-session ]
newcall policy saegw-service { all | name service_name } reject [
release-existing-session ]
newcall policy sgw-service { all | name service_name } reject [
release-existing-session ]
newcall policy samog-service { all | name service_name } drop

no newcall policy { asngw-service | asnpc-service | ePDG-Service } { all
| name service_name }
no newcall policy { fa-service | ggsn-service | ha-service | lma-service
| lns-service | mipv6ha-service | pdsn-service | pdsnclosedrpservice }
{ all | name service_name }
no newcall policy ggsn-service { apn apn_name | all | name service_name }
no newcall policy { ha-service | pdsn-service } { all | name service_name
} redirect target_ip_address [ weightweight_num ] [ target_ip_address2 [ weight
weight_num ] ... target_ip_address16 [ weightweight_num ]
no newcall policy hnbgw-service { all | name service_name }
no newcall policy mme-service { all | name service_name }
no newcall policy { pcc-af-service | pcc-policy-service } { all | name
service_name }
no newcall policy pgw-service { all | apn name apn_name | name service_name
}
no newcall policy saegw-service { all | name service_name }
no newcall policy sgw-service { all | name service_name }
no newcall policy samog-service { all | name service_name }
```

**no**

Disables the new call policy for all or specified service of a service type.

**no newcall policy { ha-service | pdsn-service } { all | name *service\_name* } redirect *target\_ip\_address* [ weight *weight\_num* ] [ *target\_ip\_address2* [ weight *weight\_num* ] ... *target\_ip\_address16* [ weight *weight\_num* ]**

Deletes up to 16 IP addresses from the redirect policy. The IP addresses must be expressed in IPv4 dotted-decimal notation

**newcall policy { asngw-service | asnpc-service | epDG-service } { all | name *service\_name* } reject**

Creates a new call policy to reject the calls based on the specified ASN-GW or ASN PC/LR service name or all services of this type.

**asngw-service:** Specifies the type of service as ASN GW for which new call policy is configured.

**asnpc-service:** Specifies the type of service as ASN PC/LR for which new call policy is configured.

**epDG-service:** Specifies the type of service as ePDG for which new call policy is configured.

**name *service\_name*:** Specifies the name of the service for which new call policy is configured. *service\_name* is name of a configured ASN GW or ASN PC/LR service.

**reject:** Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection. For ASN-GW and ASN PC/LR service rejection code is 81H (Registration Denied - administratively prohibited).

**newcall policy { fa-service | lma-service | lns-service | mipv6ha-service } { all | name *service\_name* } reject**

Creates a new call policy that rejects calls based on the specified access point name.

**fa-service | ha-service | lma-service | lns-service | mipv6ha-service | mme-service | pdsn-service | pdsnclosedrp-service**

Specifies the type of service for which to configure a new call policy. The following services are supported:

- **fa-service:** A Foreign Agent service
- **ha-service:** A Home Agent service
- **lma-service:** A Local Mobility Anchor (LMA) service
- **lns-service:** An L2TP Network Server service
- **mipv6ha-service:** A Mobile IPv6 Home Agent service
- **pdsn-service:** A Packet Data Serving Node service
- **pdsnclosedrp-service:** A Closed R-P service

**{ all | name *service\_name* }**

Specifies a filter for the new call policy. Whether the new call policy will be applied to all configured services or a specific one.

- **all:** Specifies that the new call policy will be applied to all instances of the selected service type.
- **name: *service\_name*:** Specifies the name of a specific instance of the selected service type as an alphanumeric string of 1 through 63 characters that is case sensitive.

**redirect** *target\_ip\_address* [ *weight weight\_num* ] [ *target\_ip\_address2* [ *weight weight\_num* ] ... *target\_ip\_address16* [ *weight weight\_num* ]

Configures the busy-out action. When a redirect policy is invoked, the service rejects new sessions and provides the IP address of an alternate destination. This command can be issued multiple times.

*target\_ip\_address#* is the IP address of an alternate destination expressed in IPv4 dotted-decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.

**weight** *weight\_num*: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. *weight\_num* must be an integer from 1 through 10.

Depending on the type of service that the policy is applied to, the following reason codes are reported as part of the reply:

- **ha service:** 88H (Registration Denied - unknown home agent address)
- **pdsn service:** 88H (Registration Denied - unknown PDSN address)




---

**Important**

The redirect option is not supported for use with FA and GGSN services.

---

**reject**

Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the following reason codes are reported as part of the reply to indicate the rejection:

- **asngw service:** 81H (Registration Denied - administratively prohibited)
- **fa service:** 41H (administratively prohibited)




---

**Important**

When **newcall policy** is set to reject for the FA service, the Busy Bit is set in the Agent Advertisement. Any further RRQs will be rejected with this code value.

---

- **ggsn service:** C7H (Rejected - no resources available)
- **ha service:** 81H (Registration Denied - administratively prohibited)
- **mipv6ha-service:** 81H (Registration Denied - administratively prohibited)
- **mme service:** 81H (Registration Denied - administratively prohibited)
- **pdsn service:** 81H (Registration Denied - administratively prohibited)
- **pdsnclosedrp-service:** 81H (Registration Denied - administratively prohibited)

**newcall policy hnbgw-service { all | name *service\_name* } reject****Important**

In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Creates a new call policy to reject the calls in a specified HNB-GW service name instance or all HNB-GW services on the system.

**name** *service\_name*: Specifies the name of the HNB-GW service for which new call policy is configured.

**reject**: Specifies that the policy rejects all new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection. For HNB-GW service rejection code is 81H (Registration Denied - administratively prohibited).

**newcall policy mme-service { all | name *service\_name* } reject**

Creates a new call policy to reject the calls based on the specified MME service name or all MME services on the system.

**name** *service\_name*: Specifies the name of the MME service for which new call policy is configured.

**reject**: Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection. For MME service rejection code is 0x16 (Registration Denied - administratively prohibited).

**newcall policy { pcc-af-service | pcc-policy-service | pcc-quota-service } { all | name *service\_name* } reject**

Creates a new call policy to reject the calls for PCC services on the system for any of the following PCC services:

- **pcc-af-service** **name** *service\_name*: Specifies the Policy and Charging Control-Application Function (PCC-AF) service for which new call policy is to be configured on the system.
 

**name** *service\_name*: Specifies the name of an existing PCC-AF service for which new call policy is configured.
- **pcc-policy-service** **name** *service\_name*: Specifies the Policy and Charging Control-Policy (PCC-Policy) service for which new call policy is to be configure on the system.
 

**name** *service\_name*: Specifies the name of an existing PCC-Policy service for which new call policy is configured.

**reject**: Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection. For PCC services rejection code is 81H (Registration Denied - administratively prohibited).

**newcall policy pgw-service { all | apn name *apn\_name* | name *service\_name* } reject [ release-existing-session ]**

Creates a new call policy to reject the calls based on the specified P-GW service name, APN name, or all P-GW services (and any SAEGW service associated with the P-GW service) in this context .

**all**: Rejects all P-GW services on the system. Specifies that the new call policy will be applied to all instances of the P-GW service, and any associated SAEGW service, in this context.

**apn** *apn\_name*: Specifies the name of the APN, and any associated P-GW/SAEGW service, for which new call policy is configured.

**name** *service\_name*: Specifies the name of the P-GW service, and any SAEGW service associated with this P-GW service, for which new call policy is configured.

**reject**: Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection.

**release-existing-session**: All the pre-existing sessions across all eGTP/GTP services for that IMSI/IMEI will be released gracefully. Without this keyword, the receiving node rejects the CSReq without considering the existing sessions for that IMSI/IMEI, which may lead to junk sessions. Disabled by default.

#### **newcall policy saegw-service { all | name *service\_name* } reject [ release-existing-session ]**

Creates a new call policy to reject the calls based on the specified SAEGW service name or all SAEGW services on the system.

**name** *service\_name*: Specifies the name of the SAEGW service for which new call policy is configured.

**reject**: Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection.



#### **Important**

When **newcall policy saegw-service all reject** CLI command is enabled, the handovers incoming to the S-GW part of an SAEGW, and any other applicable handovers, are not rejected.

**release-existing-session**: All the pre-existing sessions across all eGTP/GTP services for that IMSI/IMEI will be released gracefully. Without this keyword, the receiving node rejects the CSReq without considering the existing sessions for that IMSI/IMEI, which may lead to junk sessions. Disabled by default.

#### **newcall policy sgw-service { all | name *service\_name* } reject [ release-existing-session ]**

Creates a new call policy to reject the calls based on the specified S-GW service name or all S-GW services on the system.

**name** *service\_name*: Specifies the name of the S-GW service for which new call policy is configured.

**reject**: Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection.

**release-existing-session**: All the pre-existing sessions across all eGTP/GTP services for that IMSI/IMEI will be released gracefully. Without this keyword, the receiving node rejects the CSReq without considering the existing sessions for that IMSI/IMEI, which may lead to junk sessions. Disabled by default.

#### **newcall policy samog-service { all | name *service\_name* } drop**

Creates a new call policy to drop calls based on the specified SaMOG service name or all SaMOG services on the system. By default, this configuration is disabled.

**name** *service\_name*: Specifies the name of the SaMOG service for which new call policy is configured. *service\_name* must be an alphanumeric string of 1 through 63 characters.

**drop**: Specifies the policy to drop new incoming calls. When the retries are exhausted, the AP/WLC attempt session creation on alternate SaMOG services connected to the AP/WLC.



**Usage Guidelines**

This command is used to busy-out specific system services prior to planned maintenance or for troubleshooting. This is required when operator find out that the system is somehow overloaded, or needs some kind of maintenances or so.

**Example**

The following command creates a new call policy to re-direct all new calls for all PDSN services to a device having an IP address of *192.168.1.23*:

```
newcall policy pdsn-service all redirect 192.168.1.23
```

The following command creates a new call policy to reject all new calls for a GGSN service called *ggsn1*:

```
newcall policy ggsn-service name ggsn1 reject
```

The following command creates a new call policy to reject all new calls for an MME service called *MME1*:

```
newcall policy mme-service name MME1 reject
```

The following command creates a new call policy to reject all new calls for an HNB-GW service called *hnbgw1*:

```
newcall policy hnbgw-service name hnbgw1 reject
```

The following command creates a new call policy to reject all new calls for a PCC Policy service called *pcrf1*:

```
newcall policy pcc-policy-service name pcrf1 reject
```

The following command creates a new call policy to drop all new calls for the SaMOG service:

```
newcall policy samog-service all drop
```

## password change

Provides a mechanism for local-user administrative users to change their passwords.

<b>Product</b>	All
<b>Privilege</b>	All local-user administrative levels except as noted below
<b>Command Modes</b>	Exec
<b>Syntax Description</b>	<pre><b>password change [ local-user <i>name</i> ]</b></pre>

**local-user *name***

Specifies the name of an existing local-user administrative user for which to change the password as an alphanumeric string of 3 through 144 characters that is case sensitive.

**Important**

This keyword is only available to local-users with an authorization level of security-administrator.

**Usage Guidelines**

This command provides a mechanism for local-user administrative users to change their passwords. In addition, it also provides a mechanism for security-administrator local-users to change the password for other local-user accounts.

If the **local-user** keyword is not entered, the system prompts the user for their current password and for the new password. New passwords take effect at the next login. Users that have had their password changed by a security-administrator are prompted to change their passwords at their next login.

New passwords must meet the criteria dictated by the **local-user password** command options in the Global Configuration Mode.

**Important**

The system does not allow the changing of passwords unless the time limit specified by the **local-user password min-change-interval** has been reached.

**Example**

The following command, executed by a security-administrator, resets the password for a local-user name *operator12*:

```
password change local-user operator12
```

## patch plugin

Copies a patch intended for a specific plugin module onto the system. This function is associated with the patch process for accommodating dynamic software upgrades.

**Product**

ADC

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
patch plugin plugin_name binary_path certificate certificate_path signature
signature_path
```

***plugin\_name***

Specifies the name of an existing plugin that will be copied onto the system as an alphanumeric string of 1 through 16 characters.

**certificate**

Specifies the name of a certificate associated with the plugin that will be copied onto the system as an alphanumeric string of 1 through 16 characters.

**filepath**

Specifies the location of the file to copy. The path must be formatted as follows:

For the ASR 5000:

```
[ file: ]{ /flash | /pcmcia1 | /hd }[ /directory ]/file_name
```

**Important**

Use of the ASR 5000 SMC hard drive is not supported in this release.

For the ASR 5500:

```
[ file: ]{ /flash | /usb1 | /hd }[ /directory ]/file_name
```

For VPC:

```
[ file: ]{ /flash | /hd-raid | /usb1 | usb2 | /cdrom1 }[ /directory ]/file_name
```

**Important**

The USB ports and CDROM must be configured via the hypervisor to be accessible.

**Important**

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

*directory* is the directory name.

*filename* is the actual file of interest.

**binary\_path certificate certificate\_path signature signature\_path**

Validates signature along with P2P binary file for trusted builds. When P2P binary file (along with signature file) gets patched into the system, StarOS verifies the signature and accepts or rejects the P2P binary file. Verification is mandatory in trusted builds and is optional in normal builds.

**Usage Guidelines**

Use this command to verify and copy a patch onto the system. After the patch has been copied onto the system, you must run the **install plugin** command to unpack the kit and validate its contents.

**Example**

To copy the plugin module named *p2p* onto the system enter the following command:

```
patch plugin p2p http://192.168.1.2/tmp/libp2p-1.2.0.tgz certificate
http://192.168.1.2/tmp/1.2.0.cert
```

When the patch has been successfully copied the following message appears:

```
New patch for plugin p2p available for installation
```

# ping

Verifies ability to communicate with a remote node in the network by passing data packets between and measuring the response. This is accomplished by sending IPv4 Internet Control Message Protocol (ICMP) echo request packets to the target node (pinging) and waiting for an ICMP response.

---

**Product** All

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```




---

**Important**

Inspector privileges are granted for all variables except **count**. To initiate a ping count, you must have a minimum privilege level of Operator.

---



---

**Syntax Description**

```
ping ( hostname | ip_address ) [ broadcast ] [ count num_packets ] [ df-bit { off | on } ] [ dscp dscp_value ] [ flood ] [ pattern packet_pattern ] [ size octet_count ] [ src { src_host_name | src_host_ip_address } ] [ vrf vrf_name
```

***hostname***

Sends ICMP echo request packets to the remote node specified the node's name (up to 127 alphanumeric characters) or assigned IPv4 address in dotted-decimal notation.

***ip\_address***

IPv4 address of host to be pinged in dotted-decimal notation.

***broadcast***

Sends ping packets to broadcast addresses.

***count num\_packets***

Specifies the number of packets to send to the remote host for verification as an integer from 1 through 10000. Default: 5

***df-bit { off | on }***

Specifies whether or not the do-not-fragment bit will be included in the IP header.

***dscp dscp\_value***

Specifies the 6-bit DSCP value as an integer from 0 through 63. Default: 0. The DSCP value must be previously mapped to an internal-class-of-service value using the Global Configuration mode **qos ip-dscp-iphb-mapping** command.

**flood**

Sends ping packets as rapidly as possible or 100 per second, whichever is faster.

**Important**

Use with caution. Flood ping terminates after receiving (count) responses. If flood ping is used against an interface that is not responding, it will run indefinitely

**pattern *packet\_pattern***

Specifies a pattern to use to fill the internet control message protocol packets in hexadecimal format with a value in the range of 0x0000 through 0xFFFF. By default each octet of the packet is encoded with the octet number of the packet.

**size *octet\_count***

Specifies the number of bytes in each IP datagram as an integer from 40 through 18432. Default: 56

**src *host\_ip\_address***

Specifies the source IP address in IPv4 dotted-decimal notation. Default: originating system's IP address

**vrf *vrf\_name***

Specifies the VRF name for which routing information will be displayed. *vrf\_name* is an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

This command is useful in verifying network routing and if a remote node is able to respond at the IPv4 layer.

**Example**

The following command is the most basic and will report the results of trying to communication with remote node *remoteABC*.

```
ping remoteABC
```

The following command verifies communication with the remote node *10.2.3.4* using *1000* packets.

```
ping 10.2.3.4 count 1000
```

The following command verifies communication with remote node *remoteABC* while making it appears as though the source is remote node with IP address *10.2.3.4*.

```
ping remoteABC src 10.2.3.4
```

**Important**

The responses from the remote host to the ping packets will be rerouted to the host specified as the source.

# ping6

Verifies ability to communicate with a remote node in the network by passing data packets between and measuring the response. This is accomplished by sending IPv6 Internet Control Message Protocol (ICMP) echo request packets to the target node (pinging) and waiting for an ICMP response.

---

**Product** All

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **ping6** { *hostname* | *ipv6\_address* } [ **count** *num* ] [ **dscp** *dscp\_value* ] [ **flood** ] [ **interface** *interface\_name* ] [ **pattern** *val* ] [ **size** *val* ] [ **src** *ip\_address* ] [ **vrf** *vrf\_name* ]

## **host\_name**

Name of the host to be pinged.

## **ipv6\_address**

IPv6 address of host to be pinged in colon-separated-hexadecimal notation.

## **countnum**

Sets the number of ping packets to be sent as an integer from 1 through 10000.

## **dscp dscp\_value**

Specifies the 6-bit DSCP value as an integer from 0 through 63. Default: 0. The DSCP value must be previously mapped to an internal-class-of-service value using the Global Configuration mode **qos ip-dscp-iphb-mapping** command.

## **flood**

Configures ping6 to send packets as quickly as possible, or 100 per second, whichever is faster.




---

### Important

Use with caution. Flood ping terminates after receiving (count) responses. If flood ping is used against an interface that is not responding, it will run indefinitely

---

## **interface interface\_name**

Defines a named source interface from which ping packets will originate. *interface\_name* is an alphanumeric string of 1 to 79 characters.

**pattern val**

Specifies the hexadecimal pattern to fill ICMP packets as a hexadecimal number from 0x0 through 0ffff

**size val**

Specifies the size of ICMP datagram (in bytes) as an integer from 40 through 18432. Default: 56.

**src ip\_address**

Specifies the source IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. Default: originating system's IP address

**vrf name**

Specifies the name of an existing VFR as an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

This command is useful in verifying network routing and if a remote node is able to respond at the IPv6 layer.

**Example**

Use this command to ping the IPv6 address `2001:0db8:85a3:0000:0000:8a2e:0370:7334`

```
ping6 2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

## port disable, port enable

Disables or enables a port on a specified MIO/UMIO card without affecting the paired port on the other MIO/UMIO card. This capability is very useful in Active-Active LAG configurations on an ASR 5500.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
port { disable | enable } ethernet slot#/port#
```

**disable**

Disables (shuts down) the specified MIO/UMIO port without disabling its paired port on the other MIO/UMIO card.

**enable**

Enables a previously disabled port on the specified MIO/UMIO port without affecting its paired port on the other MIO/UMIO card.

**ethernet**

Specifies the port type as Ethernet.

**slot#**

Identifies the physical chassis slot (5 or 6) where the MIO/UMIO card is installed.

**port#**

Identifies the physical port on the MIO/UMIO card to disable or enable.

**Usage Guidelines**

If you use the Ethernet Port Configuration mode **shutdown** command to shut down one of the ports on an MIO/UMIO card in an Active-Active LAG configuration, by default the paired port on the other MIO/UMIO card will also be shut down.

Use this command to disable (shut down) a port on an MIO/UMIO card without affecting the paired port on the other MIO/UMIO card in an Active-Active LAG configuration.

**Example**

The following command disables port 11 on the MIO card in slot 6.

```
port disable ethernet 6/11
```

## port switch to

Performs a manual switchover to an available redundant/standby line card, SPIO port or MIO port.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
port switch to slot#/port#
```

**slot#**

Identifies the physical chassis slot where the line card, SPIO or MIO is installed.

**port#**

Identifies the physical port on the line card, SPIO or MIO to automatically switch to.

**Usage Guidelines**

This command is used to specify the redundant port on a Line Card (LC) or MIO. When port redundancy is enabled, if an external network device or cable failure occurs that causes a link down failure on the port, then the redundant port is used.





**Important** This command is not supported on all platforms.

### Example

On an ASR 5000 this command switched to port 17/1.

```
port switch to 17/1
```

On an ASR 5500 this command switches to port 6/11.

```
port switch to 6/11
```

## ppp echo-test

Sends link control protocol (LCP) keep-alive echo packet to the peer point-to-point protocol (PPP) connection to verify proper communication between PPP connections, and awaits a response.

### Product

PDSN  
GGSN

### Privilege

Security Administrator, Administrator, Operator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
ppp echo-test { callid call_id | imsi imsi_id | ipaddr ip_address | msid ms_id | username user_name } [ num_packets ] [ | { grep grep_options | more } ]
```

#### **callid** *call\_id*

Specifies the call instance ID for which the PPP link must be verified as a 4-byte hexadecimal number.

#### **imsi** *imsi\_id*

Specifies the International Mobile Subscriber Identifier (IMSI) for which the PPP link must be verified.

#### **ipaddr** *ip\_address*

Specifies the IP address for which the PPP link must be verified in IPv4 dotted-decimal notation.

#### **msid** *ms\_id*

Specifies the mobile subscriber ID for which the PPP link must be verified as 7 to 16 digits of an MIN, or RMI.

**username *user\_name***

Specifies an existing user for which the PPP link must be verified as an alphanumeric string of 1 through 127 characters.

**num\_packets**

Specifies the number of test packets to generate an integer from 1 through 1000000. Default: 1

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in *Command Line Interface Reference*.

**Usage Guidelines**

Use this command to verify the point-to-point protocol communications. This command sends LCP keep-alive echo packet to the peer PPP connection to verify proper communication between PPP connections. **ppp echo-test** command waits for LCP echo response for configured numbers of tries, if response is not received it will retry configured no of times with an interval of 5 seconds. This command accepts the parameters call ID, IMSI, IP address, MSID, and user name to specify which active PPP session to consider.

**ppp echo-test** command makes the dormant session active.

**Caution**

Issuing this command could negatively impact system performance depending on the number of subscribers using the same name and/or if the number of packets used in the test is large.

LCP includes Echo-Request and Echo-Reply codes in order to provide a Data Link Layer loopback mechanism for use in exercising both directions of the link. This is useful as an aid in debugging, link quality determination, performance testing, and for numerous other functions. Upon reception of an Echo-Request in the LCP Opened state, an Echo-Reply is transmitted.

**Example**

The following command tests the PPP link to user *user1*.

```
ppp echo-test username user1
```

The following command tests the PPP link to the user assigned IP address *10.2.3.4*.

```
ppp echo-test ipaddr 10.2.3.4
```

The following tests the PPP link associated with call ID *fe80AA12*.

```
ppp echo-test callid fe80aa12
```

## push ssh-key

Pushes the secure shell (SSH) client public key to a remote server. The key must have been previously generated via the CLI commands in the SSH Client Configuration mode.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [context_name]host_name#
<b>Syntax Description</b>	<pre>push ssh-key { host_name   host_ip_address } user username [ context context_name ]</pre> <p><b>host_name</b> Specifies the remote server using its logical host name which must be resolved via DNS lookup. It is expressed as an alphanumeric string of 1 to 127 characters.</p> <p><b>host_ip_address</b> Specifies the host IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.</p> <p><b>user username</b> Specifies a valid username on the external server as an alphanumeric string of 1 to 79 characters.</p> <p><b>context context_name</b> Specifies a valid StarOS context name. The context name is optional. If it is not provided the current context is used for processing.</p>
<b>Usage Guidelines</b>	Use this command to push a public key to an external server. The SSH public key enables SSH access without a password between a StarOS gateway and the external server via the Exec mode <b>ssh</b> command. You must first create the SSH client key pair using CLI commands in the SSH Client Configuration mode.

**Example**

The following command pushes an SSH client public key to an external server named *remoteABC*.

```
push ssh-key remoteABC user admin012 context mme
```

## radius interim accounting now

Check points current RADIUS Interim accounting messages immediately.

<b>Product</b>	PDSN GGSN ASN-GW
<b>Privilege</b>	Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
radius interim accounting now
```

**Usage Guidelines**

This command check points RADIUS Interim accounting as they are received. It is useful when preparing for system monitoring or troubleshooting.

**Example**

The following command initiates immediate checkpointing of RADIUS Interim accounting messages:

```
radius interim accounting now
```

## radius test

Verifies the RADIUS servers functions for accounting and authentication.

**Product**

PDSN

GGSN

ASN-GW

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
radius test { accounting | admin authentication | authentication | probe
  authentication server ip_addr port port_no [ username username password password
  ] } { all | [ on ] | off } | radius group group_name user_name | server
  server_name port server_port } user_name password
```

**accounting**

Tests accounting server functionality.

**admin authentication name\_admin admin\_password**

Tests the RADIUS admin authentication.

*name\_admin*: Specifies the name of the administrator as an alphanumeric string of 1 through 127 characters.

*admin\_password*: Specifies the password for the administrator as an alphanumeric string of 1 through 63 characters.

**authentication**

Tests authentication server functionality.

**all** | **radius group** *group\_name* *user\_name* | **server** *server\_name* **port** *server\_port*

**all**: Tests all configured servers.

**server** *server\_name* **port** *server\_port*: Tests only the server specified by *server\_name* and *server\_port*. The server must have been previously configured.

**radius group** *group\_name* *user\_name*: Tests all configured authentication servers in a specific RADIUS group for a specific user. Must be followed by the RADIUS group name and user name.

*group\_name* is an alphanumeric string of 1 through 63 characters that specifies the name of server group configured in the specific context for authentication/accounting.

**on/off**

Allows the user to turn RADIUS test accounting on or off.

**user\_name**

Specifies the RADIUS user who is to be verified. The user must have been previously configured.

**password**

Specifies the RADIUS user who is to have authentication verified. *password* is only applicable when the **authentication** keyword is specified.

**Usage Guidelines**

Test the RADIUS accounting for troubleshooting the system for specific users or to verify all the system RADIUS accounting functions.

**Example**

The following verifies all RADIUS servers.

```
radius test accounting all
```

```
radius test authentication all
```

The following verifies the RADIUS accounting and authentication for user **radius test authentication all***user1* for the *sampleServer*.

```
radius test accounting server sampleServer port 5000 user1
```

```
radius test authentication server sampleServer port 5000 user1 dummyPwd
```

The following commands will verify the RADIUS accounting and authentication for RADIUS server group *star1* for the current context:

```
radius test accounting server sampleServer port 5000 user1
```

```
radius test authentication server sampleServer port 5000 user1 dummyPwd
```

```
radius test authentication all
```

The following verifies the RADIUS authentication server group *star1* for user *user1*.

```
radius test authentication radius group star1 user1
```

# reload

Invokes a full system reboot. All processes are terminated and the system initiates a hardware reset (reboot). This command is identical to the **shutdown** command.

---

**Product** All

---

**Privilege** Security Administrator, Administrator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **reload** [ **ignore-locks** ] [ **-noconfirm** ]

## ignore-locks

Reboots the system regardless of any save configuration operations that may be currently running. StarOS displays a warning message but does not wait for save configuration requests to complete before initiating the reboot.

Warning: One or more other administrators are saving configuration



**Caution** Use of the **ignore-locks** keyword may result in file corruption.

---

## -noconfirm

Executes the command without any additional prompts or confirmation from the user.

---

## Usage Guidelines

The system performs a hardware reset and reloads the highest priority boot image and configuration file specified in the boot.sys file. Refer to the **boot system priority** command in the Global Configuration Mode for additional information on configuring boot images, configuration files and priorities.

By default (without the **ignore-locks** option specified) **reload** waits for save configuration operations to complete before initiating the reboot.



**Important** To avoid the abrupt termination of subscriber sessions, it is recommended that a new call policy be configured and executed prior to invoking the **reload** command. This policy sets busy-out conditions for the system and allows active sessions to terminate gracefully. Refer to the **newcall** command in the Exec Mode for additional information.

---



**Caution** Issuing this command causes the system to become unavailable for session processing until the reboot process is complete.

---

**Example**

The following command performs a hardware reset on the system:

```
reload
```

# rename

Changes the name of an existing local file.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
rename from_filepath to_filepath [ -noconfirm ]
```

***from\_filepath***

Specifies the path to the file/directory to be renamed. The path must be formatted according to the following format:

For the ASR 5000:

```
[ file: ]{ /flash | /pcmcial | /hd-raid }[ /directory ]/file_name
```

For the ASR 5500:

```
[ file: ]{ /flash | /usb1 | /hd-raid }[ /directory ]/file_name
```

**Important**

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

**Important**

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

*directory* is the directory name

*filename* is the actual file of interest

***to\_filepath***

Specifies the path to the file/directory to be renamed. The path must be formatted according to the following format:

For the ASR 5000:

```
[ file: ] { /flash | /pcmcial | /hd } [ /directory ] /file_name
```




---

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

---

For the ASR 5500:

```
[ file: ] { /flash | /usb1 | /hd } [ /directory ] /file_name
```

*directory* is the directory name

*filename* is the actual file of interest

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.




---

**Caution** Extreme caution should be taken when using the **-noconfirm** option. The paths to the source and the destination should be verified prior to performing the command.

---



---

**Usage Guidelines** Rename files as part of regular system maintenance in conjunction with the delete command.

**Example**

The following renames the directory */pub* in the local PCMCIA1 device.

```
rename /pcmcial/pub /pcmcial/pub_old
```

The following renames the directory */pub* in the local USB device.

```
rename /usb1/pub /usb1/pub_old
```

## reset active-charging

This command resets the active charging services.

---

**Product** All

---

**Privilege** Security Administrator, Administrator, Operator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `reset active-charging credit-control misc-info max-backpressure { all | facility sessmgr instance instance_number }`



**all**

Displays the maximum backpressure information among all the active session manager instances.

**facility sessmgr instance *instance\_number***

Specifies the facility session manager instance as an integer ranging from 1 through 65535 characters.

**Usage Guidelines**

Use this CLI command to get or reset the maximum back-pressure hit and the timestamp it reached the maximum value. This helps to reset the gauge value for all/specific session manager instance to zero.

**Example**

The following command resets the maximum backpressure value for all active session manager instances:

```
reset active-charging credit-control misc-info max-backpressure all
```

## reset alcap-service

Resets a named Access Link Control Application Part (ALCAP) protocol service. ALCAP is the protocol used for the control plane of the UMTS transport layer. It manages and multiplexes users into ATM AAL2 virtual connections.

**Product**

All (ASR 5000 only)

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
reset alcap-service svrc_name aal2 node node_name aal2-path { path_name | all }
```

***svrc\_name***

Specifies the name of an existing ALCAP service as an alphanumeric string of 1 through 63 characters.

**aal2 node *node\_name***

Specifies the name of an existing ATM Adaptation Layer 2 (AAL2) node as an alphanumeric string of 1 through 64 characters.

**Usage Guidelines**

Reset a named ALCAP service for a specified AAL2 node.

**Example**

The following command resets the ALCAP service *alcap\_01* for the AAL2 node *aal2\_1001*, all paths:

```
reset alcap-service alcap_01 aal2-node aal2_1001 aal2-path all
```

## reset diameter

This command clears the Diameter statistics.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<b>reset diameter aaa-statistics misc-data</b>
<b>Usage Guidelines</b>	Resets the Diameter statistics (highest backpressure statistics).

### Example

The following command resets the Diameter related miscellaneous statistics:

```
reset diameter aaa-statistics misc-data
```

## reset ims-authorization

Resets the maximum backpressure related information associated with the IMS authorization services.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<b>reset ims-authorization policy-control misc-info max-backpressure { all   facility sessmgr instance <i>instance_number</i> }</b>  <b>all</b> Displays the maximum backpressure information among all the active session manager instances.  <b>facility sessmgr instance <i>instance_number</i></b> Specifies the facility session manager instance as a integer from 0 through 10000000 characters.

**Usage Guidelines**

Use this command to reset the values of maximum backpressure related information.

**Example**

The following command resets all the backpressure related information:

```
reset ims-authorization policy-control misc-info max-backpressure all
```

## reveal disabled commands

Enables or disables the input of commands for features that do not have license keys installed. The output of the command **show cli** indicates when this feature is enabled. This command effects the current CLI session only and is disabled by default.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
[ no ] reveal disabled commands
```

**no**

Does not show disabled commands.

**Important**

This command is not available in release 20.0 and higher Trusted builds.

**Usage Guidelines**

When this command is enabled and a disabled command is entered, a message is displayed that informs you that the required feature is not enabled and also lists the name of the feature that you need to support the command.

When this command is disabled and a disabled command is entered, the CLI does not acknowledge the existence of the command and displays a message that the keyword is unrecognized.

**Example**

The following command sets the CLI to accept disabled commands and display the required feature for the current CLI session with the following command:

```
reveal disabled commands
```

The following command sets the CLI to reject disabled commands and return an error message for the current CLI session:

```
no reveal disabled commands
```

# rlogin

Attempts to connect to a remote host.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator, Operator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

**rlogin** { *host\_name* | *host\_ip\_address* } [ **user** *user\_name* ]

***host\_name* | *host\_ip\_address***

Identifies the remote node with which to attempt connection.

*host\_name*: Specifies the remote node using the node's logical host name which must be resolved via DNS lookup.

*host\_ip\_address*: Specifies the remote node using its assigned IP address in IPv4 dotted-decimal notation.

**user *user\_name***

Specifies a user name attempting connection as an alphanumeric string of 1 through 1023 characters.

---

**Usage Guidelines**

Connect to remote network elements using rlogin.


**Important**

**rlogin** is not a secure method of connecting to a remote host. **ssh** should be used whenever possible for security reasons.


**Important**

The **rlogin** command is not available in Release 20.0 and higher Trusted builds.

---

**Example**

The following connects to remote host *remoteABC* as user *user1*.

```
rlogin remoteABC user user1
```

The following connects to remote host *10.2.3.4* without any default user.

```
rlogin 10.2.3.4
```

# rmdir

Removes (deletes) a local directory.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
rmdir path [ force ]
```

***path***

Specifies the directory path to remove. The must be formatted according as follows:

For the ASR 5000:

```
[ file: ]{ /flash | /pcmcia1 | /hd-raid }[ /directory ]/file_name
```

For the ASR 5500:

```
[ file: ]{ /flash | /usb1 | /hd-raid }[ /directory ]/file_name
```

For VPC:

```
[ file: ]{ /flash | /hd-raid | /usb1 | /usb2 | /cdrom1 }[ /directory ]/file_name
```




---

**Important**

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

*directory* is the directory name

*filename* is the actual file of interest

**force**

Over-rides any warnings to force deletion of the directory and any files contained therein.




---

**Important**

Use of the **force** keyword should be done with care to ensure the directory is specified accurately as there is no method to recover a directory which has been removed.

---

**Usage Guidelines**

Remove old directories as part of regular maintenance.

**Example**

The following removes the local directory `/pcmcia1/pub`.

```
rmdir /pcmcia1/pub
```

## rollback module

Loads a specified software plugin module from the Version Priority List (VPL) with the next higher priority number. This function is associated with the patch process for accommodating dynamic software upgrades.

<b>Product</b>	ADC
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec
<b>Syntax Description</b>	<b>rollback module</b> <i>plugin_name</i>

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

***plugin\_name***

Specifies the name of an existing plugin module that you want to downgrade as an alphanumeric string of 1 through 16 characters. If the named module is not known to the system, an error message is displayed.

**Usage Guidelines**

Use this command to initiate a rollback of a previously loaded software plugin module. If it fails to load, the module with next highest priority will be loaded. If none of the modules are installed, the default patch which comes along with the ASR 5000 build is automatically loaded. The specified module must have been previously unpacked/verified and configured via the **install plugin** and **plugin** commands respectively.

For additional information, refer to the *Plugin Configuration Mode Commands* chapter.

**Example**

To load the next plugin module named `p2p` enter the following command:

```
rollback module p2p
```

## rotate-hd-file

Rotates the Diameter files stored on the hard disk drive.

<b>Product</b>	HSGW
	P-GW
	SAEGW

S-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`**Syntax Description****rotate-hd-file diameter** [ **name** *policy\_name* ]**name** *policy\_name*

Specifies the hd-storage policy name of an existing HD Storage Policy as an alphanumeric string of 0 through 63 characters.

**Usage Guidelines**

Use this command to manually rotate the Diameter HD stored files.

**Example**

The following command rotates Diameter files that were stored using the HD storage policy named CDR1:

**rotate-hd-file diameter name** *CDR1*

## save configuration

Saves the configuration of current contexts to a local or remote location. The configuration contains the sequence of CLI commands that define system parameters and ends with the **.cfg** extension.**Important**In release 20.0 and higher Trusted StarOS builds, FTP is not supported. SFTP is the recommended file transfer protocol.**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`**Syntax Description****save configuration** *url* [ **confd** | **ignore-locks** | **obsolete-encryption** | **showsecrets** | **verbose** ] [ **-redundant** ] [ **-noconfirm** ] [ **legacy-password-expiry** ]

**url**

Default: saves to the location of the active configuration currently loaded.

Specifies the location in which to store the configuration file. *url* may refer to a local or a remote file and must be entered in the following format:

For the ASR 5500:

```
[ file: ] { /flash | /usb1 | /hd-raid } [ /directory ] /file_name
tftp:// { host [ : port# ] } [ /directory ] /file_name
[ ftp: | sftp: ] // [ username [ :password ] @ ] { host } [ : port# ] [ /directory ] / file_name
```

For VPC:

```
[ file: ] { /flash | /hd-raid | /usb1 | usb2 | cdrom1 } [ /directory ] /file_name
tftp:// { host [ : port# ] } [ /directory ] /file_name
[ ftp: | sftp: ] // [ username [ :password ] @ ] { host } [ : port# ] [ /directory ] / file_name
```

**Important**

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

*directory* is the directory name.

*filename* is the actual file of interest.

*username* is the user to be authenticated.

*password* is the password to use for authentication.

*host* is the IP address or host name of the server.

**Important**

*host* can **only** be used if the **networkconfig** parameter is configured for DHCP and the DHCP server returns a valid nameserver.

The following file transfer protocols are supported on all platforms to save the configuration to a destination on the network (off box):

**tftp** – Trivial File Transfer Protocol [no username/password required]

**ftp** – File Transfer Protocol [username/password required]

**sftp** – SSH File Transfer Protocol [SSH username/password required]

*port#* is the logical port number that the communication protocol is to use.

**[ confd | ignore-locks | obsolete-encryption | showsecrets | verbose ]**

Specifies options when saving the configuration file.

**confd**: Saves only those configuration commands associated with the YANG model in support of Cisco NSO ConfD and the NETCONF protocol.



**ignore-locks:** Saves the configuration regardless of any configuration mode locks held by other administrative users or other external restrictions.



---

**Important** Use of the **ignore-locks** keyword may result in file corruption.

---

**obsolete-encryption:** Saves the configuration with encrypted values generated via an obsolete encryption method. This option may be required to preserve a configuration for a possible downgrade.



---

**Important** The **obsolete-encryption** keyword is only available in StarOS 19.1 and prior releases.

---

**showsecrets:** Saves the CLI configuration file with all passwords in plain text, rather than their default encrypted format.



---

**Important** The **showsecrets** keyword is only available in StarOS 19.1 and prior releases.

---

**verbose:** Saves as much information as possible, including default values. If this option is not specified, the configuration does not include default values.

### **legacy-password-expiry**

Generates a backward compatible file by removing new Expiry Notification keywords, which were introduced as part of Password Expiry Notification Feature in StarOS 21.23 release. The new `save config` CLI option makes the configuration compatible with older StarOS versions in which the Password Expiry Notification Feature is not present.

### **-redundant**

Saves the configuration file to the local device on the management card, defined by the `url` variable, and then automatically copies that same file to the like device on the standby management card, if available.

The management card can be any of the following:

- ASR 5500 – Management Input/Output (MIO) card [/flash, usb1, usb2]
- VPC-DI – Control Function (CF) virtual machine

Use the **-redundant** keyword if you have only made changes to the configuration, but not to the boot order or after installing a new boot image. Changes to the boot order or installing a new image requires file synchronization via the **filesystem synchronize** command.



---

**Important** This keyword will only work for local devices on both the active and standby management cards. Otherwise, a failure message is displayed. When saving the file to an external network (non-local) device, the system disregards this keyword.

---

**Important**

This keyword does not synchronize the local file system. If you have added, modified, or deleted other files or directories to or from a local device for the active management card, then synchronize the local file system on both cards.

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

**Caution**

Exercise caution when using the **-noconfirm** option as this overwrites data if the URL targets an existing file.

**Usage Guidelines**

Backup the current configuration as part of periodic maintenance activities for emergency recovery.

**Important**

Saving a configuration does not save the boot options as configured via the Global Configuration mode **boot** commands.

**Example**

The following command saves the configuration data to the local file */flash/pub/juneconfig.cfg* with no confirmation from the user:

```
save configuration /flash/pub/juneconfig.cfg -noconfirm
```

The following command saves the configuration data to remote host *remoteABC* at */pub/juneconfig.cfg*:

```
save configuration tftp://remoteABC/pub/juneconfig.cfg
```

The following command saves only those configuration commands associated with the YANG model in support of Cisco NSO ConfD and the NETCONF protocol:

```
save configuration confd /flash/netconf/confd.cfg
```

The following command generates a backward compatible file by removing new Expiry Notification keywords:

```
save config /flash/start-downgrade-20211012-c-op.cfg legacy-password-expiry
```

## save logs

Saves the current log file to a local or remote location.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
save logs { url } [ active ] [ inactive ] [ callid call_id ] [
event-verbosity evt_verbosity ] [ facility facility ] [ level severity_level ]
[ pdu-data pdu_format ] [ pdu-verbosity pdu_verbosity ] [ since from_date_time
[ until to_date_time ] ] [ | { grep grep_options | more } ]
```

#### *url*

Specifies the location to store the log file(s). *url* may refer to a local or a remote file and must be entered in the following format.

For the ASR 5000:

```
[ file: ] { /flash | /pcmcia1 | /hd-raid } [ /directory ] /file_name
tftp:// { host [ : port# ] } [ /directory ] /file_name
[ ftp: | sftp: ] // [ username[ :password ] @ ] { host } [ : port# ] [ /directory
] / file_name
```



#### Important

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

For the ASR 5500:

```
[ file: ] { /flash | /usb1 | /hd-raid } [ /directory ] /file_name
tftp:// { host [ : port# ] } [ /directory ] /file_name
[ ftp: | sftp: ] // [ username[ :password ] @ ] { host } [ : port# ] [ /directory
] / file_name
```

For VPC:

```
[ file: ] { /flash | /hd-raid | /usb1 | /usb2 | /cdrom1 } [ /directory ]
/file_name
tftp:// { host [ : port# ] } [ /directory ] /file_name
[ ftp: | sftp: ] // [ username[ :password ] @ ] { host } [ : port# ] [ /directory
] / file_name
```



#### Important

The USB ports and CDROM must be configured via the hypervisor to be accessible.



#### Important

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

*directory* is the directory name.

*filename* is the actual file of interest.

*username* is the user to be authenticated.

*password* is the password to use for authentication.

*host* is the IP address or host name of the server.




---

**Important** *hostname* can only be used if the **networkconfig** parameter is configured for DHCP and the DHCP server returns a valid nameserver.

---

*port#* is the logical port number that the communication protocol is to use.

#### **active**

Saves data from active logs.

#### **inactive**

Saves data from inactive logs.

#### **callid *call\_id***

Specifies a call ID for which log information is to be saved as a 4-byte hexadecimal number.

#### **event-verbosity *evt\_verbosity***

Specifies the level of verbosity to use in displaying of event data as one of:

- *min*: Logs minimal information about the event. Information includes event name, facility, event ID, severity level, date, and time.
- *concise*: Logs detailed information about the event, but does not provide the event source within the system.
- *full*: Logs detailed information about event, including source information, identifying where within the system the event was generated.

#### **facility *facility***

Specifies the facility to modify the filtering of logged information. Valid facilities for this command are:

- **a10**: A10 interface facility
- **a11**: A11 interface facility
- **a11mgr**: A11 Manager facility
- **aaa-client**: Authentication, Authorization and Accounting (AAA) client facility
- **aaamgr**: AAA manager logging facility
- **aaaproxy**: AAA Proxy facility
- **aal2**: ATM Adaptation Layer 2 (AAL2) protocol logging facility
- **acl-log**: Access Control List (ACL) logging facility
- **acsctrl**: Active Charging Service (ACS) Controller facility
- **acsmgr**: ACS Manager facility

- **afctrl**: Fabric Controller facility [ASR 5500 only]
- **afmgr**: Fabric Manager logging facility [ASR 5500 only]
- **alarmctrl**: Alarm Controller facility
- **alcap**: Access Link Control Application Part (ALCAP) protocol logging facility
- **alcapmgr**: ALCAP manager logging facility
- **all**: All facilities
- **asnwmgr**: Access Service Network (ASN) Gateway Manager facility
- **asnpcmgr**: ASN Paging Controller Manager facility
- **bfd**: Bidirectional Forwarding Detection (BFD) protocol logging facility
- **bgp**: Border Gateway Protocol (BGP) facility
- **bindmux**: IPCF BindMux-Demux Manager logging facility
- **bngmgr**: Broadband Network Gateway (BNG) Demux Manager logging facility
- **bssap+**: Base Station Sub-system Application Part+ protocol facility for the login interface between the SGSN and the MSC/VLR (2.5G and 3G)
- **bssgp**: Base Station Sub-system GPRS Protocol logging facility handles exchange information between the SGSN and the BSS (2.5G only)
- **callhome**: Call Home application logging facility
- **cap**: CAMEL Application Part (CAP) logging facility for protocol used in prepaid applications (2.5G and 3G)
- **cbsmgr**: Cell Broadcasting Service (CBS) logging facility [HNBGW]
- **cdf**: Charging Data Function (CDF) logging facility
- **cgw**: Converged Access Gateway (CGW) logging facility
- **cli**: Command Line Interface (CLI) logging facility
- **cmp**: Certificate Management Protocol (IPSec) logging facility
- **connectedapps**: SecGW ASR 9000 oneP communication protocol
- **connproxy**: Controller Proxy logging facility
- **credit-control**: Credit Control (CC) facility
- **csp**: Card/Slot/Port controller facility
- **css**: Content Service Selection (CSS) facility
- **css-sig**: CSS RADIUS Signaling facility
- **cx-diameter**: Cx Diameter Messages facility [CSCF <--> HSS]
- **data-mgr**: Data Manager Framework logging facility
- **dcardctrl**: IPSec Daughter Card Controller logging facility

- **dcardmgr**: IPSec Daughter Card Manager logging facility
- **demuxmgr**: Demux Manager API facility
- **dgmbmgr**: Diameter Gmb Application Manager logging facility
- **dhcp**: Dynamic Host Configuration Protocol (DHCP) logging facility
- **dhcpv6**: DHCPv6
- **dhost**: Distributed Host logging facility
- **diabase**: Diabase messages facility
- **diactrl**: Diameter Controller proctlet logging facility
- **diameter**: Diameter endpoint logging facility
- **diameter-acct**: Diameter Accounting
- **diameter-auth**: Diameter Authentication
- **diameter-dns**: Diameter DNS subsystem
- **diameter-ecs**: ACS Diameter signaling facility
- **diameter-engine**: Diameter version2 engine logging facility
- **diameter-hdd**: Diameter Horizontal Directional Drilling (HDD) Interface facility
- **diameter-svc**: Diameter Service
- **diamproxy**: DiamProxy logging facility
- **dpath**: IPSec Data Path facility
- **drvctrl**: Driver Controller facility
- **dpath**: IPSec Data Path logging facility
- **drvctrl**: Driver Controller logging facility
- **doulosuemgr**: Doulos (IMS-IPSec-Tool) user equipment manager
- **eap-diameter**: Extensible Authentication Protocol (EAP) IP Sec urity facility
- **eap-ipsec**: Extensible Authentication Protocol (EAP) IPSec facility
- **eap-sta-s6a-s13-s6b-diameter**: EAP/STA/S6A/S13/S6B Diameter messages facility
- **ecs-css**: ACSMGR <-> Session Manager Signalling Interface facility
- **egtpc**: eGTP-C logging facility
- **egtpmgr**: enhanced GPRS Tunneling Protocol (eGTP) manager logging facility
- **egtpu**: eGTP-U logging facility
- **embms**: evolved Multimedia Broadcast Multicast Services Gateway facility
- **embms**: eMBMS Gateway Demux facility
- **epdg**: evolved Packet Data (ePDG) gateway logging facility

- **event-notif**: Event Notification Interface logging facility
- **evlog**: Event log facility
- **famgr**: Foreign Agent manager logging facility
- **firewall**: Firewall logging facility
- **fng**: Femto Network Gateway (FNG) logging facility
- **gbmgr**: SGSN Gb Interface Manager facility
- **gmm**:
  - For 2.5G: Logs the GPRS Mobility Management (GMM) layer (above LLC layer)
  - For 3G: Logs the access application layer (above the RANAP layer)
- **gprs-app**: GPRS Application logging facility
- **gprs-ns**: GPRS Network Service Protocol (layer between SGSN and the BSS) logging facility
- **gq-rx-tx-diameter**: Gq/Rx/Tx Diameter messages facility
- **gss-gcdr**: GTP Storage Server GCDR facility
- **gtpe**: GTP-C protocol logging facility
- **gtpcmgr**: GTP-C protocol manager logging facility
- **gtp**: GTP-prime protocol logging facility
- **gtpu**: GTP-U protocol logging facility
- **gtpumgr**: GTP-U Demux manager
- **gx-ty-diameter**: Gx/Ty Diameter messages facility
- **gy-diameter**: Gy Diameter messages facility
- **h248prt**: H.248 port manager facility
- **hamgr**: Home Agent manager logging facility
- **hat**: High Availability Task (HAT) process facility
- **hdctrl**: HD Controller logging facility
- **henbapp**: Home Evolved NodeB (HENB) App facility



---

**important** In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

- **henbgw**: HENB-GW facility




---

**important** In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

- **henbgw-pws**: HENB-GW Public Warning System logging facility




---

**important** In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

- **henbgw-sctp-acs**: HENB-GW access Stream Control Transmission Protocol (SCTP) facility




---

**important** In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

- **henbgw-sctp-nw**: HENBGW network SCTP facility




---

**important** In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

- **henbgwdemux**: HENB-GW Demux facility




---

**important** In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

- **henbgwmgr**: HENB-GW Manager facility




---

**important** In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

- **hnb-gw**: HNB-GW (3G Femto GW) logging facility






---

**hnbgr** In Release 20 and later, HNBGW is not supported. This keyword must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

---

- **hnbmgr**: HNB-GW Demux Manager logging facility




---

**hnbgr** In Release 20 and later, HNBGW is not supported. This keyword must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

---

- **hss-peer-service**: Home Subscriber Server (HSS) Peer Service facility
- **igmp**: Internet Group Management Protocol (IGMP)
- **ikev2**: Internet Key Exchange version 2 (IKEv2)
- **ims-authorizatn**: IP Multimedia Subsystem (IMS) Authorization Service facility
- **ims-sh**: HSS Diameter Sh Interface Service facility
- **imsimgr**: SGSN IMSI Manager facility
- **imsue**: IMS User Equipment (IMSUE) facility
- **ip-arp**: IP Address Resolution Protocol facility
- **ip-interface**: IP interface facility
- **ip-route**: IP route facility
- **ipms**: Intelligent Packet Monitoring System (IPMS) logging facility
- **ipne**: IP Network Enabler (IPNE) facility
- **ipsec**: IP Security logging facility
- **ipsecdemux**: IPSec demux logging facility
- **ipsg**: IP Service Gateway interface logging facility
- **ipsgmgr**: IP Services Gateway facility
- **ipsp**: IP Pool Sharing Protocol logging facility
- **kvstore**: Key/Value Store (KVSTORE) Store facility
- **l2tp-control**: Layer 2 Tunneling Protocol (L2TP) control logging facility
- **l2tp-data**: L2TP data logging facility
- **l2tpdemux**: L2TP Demux Manager logging facility
- **l2tpmgr**: L2TP Manager logging facility
- **lagmgr**: Link Aggregation Group (LAG) manager logging facility

- **lcs**: Location Services (LCS) logging facility
- **ldap**: Lightweight Directory Access Protocol (LDAP) messages logging facility
- **li**: Refer to the *Lawful Intercept Configuration Guide* for a description of this command.
- **linkmgr**: SGSN/BSS SS7 Link Manager logging facility (2.5G only)
- **llc**: Logical Link Control (LLC) Protocol logging facility; for SGSN: logs the LLC layer between the GMM and the BSSGP layers for logical links between the MS and the SGSN
- **local-policy**: Local Policy Service facility
- **location-service**: Location Services facility
- **m3ua**: M3UA Protocol logging facility
- **magmgr**: Mobile Access Gateway manager logging facility
- **map**: Mobile Application Part (MAP) protocol logging facility
- **megadiammgr**: MegaDiameter Manager (SLF Service) logging facility
- **mme-app**: Mobility Management Entity (MME) Application logging facility
- **mme-misc**: MME miscellaneous logging facility
- **mmedemux**: MME Demux Manager logging facility
- **mmemgr**: MME Manager facility
- **mmgr**: Master Manager logging facility
- **mobile-ip**: Mobile IP processes
- **mobile-ip-data**: Mobile IP data facility
- **mobile-ipv6**: Mobile IPv6 logging facility
- **mpls**: Multiprotocol Label Switching (MPLS) protocol logging facility
- **mrme**: Multi Radio Mobility Entity (MRME) logging facility
- **mseg-app**: Mobile Services Edge Gateway (MSEG) application logging facility (This option is not supported in this release.)
- **mseg-gtpc**: MSEG GTP-C application logging facility (This option is not supported in this release.)
- **mseg-gtpu**: MSEG GTP-U application logging facility (This option is not supported in this release.)
- **msegmgr**: MSEG Demux Manager logging facility (This option is not supported in this release.)
- **mtp2**: Message Transfer Part 2 (MTP2) Service logging facility
- **mtp3**: Message Transfer Part 3 (MTP3) Protocol logging facility
- **multicast-proxy**: Multicast Proxy logging facility
- **nas**: Non-Access Stratum (NAS) protocol logging facility [MME 4G]
- **netwstrg**: Network Storage facility
- **npuctrl**: Network Processor Unit Control facility

- **npudrv**: Network Processor Unit Driver facility [ASR 5500 only]
- **npumgr**: Network Processor Unit Manager facility
- **npumgr-acl**: NPUMGR ACL logging facility
- **npumgr-drv**: NPUMGR DRV logging facility
- **npumgr-flow**: NPUMGR FLOW logging facility
- **npumgr-fwd**: NPUMGR FWD logging facility
- **npumgr-init**: NPUMGR INIT logging facility
- **npumgr-lc**: NPUMGR LC logging facility
- **npumgr-port**: NPUMGR PORT logging facility
- **npumgr-recovery**: NPUMGR RECOVERY logging facility
- **npumgr-rri**: NPUMGR RRI (Reverse Route Injection) logging facility
- **npumgr-vpn**: NPUMGR VPN logging facility
- **npusim**: NPUSIM logging facility [ASR 5500 only]
- **ntfy-intf**: Notification Interface logging facility [Release 12.0 and earlier versions only]
- **ocsp**: Online Certificate Status Protocol logging facility.
- **orbs**: Object Request Broker System logging facility
- **ospf**: OSPF protocol logging facility
- **ospfv3**: OSPFv3 protocol logging facility
- **p2p**: Peer-to-Peer Detection logging facility
- **pagingmgr**: PAGINGMGR logging facility
- **pccmgr**: Intelligent Policy Control Function (IPCF) Policy Charging and Control (PCC) Manager library
- **pdg**: Packet Data Gateway (PDG) logging facility
- **pdgdmgr**: PDG Demux Manager logging facility
- **pdif**: Packet Data Interworking Function (PDIF) logging facility
- **pgw**: Packet Data Network Gateway (PGW) logging facility
- **pmm-app**: Packet Mobility Management (PMM) application logging facility
- **ppp**: Point-To-Point Protocol (PPP) link and packet facilities
- **pppoe**: PPP over Ethernet logging facility
- **proclat-map-frwk**: Proclat mapping framework logging facility
- **push**: VPNMGR CDR push logging facility
- **radius-acct**: RADIUS accounting logging facility
- **radius-auth**: RADIUS authentication logging facility

- **radius-coa**: RADIUS change of authorization and radius disconnect
- **ranap**: Radio Access Network Application Part (RANAP) Protocol facility logging info flow between SGSN and RNS (3G)
- **rct**: Recovery Control Task logging facility
- **rdt**: Redirect Task logging facility
- **resmgr**: Resource Manager logging facility
- **rf-diameter**: Diameter Rf interface messages facility
- **rip**: Routing Information Protocol (RIP) logging facility [RIP is not supported at this time.]
- **rlf**: Rate Limiting Function (RLF) logging facility
- **rohc**: Robust Header Compression (RoHC) facility
- **rsvp**: Reservation Protocol logging facility
- **rua**: RANAP User Adaptation (RUA) [3G Femto GW - RUA messages] logging facility
- **s102**: S102 protocol logging facility
- **s102mgr**: S102Mgr logging facility
- **s1ap**: S1 Application Protocol (S1AP) Protocol logging facility
- **sabp**: Service Area Broadcast Protocol (SABP) logging facility
- **saegw**: System Architecture Evolution (SAE) Gateway facility
- **sbc**: SBc protocol logging facility
- **sccp**: Signalling Connection Control Part (SCCP) Protocol logging (connection-oriented messages between RANAP and TCAP layers).
- **sct**: Shared Configuration Task logging facility
- **sctp**: Stream Control Transmission Protocol (SCTP) Protocol logging facility
- **sef\_ecs**: Severely Errored Frames (SEF) APIs printing facility
- **sess-gr**: SM GR facility
- **sessctrl**: Session Controller logging facility
- **sessmgr**: Session Manager logging facility
- **sesstrc**: session trace logging facility
- **sft**: Switch Fabric Task logging facility
- **sgs**: SGs interface protocol logging facility
- **sgsn-app**: SGSN-APP logging various SGSN "glue" interfaces (for example, between PMM, MAP, GPRS-FSM, SMS).
- **sgsn-failures**: SGSN call failures (attach/activate rejects) logging facility (2.5G)
- **sgsn-gtpc**: SGSN GTP-C Protocol logging control messages between the SGSN and the GGSN

- **sgsn-gtpu**: SGSN GTP-U Protocol logging user data messages between the SGSN and GGSN
- **sgsn-mbms-bearer**: SGSN Multimedia Broadcast/Multicast Service (MBMS) Bearer app (SMGR) logging facility
- **sgsn-misc**: Used by stack manager to log binding and removing between layers
- **sgsn-system**: SGSN System Components logging facility (used infrequently)
- **sgsn-test**: SGSN Tests logging facility; used infrequently
- **sgtpcmgr**: SGSN GTP-C Manager logging information exchange through SGTPC and the GGSN
- **sgw**: Serving Gateway facility
- **sh-diameter**: Sh Diameter messages facility
- **sitmain**: System Initialization Task main logging facility
- **sls**: Service Level Specification (SLS) protocol logging facility
- **sm-app**: SM Protocol logging facility
- **sms**: Short Message Service (SMS) logging messages between the MS and the SMSC
- **sndcp**: Sub Network Dependent Convergence Protocol (SNDCP) logging facility
- **snmp**: SNMP logging facility
- **sprmgr**: IPCF Subscriber Policy Register (SPR) manager logging facility
- **srdp**: Static Rating Database
- **srp**: Service Redundancy Protocol (SRP) logging facility
- **sscfnni**: Service-Specific Coordination Function for Signaling at the Network Node Interface (SSCF-NNI) logging facility
- **sscop**: Service-Specific Connection-Oriented Protocol (SSCOP) logging facility
- **ssh-ipsec**: Secure Shell (SSH) IP Security logging facility
- **ssl**: Secure Socket Layer (SSL) message logging facility
- **stat**: Statistics logging facility
- **supserv**: Supplementary Services logging facility [H.323]
- **system**: System logging facility
- **tacacsplus**: TACACS+ Protocol logging facility
- **tcap**: TCAP Protocol logging facility
- **testctrl**: Test Controller logging facility
- **testmgr**: Test Manager logging facility
- **threshold**: threshold logging facility
- **ttg**: Tunnel Termination Gateway (TTG) logging facility

- **tucl**: TCP/UDP Convergence Layer (TUCL) logging facility
- **udr**: User Data Record (UDR) facility (used with the Charging Service)
- **user-data**: User data logging facility
- **user-l3tunnel**: User Layer 3 tunnel logging facility
- **usertcp-stack**: User TCP Stack
- **vim**: Voice Instant Messaging (VIM) logging facility
- **vinfo**: VINFO logging facility
- **vmgctrl**: Virtual Media Gateway (VMG) controller facility
- **vmgctrl**: VMG Content Manager facility
- **vpn**: Virtual Private Network logging facility
- **wimax-data**: WiMAX DATA
- **wimax-r6**: WiMAX R6
- **wsg**: Wireless Security Gateway (ASR 9000 Security Gateway)
- **x2gw-app**: X2GW (X2 proxy Gateway, eNodeB) application logging facility
- **x2gw-demux**: X2GW demux task logging facility

#### **level severity\_level**

Specifies the level of information to be logged from the following list which is ordered from highest to lowest:

- *critical*: Logs critical events
- *error*: Logs error events and all events with a higher severity level
- *warning*: Logs warning events and all events with a higher severity level
- *unusual*: Logs unusual events and all events with a higher severity level
- *info*: Logs info events and all events with a higher severity level
- *trace*: Logs trace events and all events with a higher severity level
- *debug*: Logs all events

#### **pdu-data pdu\_format**

Specifies output format for the display of packet data units as one of:

- *none* - raw format (unformatted).
- *hex* - hexadecimal format.
- *hex-ascii* - hexadecimal and ASCII similar to a main-frame dump.

#### **pdu-verbosity pdu\_verbosity**

Specifies the level of verbosity to use in displaying of packet data units as a value from 1 to 5, where 5 is the most detailed.

**since *from\_date\_time* [ until *to\_date\_time* ]**

Default: no limit.

**since *from\_date\_time***: Saves only the log information which has been collected more recently than *from\_date\_time*.

**until *to\_date\_time***: Saves no log information more recent than *to\_date\_time*. Defaults to current time when omitted.

*from\_date\_time* and *to\_date\_time* must be formatted as YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss. Where:

- YYYY = 4-digit year
- MM = 2-digit month in the range 01 through 12
- DD = 2-digit day in the range 01 through 31
- HH = 2-digit hour in the range 00 through 23
- mm = 2-digit minute in the range 00 through 59
- ss = 2 digit second in the range 00 through 59

*to\_date\_time* must be a time which is more recent than *from\_date\_time*.

Using the **until** keyword allows for a time range of log information; using only the **since** keyword will display all information up to the current time.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in *Command Line Interface Reference*.

**Usage Guidelines**

Backup the current log file as part of periodic maintenance activities.

**Example**

The following saves the log to the local file */flash/pub/junelogs.logs* with no confirmation from the user:

```
save logs /flash/pub/junelogs.logs -noconfirm
```

The following saves the configuration data to remote host *remoteABC* as */pub/junelogs.logs*:

```
save logs tftp://remoteABC/pub/junelogs.logs
```

## session trace

Enable or disables the subscriber session trace functionality based on a specified subscriber device or ID on one or all instance of session on a specified UMTS/EPS network element. It also clears/resets the statistics collected for subscriber session trace on a system.

---

**Product**

GGSN  
MME  
P-GW  
SAEGW  
S-GW

---

**Privilege**

Operator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
session trace { reset statistics | subscriber network-element { mme | pgw
| sgw | ggsn saegw [func-pgw | func-sgw ] { imei id | imsi id | interface
{ all | interface } | target-all-ne | target-ne { enb [ target-interface
{ all | interface } ] | pgw [ target-interface { all | interface } ] | sgw [
target-interface { all | interface ] } } trace-ref id collection-entity
ip_address
no session trace subscriber network-element [ mme | pgw | sgw | ggsn ] [
trace-ref id ]
```

**no**

Disables the entire session trace or for a specific network element and/or trace reference.

**reset statistics**

Clears/resets the entire session trace statistical data collected on a system.



**Caution**

This is a system wide command that affects all statistical data.

---

**session trace subscriber network-element { mme | pgw | sgw | ggsn }**

Identifies the network element that, in turn, identifies the interfaces where the session trace is to occur. Specific interfaces can be specified using the interface keyword described below.

**ggsn**: Specifies that the session trace is to occur on one or all interfaces on the GGSN.

**mme**: Specifies that the session trace is to occur on one or all interfaces on the MME.

**pgw**: Specifies that the session trace is to occur on one or all interfaces on the P-GW.

**sgw**: Specifies that the session trace is to occur on one or all interfaces on the S-GW.

**imei *id***

Specifies the International Mobile Equipment Identification number of the subscriber UE. *id* must be the 8-digit TAC (Type Allocation Code) and 6-digit serial number. Only the first 14 digits of the IMEI/IMEISV are used to find the equipment ID.



**imsi *id***

Specifies the International Mobile Subscriber Identification (IMSI). *id* must be the 3-digit MCC (Mobile Country Code), 2- or 3- digit MNC (Mobile Network Code), and the MSIN (Mobile Subscriber Identification Number). The total should not exceed 15 digits.

**interface { *all* | *interface* }**

Specifies the interfaces where the session trace application will collect data.

**all:** Specifies all interfaces associated with the selected network element

*interface:* Specifies the interface type where the session trace application will collect trace data. The following interfaces are applicable for each network element type:

**GGSN:**

- **gi:** Specifies that the interface where the trace will be performed is the Gi interface between the GGSN and RADIUS server.
- **gmb:** Specifies that the interface where the trace will be performed is the Gmb interface between the GGSN and BM-SC.
- **gn:** Specifies that the interface where the trace will be performed is the Gn interface between the GGSN and the SGSN.
- **gx:** Specifies that the interface where the trace will be performed is the Gx interface between the GGSN and PCRF.
- **gy:** Specifies that the interface where the trace will be performed is the Gy interface between the GGSN and OCS.

**MME:**

- **s1mme:** Specifies that the interface where the trace will be performed is the S1-MME interface between the MME and the eNodeB.
- **s3:** Specifies that the interface where the trace will be performed is the S3 interface between the MME and an SGSN.
- **s6a:** Specifies that the interface where the trace will be performed is the S6a interface between the MME and the HSS.
- **s10:** Specifies that the interface where the trace will be performed is the S10 interface between the MME and another MME.
- **s11:** Specifies that the interface where the trace will be performed is the S11 interface between the MME and the S-GW.
- **s13:** Specifies that the interface where the trace will be performed is the S13 interface between the MME and the EIR.

**P-GW:**

- **gx:** Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
- **gy:** Specifies that the interface where the trace will be performed is the Gy interface between the P-GW and OCS.

- **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the P-GW and the HSGW.
- **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the P-GW and an ePDG.
- **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the P-GW and a trusted, non-3GPP access device.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.
- **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the P-GW and the 3GPP AAA server.
- **s8b**: Specifies that the interface where the trace will be performed is the S8b interface between the P-GW and the S-GW.
- **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the P-GW and the PDN.

#### S-GW:

- **gxc**: Specifies that the interface where the trace will be performed is the Gxc interface between the S-GW and the PCRF.
- **gy**: Specifies that the interface where the trace will be performed is the Gy interface between the S-GW and OCS.
- **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the S-GW and the MME.
- **s4**: Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and an SGSN.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the S-GW and the P-GW.
- **s8b**: Specifies that the interface where the trace will be performed is the S8b interface between the S-GW and the P-GW.

#### target-all-ne

This option is applicable for MME only. Specifies that the trace be propagated to neighboring Network Elements (NEs) including the eNodeB, P-GW and S-GW. With this option, tracing will occur on all applicable interfaces on the respective NEs.

**target-ne { enb [ target-interface { all | interface } ] | pgw [ target-interface { all | interface } ] | sgw [ target-interface { all | interface } ] }**

This option is applicable for MME only.

The **target-ne { enb | pgw | sgw }** keyword specifies that the trace be propagated to the specified neighboring Network Elements (NE). More than one **target-ne** can be configured in the same command.

**target-interface { all | interface }**: This optional keyword specifies the interface on the target NE where the trace will be performed. Multiple target-interfaces can be defined within the same command.

**trace-ref *id***

Specifies the trace reference for the trace being initiated. *id* must be the MCC (3 digits), followed by the MNC (3 digits), then the trace ID number (3-byte octet string).

**collection-entity *ip\_address***

Specifies the IP address of the collection entity where session trace data is pushed in IPv4 dotted-decimal notation.

**Usage Guidelines**

Use this command to initiate a session trace for a specified subscriber device or ID on one or all interfaces on a specified network element.

**Important**

Session trace configuration is performed in the *Global Configuration Mode* using the **session trace** command. Refer to the *Global Configuration Mode Commands* chapter for more information.

**Example**

The following command initiates a session trace on a P-GW S5 interface for a subscriber with an IMSI of *322233123456789* and sets the trace reference as *322233987654* and the collection entity IP address as *10.2.3.4*:

```
session trace subscriber network-element pgw imsi 322233123456789 interface
s5 trace-ref 322233987654 collection-entity 10.2.3.4
```

The following command initiates a session trace on an MME S6a interface for a subscriber with an IMSI of *322233123456789* and sets the trace reference as *322233987654* and the collection entity IP address as *10.2.3.4*:

```
session trace subscriber network-element mme imsi 322233123456789 interface
s6a trace-ref 322233987654 collection-entity 10.2.3.4
```

The following command initiates a session trace on a Gn interface on GGSN between GGSN and SGSN for a subscriber with an IMSI of *322233123456789* and sets the trace reference as *322233987654* and the collection entity IP address as *10.2.3.4*:

```
session trace subscriber network-element ggsn imsi 322233123456789
interface gn trace-ref 322233987654 collection-entity 10.2.3.4
```

**MME Only:** The following command activates a session trace on S-GW for S5 interface from the MME:

```
session trace subscriber network-element mme imsi 000012345 target-ne
sgw target-interface s5
```

## session trace random

Enable or disables the subscriber session trace functionality based on a the random trace on the network element. If enabled, the subscriber selection will be based on random logic all instance of session on a specified UMTS/EPS network element. It also clears/resets the statistics collected for subscriber session trace on a system.

**Product** GGSN  
P-GW

**Privilege** Operator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **[no] session trace random** *random\_num* **network-element** {**ggsn** | **pgw**} [**interface** {**all** | *interface*}]

#### **no**

Disables the entire random subscriber session trace or for a specific network element and/or interface.

#### **session trace random** *random\_num*}

Configures the number of random subscriber sessions where the session trace is to occur.

*random\_num* is an integer between 1 to 1000 identified the number of subscribers to be selected by random logic.

#### **network-element** {**ggsn** | **pgw**}

Identifies the network element that, in turn, identifies the interfaces where the random session trace is to occur. Specific interfaces can be specified using the interface keyword described below.

**ggsn**: Specifies that the random session trace is to occur on one or all interfaces on the GGSN.

**pgw**: Specifies that the random session trace is to occur on one or all interfaces on the P-GW.

#### **interface** { **all** | *interface* }

Specifies the interfaces where the random session trace application will collect data.

**all**: Specifies all interfaces associated with the selected network element

*interface*: Specifies the interface type where the random session trace application will collect trace data. The following interfaces are applicable for the network element type:

- **GGSN**:
  - **gi**: Specifies that the interface where the trace will be performed is the Gi interface between the GGSN and RADIUS server.
  - **gmb**: Specifies that the interface where the trace will be performed is the Gmb interface between the GGSN and BM-SC.
  - **gn**: Specifies that the interface where the trace will be performed is the Gn interface between the GGSN and the SGSN.
  - **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the GGSN and PCRF.

- **gy**: Specifies that the interface where the trace will be performed is the Gy interface between the GGSN and Diameter.
- P-GW:
  - **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
  - **gy**: Specifies that the interface where the trace will be performed is the Gy interface between the GGSN and Diameter.
  - **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the P-GW and the HSGW.
  - **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the P-GW and an ePDG.
  - **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the P-GW and a trusted, non-3GPP access device.
  - **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.
  - **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the P-GW and the 3GPP AAA server.
  - **s8b**: Specifies that the interface where the trace will be performed is the S8b interface between the P-GW and the S-GW.
  - **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the P-GW and the PDN.

### Usage Guidelines

Use this command to initiate the session trace for a specified subscriber sessions selected on random logic on one or all interfaces on a specified network element.



### Important

Session trace configuration is performed in the *Global Configuration Mode* using the **session trace** command. Refer to the *Global Configuration Mode Commands* chapter for more information.

### Example

The following command initiates a session trace on a GGSN Gx interface for 1000 subscriber session selected on random logic:

```
session trace random 1000 network-element ggsn interface gx
```

## session trace signaling

Enable or disables the subscriber session trace functionality based on signaling information on one or all instance of session on a specified UMTS/EPS network element. It also clears/resets the statistics collected for subscriber session trace on a system.

---

**Product** GGSN  
P-GW

---

**Privilege** Operator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `[no] session trace signaling network-element {ggsn | pgw}`

**no**

Disables the entire session trace based on signaling information for a specific network element and/or trace reference.

**session trace signaling network-element {pgw | ggsn}**

Identifies the network element that where the session trace based on signaling information for a subscriber session is to occur. Specific network element GPRS/EPS can be specified for this session trace.

**ggsn**: Specifies that the session trace based on signaling is to occur on one or all interfaces on the GGSN.

**pgw**: Specifies that the session trace based on signaling is to occur on one or all interfaces on the P-GW.

---

**Usage Guidelines** Use this command to initiate a session trace for a specified subscriber based on signaling information on a specified network element.



**Important**

Session trace configuration is performed in the *Global Configuration Mode* using the **session trace** command. Refer to the *Global Configuration Mode Commands* chapter for more information.

---

**Example**

The following command initiates a session trace on a GGSN for a subscriber based on signaling information.

```
session trace signaling network-element ggsn
```

## setup

Enters the system setup wizard which guides the user through a series of questions regarding the system basic configuration options, such as initial context-level administrative users, host name, etc.

---

**Product** All

---

**Privilege** Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description****setup****Usage Guidelines**

The setup wizard provides a user friendly interface for initial system configuration.

**Important**

If the configuration script generated by the setup wizard is applied when an existing configuration is in use, the options which are common to both are updated and all remaining options are left unchanged.

**Example**

The following command starts the setup wizard:

```
setup
```

## sgs offload

Enables or disables offloading of UEs associated with a VLR which has become unavailable. This enables the MME to preemptively move subscribers away from a VLR which is scheduled to be put in maintenance mode.

**Product**

MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
sgs offload sgs-service sgs_svc_name vlr vlr_name { start time-duration minutes
| stop } [ -noconfirm ]
```

**sgs-service** *sgs\_svc\_name*

Specifies the SGs service to which the VLR belongs.

*sgs\_svc\_name* specifies the name of a pre-configured SGs service. For more information on the SGs service, refer to the **sgs-service** command in the *Context Configuration Mode Commands* chapter and refer to the *MME SGs Service Configuration Mode Commands* chapter.

**vlr** *vlr\_name*

Specifies the VLR service which must have its UEs offloaded.

*vlr\_name* specifies the name for a pre-configured VLR and must be an alphanumeric string of 1 through 63 characters. For more information, refer to the **vlr** command in the *MME SGs Service Configuration Mode Commands* chapter.

#### **start time-duration minutes**

Specifies that the UE offloading should be started for the specified the VLR.

**time-duration** defines the period in *minutes* over which all qualifying subscribers will be offloaded.

*minutes* must be an integer from 0 to 3000.

A value of 0 enables only Passive VLR Offloading, where the MME marks all affected session manager with the "VLR Offload" flag. During the next UE activity, the MME requires each UE to perform a combined TAU/LAU. This flag is not affected by the removal of the "offload" state by the operator. Even though the VLR state may later change from "offloaded" to "not-offloaded", the subscriber's state will not change to "not-offloaded".

A value of 1-3000 enables Active VLR Offloading and Passive VLR Offloading. The MME splits this time-duration into *n* intervals, 5 seconds apart. A maximum of 50 subscribers will be actively detached per interval. For example, a setting of 5 minutes with 600 subscribers in a sessmgr (from the given VLR) would detach 10 subscribers per 5-second interval. Node level detach rate should be estimated by taking into account the number of sessmgr tasks. Any subscribers remaining at the expiry of the time-duration will not be detached.

**Note:** For Release 12.2, only Passive VLR Offloading is supported. While the **time-duration** value is not used in Release 12.2 or earlier, it is required for completion of the **start** command.

#### **stop**

Specifies that the offload state should no longer be set for the specified the VLR.

#### **-noconfirm**

Indicates that the command is to execute without additional prompt and confirmation from the user.

### Usage Guidelines

This command enables the MME to preemptively move subscribers away from a VLR which is scheduled to be put in maintenance mode. When this offload command is set on the MME, all session manager matching this VLR are marked with an "offload" flag. If the time-duration keyword is set to 1-3000, session manager are also detached and required to reattach.

The configured time-duration is used to explicitly detach the subscriber in a specified rate. Upon expiry of the timer, the offload state of the VLR will not be changed and the offloading must be stopped by explicitly triggering the "stop" option.

The behavior of SGs with respect to "Location Updates" towards the MSC is similar to the behavior when the "VLR Reliable" flag is set to "false". In other words, for offloaded subscribers, normal Combined TAUs (without IMSI Attach) and periodic TAUs will trigger a LU towards the MSC.

When issuing the command, the MME notifies the operator if this is the last available VLR in a pool.

More than one VLR may be offloaded at the same time.

VLR Offloading and MME offloading cannot be performed at the same time.



#### Important

This is a licensed feature and is unavailable unless the proper licensed is installed.



**Related Commands:**

- To display VLR offload information and statistics for a specified SGs service name, refer to the **show sgs-service offload-status service-name** *sgs\_svc\_name* command.
- To clear the counters displayed by the previous command, issue the **clear sgs-service statistics service-name** *sgs\_svc\_name* command.

**Example**

The following command starts offloading the subscribers associated with *vlr1* over the next 60 minutes.

```
sgs offload sgs-service sgs1 vlr vlr1 start time-duration 60 -noconfirm
```

## sgs vlr-failure

This command configures the MME to monitor all VLRs and perform a controlled release (detach) of affected UEs when any VLR becomes unavailable.

---

**Product** MME

---

**Privilege** Security Administrator, Administrator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **sgs vlr-failure sgs-service** *sgs\_svc\_name* **duration** *minutes* **backoff-timer** *seconds*  
[ **-noconfirm** ]

**no sgs vlr-failure sgs-service** *sgs\_svc\_name*

**no**

Resets the command to its default setting of disabled.

**sgs**

Specifies SGS exec commands.

**vlr-failure**

Specifies VLR failure configuration.

**sgs-service** *sgs\_svc\_name*

Specifies the name of a pre-configured SGs Service to which the VLR belongs.

*sgs\_svc\_name* must be a string of size 1 to 63.

**duration *minutes***

Specifies the amount of time in minutes during which all qualifying UEs will be detached.

The MME splits this duration into  $n$  intervals, 5 seconds apart. A maximum of 50 subscribers are processed per interval per session manager. For example, a setting of 5 minutes with 600 subscribers in a session manager (from a given VLR) would result in the session manager processing 10 subscribers per 5-second interval. Node level detach rate should be estimated by taking into account the number of sessmgr tasks. Any subscribers remaining at the expiry of the duration will not be processed.

*minutes* must be an integer from 1 through 3000.

**backoff-timer *seconds***

Specifies the period of time the MME will wait following the detection of a VLR condition before starting the controlled release of affected UEs.

Specifies the backoff timer in seconds.

*seconds* must be an integer from 1 to 3000.

**-noconfirm**

Indicates that the command is to execute without additional prompt and confirmation from the user.

**Usage Guidelines**

When this command is issued, the MME monitors the availability of all VLRs. If one or more VLRs become unavailable, the MME performs a controlled release (EPS IMSI detach) for all UEs associated with that VLR. If another VLR is available, the MME sends a combined TA/LA Update with IMSI attach.

This command remains active until it is disabled with the **no sgs vlr-failure** command.

**Important**

This is a licensed feature and is unavailable unless the proper licensed is installed.

**Related Commands:**

- To display VLR failure information and statistics, refer to the **show sgs-service vlr-status full** command.

**Example**

The following enables the monitoring and automatic detach of UEs when any VLR becomes unavailable. The MME will wait 2 minutes (120 seconds) after detecting a VLR condition before starting the controlled release of the affected UEs. The MME will process the UEs over a span of 60 minutes.

```
sgs vlr-failure sgs-service sgs1 duration 60 backoff-timer 120 -noconfirm
```

## sgs vlr-recover

This command enables active recovery of Circuit Switched Fall Back (SMS-only) UEs when a failed VLR becomes responsive again.

<b>Product</b>	MME
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<p><b>[no] sgs vlr-recover sgs-service</b> <i>sgs_svc_name</i> <b>duration</b> <i>minutes</i> <b>backoff-timer</b> <i>seconds</i> [ <b>-noconfirm</b> ]</p> <p><b>no</b></p> <p>Resets the command to its default setting of disabled.</p> <p><b>sgs-service</b> <i>sgs_svc_name</i></p> <p>Specifies the SGs service to which the VLR belongs. <i>sgs_svc_name</i> specifies the name for a pre-configured SGs service.</p> <p><b>duration</b> <i>minutes</i></p> <p>Specifies the amount of time in minutes over which all qualifying UEs will be recovered. The MME splits this duration into <i>n</i> intervals, 5 seconds apart. A maximum of 50 subscribers will be processed per interval per session manager. For example, a setting of 5 minutes with 600 subscribers in a session manager (from a given VLR) would result in the session manager processing 10 subscribers per 5-second interval. Node level detach rate should be estimated by taking into account the number of session manager tasks. Any subscribers remaining at the expiry of the duration will not be processed. <i>minutes</i> must be an integer from 1 through 3000.</p> <p><b>backoff-timer</b> <i>seconds</i></p> <p>Specifies the period of time the MME will wait following the detection of a recovered VLR before starting the VLR recovery actions. <i>seconds</i> must be an integer from 1 to 3000.</p> <p><b>-noconfirm</b></p> <p>Indicates that the command is to execute without additional prompt and confirmation from the user.</p>
<b>Usage Guidelines</b>	When this command is issued, the MME monitors the availability of all VLRs. If a failed VLRs become available again, the MME attempts to recover CSFB (SMS-only) UEs that failed while the VLR was unavailable with an EPS Detach.

**Important**

This is a licensed feature and is unavailable unless the proper licensed is installed.

**Related Commands:**

- To display VLR recovery information and statistics, refer to the **show sgs-service vlr-status full** command.

**Example**

The following enables the active recovery of Circuit Switched Fall Back (SMS-only) UEs when a failed VLR becomes responsive again. The MME will wait 2 minutes (120 seconds) after detecting a recovered VLR before starting the recovery of the affected UEs. The MME will process the UEs over a span of 60 minutes.

```
sgs vlr-recover sgs-service sgs1 duration 60 backoff-timer 120 -noconfirm
```

## sgsn clear-congestion

This command clears (terminates) congestion triggered using the **sgsn trigger-congestion** command.

<b>Product</b>	SGSN
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

<b>Syntax Description</b>	<b>sgsn clear-congestion</b>
---------------------------	------------------------------

<b>Usage Guidelines</b>	This command is only used if the <b>sgsn trigger-congestion</b> command has been issued in an OAM scenario. This <b>sgsn clear-congestion</b> command causes the SGSN to resume normal operations and does not apply any congestion control policy.
-------------------------	---

**Example**

Clear the triggered congestion on the SGSN.

```
sgsn clear-congestion
```

## sgsn clear-detached-subscriptions

Clears subscription data belonging to a subscriber who has already detached.

<b>Product</b>	SGSN
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
sgsn clear-detached-subscriptions imsi imsi
```

**imsi *imsi***

Specifies the international mobile subscriber identity (IMSI) of the subscriber session identifying the subscription data to be cleared.

**Usage Guidelines**

This command can be issued on either a 2G or 3G SGSN to clear subscription data (including subscription information, and information for P-TMSI allocated, received authorization vectors, and NGAF flag values). This command is only effective if the subscriber has already detached.

After the data is purged, the SGSN sends an appropriate message to the HLR.

**Related Commands:**

- To clear subscription data for subscribers that are currently attached, refer to the **admin-disconnect-behavior clear-subscription** commands described in the chapters for *GPRS Service Configuration Mode* or the *SGSN Service Configuration Mode*.

**Example**

```
sgsn clear-detached-subscriptions imsi 040501414199978
```

## sgsn imsimgr

Initiates an audit for managing the SGSN's IMSI manager's (IMSIMgr) IMSI table.

**Important**

These commands are used primarily for troubleshooting purposes and are intended for the use of specially trained service representatives.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
sgsn imsimgr { instance instance_id } { add-record imsi sessmgr instance
sessmgr# | audit-with sessmgr { all | instance sessmgr# } | remove-record
imsi }
```

**instance *instance\_id***

The number of IMSI Managers supported is scaled up to "4" on ASR 5500 and a VPC-DI platforms. This keyword is used to specify the IMSI manager instance for which the audit is initiated. The audit is initiated

from only one specified instance of IMSI Manager at a time. This feature is only supported on ASR5500 and VPC-DI platforms.

*instance\_id*: The *instance\_id* is an integer from 1 through 4, it identifies the IMSI Manager instance for which the audit is initiated.

#### **add-record *imsi***

Adds a record for an IMSI to the IMSI manager's table and associates a specific session manager (SessMgr) with the IMSI.

*imsi*: Enter up to 15 digits. An IMSI consists of the 3-digit MCC (mobile country code) + the 2- or 3-digit MNC (mobile network code) + the MSIN (mobile station identification number) for the remaining 10 or 9 digits (depending on the length of the MNC).

#### **audit-with**

Initiates an IMSI audit with all SessMgrs or a Session Manager (SessMgr) instance specified.

#### **remove-record *imsi***

Deletes a specific IMSI from the IMSI table.

*imsi*: Enter up to 15 digits. An IMSI consists of the 3-digit MCC (mobile country code) + the 2- or 3-digit MNC (mobile network code) + the MSIN (mobile station identification number) for the remaining 10 or 9 digits (depending on the length of the MNC).

#### **sessmgr instance *sessmgr#***

For releases prior to 14.0, this keyword specifies a Session Manager (SessMgr) instance associated with the IMSI as an integer from 0 through 4095.

For releases 14.0 and later, this keyword specifies a Session Manager (SessMgr) instance associated with the IMSI as an integer from 0 through 384.

### **Usage Guidelines**

Use this command to manage the IMSIMgr's IMSI table, and to initiate an audit of one or more SessMgrs with the IMSIMgr so that the IMSI table has the correct IMSI-SessMgr association. After this audit, any IMSI in the IMSIMGR which is not found in any Sessmgr is deleted and similarly any missing entries at the IMSIMgr are created.

#### **Example**

Delete IMSI *044133255524211* from the audit table:

```
sgsn imsimgr remove-record 044133255524211
```

## **sgsn offload**

Instructs the SGSN to begin the offloading procedure and actually starts and stops the offloading of subscribers which is part of the SGSN Gb (2G) or Iu (3G) Flex load redistribution functionality.

### **Product**

SGSN

---

**Privilege** Security Administrator, Administrator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
sgsn offload { gprs-service service_name | sgsn-service service_name } {
activating [ imsi imsi | nri-value nri_value | stop [ imsi imsi | nri-value
nri_value ] ] | connecting [ nri-value nri_value | stop [ imsi imsi |
nri-value nri_value | target-nri target_nri ] | t3312-timeout seconds [
nri-value nri_value | target-nri target_nri ] | target-nri target_nri [ imsi
imsi | target-count num_to_offload ] }
```

**gprs-service *svc\_name***

Specifies a unique alphanumeric string of 1 through 63 characters that identifies a GPRS service that has already been defined for the 2G SGSN configuration.

**sgsn-service *svc\_name***

Specifies a unique alphanumeric string of 1 through 63 characters that identifies an SGSN service that has already been defined for the 3G SGSN configuration.

**activating**

Instructs the SGSN to off load any subscribers sending an "activate request" message.

**connecting**

Instructs the SGSN to off load any subscribers sending either an Attach Request or a RAU Request message. Including this keyword without adding the **target-nri** and **target-count** keywords activates local offloading.

**imsi *imsi***

Identifies a subscriber by the international mobile subscriber ID (IMSI) which consists of the 3-digit MCC (mobile country code) + the 2- or 3-digit MNC (mobile network code) + the MSIN (mobile station identification number) for the remaining 10 or 9 digits (depending on the length of the MNC).

*imsi*- enter an integer comprising up to 15 digits.

**nri-value *nri\_value***

Sets the local NRI. Including this keyword in the configuration instructs the SGSN to check the P-TMSI and use the SGSN matching the configured NRI value to off load subscribers.




---

**Important** **nri-value** and **target-nri** are mutually exclusive.

---

*nri\_value* is an integer from 1 through 63 that identifies a specific, already defined, SGSN in a pool. (NRI defined in the service configuration.)

Use of 0 (zero) value is not recommended.

**stop**

Instructs the SGSN to stop offloading subscribers from the pool area.

**target-nri *target\_nri***

Instructs the SGSN to begin dynamically load balancing across a network of pooled SGSNs.

*target\_nri* is an integer from 0 through 63 that identifies an already defined target NRI (SGSN) to which the subscribers are to be offloaded. (NRI previously defined in the service configuration.)

Use of 0 (zero) value is not recommended.

**target-count *target\_count***

Identifies the number of subscribers to be offloaded as an integer from 0 through 4000000. Instructs the SGSN to begin target count-based offloading.

**t3312-timeout *seconds***

Sets the timer (in seconds) for sending period RAUs to the MS as an integer from 2 through 60. Default: 4

**Usage Guidelines**

Use this command to configure the offloading of subscribers which is a part of the SGSN's load redistribution operation. This command can be used anytime an SGSN is to be taken out of service.

Commands, with different NRI values, are repeated to expand/contract the radius of the offloading.

Target count-based offloading and local offloading can not run simultaneously. When target count offloading is to be used, you should choose an algorithm to control offloading from the perspective of the IMSIMGR and SESSMGR. This is done with the **target-offloading** command in the SGSN-Global configuration mode.

**Example**

The following two commands initiate **local offloading**.

Command 1: The following command instructs the SGSN to begin local offloading for the local NRI *id 1* included in the *gprs1* GPRS service configuration:

```
sgsn offload gprs-service gprs1 connecting nri-value 1
```

Command 2: Enter this second command to add offloading for NRI 2 to the offloading already occurring for NRI 1:

```
sgsn offload gprs-service gprs1 connecting nri-value 2
```

The following two commands discontinue local offloading and initiate **target count-based offloading**.

Command 1: The following command instructs the SGSN to discontinue local offloading for NRIs 5 included in the *sgnserv4* SGSN service configuration :

```
sgsn offload sgsn-service sgnserv4 connecting stop nri 5
```

**Important**

The next command is an example of provision configuration for multiple NRI with a single command.

Command 2: The following command instructs the SGSN to initiate target count-based offloading for target NRI 5 to a target count of 10000 and target NRI 6 to count of 300000:



```
sgsn offload sgsn-service sgsnserv4 connecting target-nri 5 target-count
100000 target-nri 6 target-count 300000
```

## sgsn op

Instructs the SGSN to begin specific operations or functions.

---

### Product

SGSN

---

### Privilege

Security Administrator, Administrator

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

```
sgsn op { auth-ptmsi-counters imsi imsi | convert | nse { fr | ip |  
sgsn-invoke-trace } | show | ss7-rd ss7-rd_id { destination | link | linkset  
| peer } }
```

#### **auth-ptmsi-counters imsi *imsi***

Displays the authentication, P-TMSI reallocation, and P-TMSI signature reallocation counters for the specified IMSI.

*imsi*: Enter a unique 15-digit number associated with a mobile phone.

#### **convert point-code *pt\_code* variant *variant***

Converts SS7 point codes, according to identified variants, from dotted-decimal format to decimal format and vice versa.

**point-code *pt\_code***: Enters an SS7 point code in either dotted-decimal format or decimal format.

**variant *variant***: Identifies the appropriate variant for the point code:

- **ansi**
- **itu**
- **ttc**

#### **nse { fr *operation* | ip *operation* | sgsn-invoke-trace nse-id *nse\_id* }**

Enables the operator to perform a range of live control functions (for example, reset, block, unblock) for various types of virtual connections based on the signalling type of the NSE:

**fr**: Identifies a Frame Relay NSE.

**ip**: Identifies an IP NSE.

*operation*: Identifies the operation to be performed for the NSE connection (if available for the selected signalling type):

- **block nse-id** *nse\_id*: Blocks signal flow through all network service virtual connections (NSVC) for the specified NSE:
  - *nse\_id*: an integer from 0 to 65535.
- **bvc-flc-limit rate** *rate* **bvc-id** *bvc\_id* **nse-id** *nse\_id* - SGSN initiates flow control at the defined percentage rate to limit the flow through the BSSGP virtual connection (BVC) for the specified NSE and optionally for a specified BVC.
  - *rate*: an integer from 0 to 100.
  - *bvc\_id*: an integer from 0 to 65000.
  - *nse\_id*: an integer from 0 to 65535.
- **bvc-reset** **bvc-id** *bvc\_id* **nse-id** *nse\_id*: SGSN initiates a BVC-Reset on the specified BVC and NSE:
  - *bvc\_id*: an integer from 0 through 65000.
  - *nse\_id*: an integer from 0 through 65535.
- **nsvc** *nsvc\_id* { **block** | **enable** | **disable** | **unblock** } *nse\_id* - SGSN initiates NS-Block or NS-Unblock for the specified NSVC of the specified NSE:
  - *nsvc\_id*: an integer from 0 through 65535.
  - *nse\_id*: an integer from 0 through 65535.
- **reset nse-id** *nse\_id* - SGSN initiates NS-Reset for all NSVC configured in the NSE. *nse\_id* is an integer from 0 through 65535.
- **unblock nse-id** *nse\_id* - SGSN initiates NS-Unblock for all NSVC configured for the specified NSE. *nse\_id* is an integer from 0 through 65535.

**sgsn-invoke-trace** **nse-id** *nse\_id* **record-type** *record\_type* **trace-reference** *reference* [ **mobile-id** *id\_type* | **trace-transaction-id** *trace\_id* ] :



#### Important

This command can be used for troubleshooting/debugging purposes and is primarily intended for the use of specially trained service representatives.

Instructs the SGSN (1) to send the BSSGP message SGSN-INVOKE-TRACE to the BSC to initiate a BSC trace of a particular MS and (2) to define the type and triggering of the trace.

- *nse\_id*: Identifies the peer NSE, enter an integer from 0 to 65535.
- *record\_type*: Specifies the type of trace to be performed:
  - **basic**
  - **handover**
  - **no-bss-trace**
  - **radio**

- **trace-reference** *reference* : Specifies the trace reference ID as an integer from 0 to 65535.
- **mobile-id type** *id\_type*: Select the appropriate mobile ID type for the MS that is to be traced:
  - **imei value** *value* - Specifies the mobile ID type as the unique International Mobile Equipment Identity.  
*value*: 15-digit IMEI value.
  - **imeisv value** *value*: Specifies the mobile ID type as the unique International Mobile Equipment Identity with the two-digit software version number.  
*value*: 16-digit IMEISV value.
  - **imsi value** *value* - Specifies the mobile ID type as a network unique International Mobile Subscriber Identity as a 15-digit IMSI value.
- **trace-transaction-id** *trace\_id*: Specifies the trace transaction ID as an integer from 0 through 65535.

### show plmn-list smgr-inst *sessmgr#*



#### Important

This function is only available in release 8.1.

SGSN displays the configured PLMN list for the specified session manager (SessMgr):

*sessmgr#*: Enter up to 4 digits, 0 to 4095.

### ss7-rd *ss7-rd\_id*{ **destination** | **link** | **linkset** | **peer** }

The **ss7-rd** commands assist with troubleshooting connections between the SGSN and the peer server.

*ss7-rd\_id*: Specifies the configured SS7 routing domain as an integer from 1 through 12.

- **destination audit asp-instance** *asp\_id* **peer-server-id** *peer\_id* **psp-instance-id** *psp\_id*  
Initiates destination audit (DAUD) messages for all point codes reachable via the identified peer-server, which is in restricted/unavailable/congested state due to DRST/DUNA/SCON messages respectively from the far end.
  - *asp\_id*: Specifies the relevant ASP configuration ID as an integer from 1 through 4.
  - *peer\_id*: Specifies the relevant peer server configuration ID as an integer from 1 through 144.
  - *psp\_id*: Specifies the relevant PSP configuration ID as an integer from 1 through 4
- **link procedure linkset-id** *linkset\_id* **link-id** *link\_id*  
Initiates MTP3 network link management procedures for the specified link:
  - **activate**: Activates the deactivated link.
  - **deactivate**: Deactivates specified link.
  - **deactivate-l2-only**: Deactivates the link only at the MTP3 layer.
  - **inhibit**: Inhibits the link only if it does *not* make any destination unreachable.

- **uninhibit**: Uninhibits the inhibited link.
- *linkset\_id*: an integer between 1 and 144.
- *link\_id*: an integer between 1 and 16.
- **linkset-id procedure linkset-id linkset\_id**  
Initiates MTP3 network link management procedures for all the links in the specified linkset:
  - **activate**: Activates the deactivated linkset.
  - **deactivate**: Deactivates the linkset.
  - **deactivate-l2-only**: Deactivates the linkset only at MTP3 layer.
  - *linkset\_id*: an integer between 1 and 144.
- **peer message asp-instance asp\_id peer-server-id peer\_id psp-instance-id psp\_id**  
Initiates one of the following SCTP/M3UA management messages from the identified link:
  - **abort**: Sends an SCTP Abort message which aborts the SCTP association ungracefully.
  - **activate**: Sends an M3UA ASP Active message to activate the link.
  - **down**: Sends an M3UA ASP Down message to bring down the M3UA link.
  - **establish**: Sends an SCTP INIT message to start the SCTP association establishment.
  - **inactivate**: Sends an M3UA ASP Inactive message to deactivate the link.
  - **inhibit**: Inhibits the M3UA link locally when the operator wants to lockout the link.
  - **terminate**: Sends SCTP Shutdown message which closes the SCTP association gracefully.
  - **un-inhibit**: Uninhibits the M3UA link.
  - **up**: Sends an M3UA ASP UP message to bring up the M3UA link.
  - *asp\_id*: Specifies a relevant ASP configuration ID as an integer from 1 through 4.
  - *peer\_id*: Specifies the relevant peer server configuration ID as an integer from 1 through 144.
  - *psp\_id*: Specifies the relevant PSP configuration ID as an integer from 1 through 4.

### Usage Guidelines

In most cases, an operator will block/unblock/reset from the BSC-side. The **nse** commands cause the SGSN to initiate actions, usually for one of the following reasons:

- to resolve issues on the BSC-side,
- as part of an upgrade to the BSC,
- as part of link expansion,
- to resolve NSVC/BVC status mismatches observed between the SGSN and BSC.

The **sgsn-invoke-trace** command initiates the trace procedure where the BSC begins a trace record on a specified MS.

**Example**

The following command instructs the SGSN to initiate an NS-Block for all NSVC associated with Frame Relay NSE ID 2422:

```
sgsn op nse fr unblock nse-id 2422
```

Activate linkset *I* configured in SS7 routing domain *I*:

```
sgsn op ss7-rd 1 linkset activate linkset-id 1
```

## sgsn retry-unavailable-ggsn

Marks the GGSN as available for further activation.

<b>Product</b>	SGSN
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec
	The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<b>sgsn retry-unavailable-ggsn</b> <i>ip_address</i>

***ip\_address***

Specifies the IP address of a GGSN in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

<b>Usage Guidelines</b>	This command allows the operator to directly inform both the session manager and the SGTPC manager that the GGSN has been removed from a blacklist and is now available for activations. This action would override the GGSN blacklist timer configuration with <b>ggsn-fail-retry-timer</b> in the SGTP service configuration mode.
-------------------------	--

**Example**

The following command indicates that the GGSN identified by its IP address is now available for activation:

```
sgsn retry-unavailable-ggsn 198.168.128.8
```

## sgsn trigger-congestion

This command triggers a congestion state for the entire SGSN for operations and maintenance purposes (e.g., testing).

<b>Product</b>	SGSN
----------------	------

<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<b>sgsn trigger-congestion level { critical   major   minor }</b>  <b>critical   major   minor</b> Select one of the three congestion severity levels. Each level is associated with congestion threshold settings and a congestion-action-profile.
<b>Usage Guidelines</b>	Use the <b>sgsn clear congestion</b> to disable congestion simulation and return to normal operations. Use the <b>show congestion-control configuration</b> command to display the SGSN's congestion-control policy with the congestion-action-profile name association with the level of congestion severity.
<b>Example</b>	Enable critical congestion control response testing with the following command: <b>sgsn trigger-congestion level critical</b>

## sgtpc test echo sgsn-address

Initiates SGTPC echo test procedure.

<b>Product</b>	SGSN
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<b>sgtpc test echo sgsn-address</b> <i>sgsn_ip_address</i> { <b>all</b>   <b>ggsn-address</b> <i>ggsn_ip_address</i> }  <b>sgsn-address</b> <i>sgsn_ip_address</i> Identifies the IP address of the SGSN issuing the test in IPv4 dotted-decimal notation.  <b>all</b> Sends GTPC echo requests to all GGSNs having current sessions with the SGTP service.

**ggsn-address ggsn\_ip\_address**

Sends a GTPC echo request to the specified GGSN whether or not the GGSN has active sessions with the SGTP service. *ggsn\_ip\_address* is entered using IPv4 dotted-decimal notation.

**Usage Guidelines**

This command initiates a test for the GTPC echo procedure -- echo from the specified SGSN to a specified GGSN or to all GGSNs that have sessions with the SGTP service. Issue the command from the Exec Mode within the context in which the SGTP service is configured.

Note that if the GGSN does not respond to the initial echo request, the echo requests will be retried for the max-retransmissions times.

**Example**

This SGSN with IP address of *10.1.1.1* sends an echo test to all GGSNs attached to the SGTP service:

```
sgtpc test echo ggsn-address 10.1.1.1 all
```

# shutdown

Terminates all processes within the chassis. After all processes are terminated, the system initiates a hardware reset (reboot). This command is identical to the **reload** command.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
shutdown [ ignore-locks ] [ -noconfirm ]
```

**ignore-locks**

Reboots the system regardless of any save configuration operations that may be currently running. StarOS displays a warning message but does not wait for save configuration requests to complete before initiating the reboot.

Warning: One or more other administrators are saving configuration

**Caution**

Use of the **ignore-locks** keyword may result in file corruption.

**-noconfirm**

Executes the command without any additional prompts or confirmation from the user.

**Usage Guidelines**

The system performs a hardware reset and reloads the highest priority boot image and configuration file specified in the `boot.sys` file. Refer to the **boot system priority** command in the Global Configuration Mode for additional information on configuring boot images, configuration files and priorities.

By default (without the **ignore-locks** option specified) **shutdown** waits for save configuration operations to complete before initiating the reboot.

**Important**

To avoid the abrupt termination of subscriber sessions, it is recommended that a new call policy be configured and executed prior to invoking the **shutdown** command. This policy sets busy-out conditions for the system and allows active sessions to terminate gracefully. Refer to the **newcall** command in the Exec Mode for additional information.

**Caution**

Issuing this command causes the system to become unavailable for session processing until the reboot process is complete.

**Example**

The following command performs a hardware reset on the system:

```
shutdown
```

# sleep

Pauses the command line interface (CLI).

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
sleep seconds
```

**sleep seconds**

Specifies the number of seconds to pause as an integer from 1 through 3600.

**Usage Guidelines**

Sleep is a command delay which is only useful when creating command line interface scripts such as predefined configuration files/scripts.

**Example**

The following will cause the CLI to pause for 30 seconds.



```
sleep 30
```

## srp disable

Disables the sending of a NACK from a standby ICSR chassis.

---

### Product

All products that support ICSR

---

### Privilege

Security Administrator, Administrator, Operator, Inspector

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

```
srp disable nack micro-chkpt-cmd chkpt_number [ -noconfirm ]
```

#### ***chkpt\_number***

Specifies the checkpoint number to be disabled as an integer from 1 through 255. You can obtain checkpoint numbers (CMD ID) via the output of the **show srp checkpoint info** command.

#### **-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

---

### Usage Guidelines

Use this command to disable the sending of NACK messages from the standby chassis that trigger a full checkpoint from the active chassis. Sending full checkpoints increases SRP bandwidth. This command disables the NACK feature for a specific micro-checkpoint which is failing continuously.

You can re-enable the micro-checkpoint using the **srp enable nack micro-chkpt-cmd** command.

### Example

The following command disables CMD ID 9 (SESS\_UCHKPT\_CMD\_UPDATE\_L2TPLNSSTATS).

```
srp disable nack micro-chkpt-cmd 9
```

## srp enable

Enables the sending of a previously disabled NACK from a standby ICSR chassis.

---

### Product

All products that support ICSR

---

### Privilege

Security Administrator, Administrator, Operator, Inspector

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**    **srp enable nack micro-chkpt-cmd** *chkpt\_number* [ **-noconfirm** ]

***chkpt\_number***

Specifies the checkpoint number to be enabled as an integer from 1 through 255. You can obtain checkpoint numbers (CMD ID) via output of the **show srp checkpoint info** command.

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

---

**Usage Guidelines**    Use this command to enable the sending of previously disabled NACK messages from the standby chassis. This command enables the NACK feature for a specific micro-checkpoint.

You can disable a micro-checkpoint using the **srp disable nack micro-chkpt-cmd** command.

**Example**

The following command enables CMD ID 9 (SESS\_UCHKPT\_CMD\_UPDATE\_L2TPLNSSTATS).

```
srp enable nack micro-chkpt-cmd 9
```

## srp initiate-audit

Initiates an SRP audit between active and standby ICSR chassis.

---

**Product**    All products that support ICSR

---

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

---

**Command Modes**    Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**    **srp initiate-audit manual-with-sync**

---

**Usage Guidelines**    When issued from the active chassis, this command initiates a forced audit between ICSR chassis. This audit ensures that two ICSR peers are synchronized and identifies any discrepancies prior to scheduled or unscheduled switchover events.

**Example**

The following command initiates a forced audit between ICSR chassis.

```
srp initiate-audit manual-with-sync
```

# srp initiate-switchover

Changes the device status on the primary and backup chassis configured for Interchassis Session Recovery (ICSR) support employing Service Redundancy Protocol (SRP).

<b>Product</b>	All products that support ICSR
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `srp initiate-switchover [ force | post-processing-timeout | reset-route-modifier | timeout seconds ] [ -noconfirm ]`



## Important

For release 20.0 and higher, ICSR will verify session manager connectivity on both chassis prior to allowing a manual switchover. If one or more of the session managers in the active chassis is not connected on the standby chassis, the switchover will not be initiated. An error message will appear on the screen noting the number of session managers that are mismatched. The **force** keyword can be used to initiate the switchover despite the mismatch(es). The output of the **show checkpoint statistics verbose** command will not indicate "Ready" for a session manager instance ("smgr inst") in the "peer conn" column for any instance that is not connected in the standby chassis.

### force

Switchover by force, without any validating checks.

### post-processing-timeout

Specifies the timeout value (in seconds) to initiate the post-switchover process as an integer from 0 through 3600.

### reset-route-modifier

During a switchover, resets the route-modifier to the initial value.

### timeout *seconds*

Specifies the number of seconds before a forced switchover occurs as an integer from 0 through 65535. Default: 300

### -noconfirm

Executes the command without any additional prompt and confirmation from the user.

## Usage Guidelines

This command executes a forced switchover from active to inactive. The command must be executed on the active system and switches the active chassis to the inactive state and the standby system to an active state.

The switchover will be blocked if one or more session managers are not connected on the standby chassis. The **force** keyword will initiate the switchover despite any session manager mismatches.

### Example

The following initiates a switchover in 30 seconds.

```
srp initiate-switchover timeout 30
```

## srp reset-auth-probe-fail

Resets Service Redundancy Protocol (SRP) authentication probe monitor failure information.

**Product** All products that support Interchassis Session Recovery (ICSR)

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

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **srp reset-auth-probe-fail**

**Usage Guidelines** This command resets the auth probe monitor failure information to 0.

### Example

The following command resets the auth probe monitor failure information to 0:

```
srp reset-auth-probe-fail
```

## srp reset-diameter-fail

Resets Service Redundancy Protocol (SRP) Diameter monitor failure information.

**Product** All products that support Interchassis Session Recovery (ICSR)

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

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **srp reset-diameter-fail**

**Usage Guidelines** This command resets the Diameter monitor failure information to 0.

**Example**

The following command resets the SRP Diameter monitor failure information:

```
srp reset-diameter-fail
```

## srp reset-sx-fail

Resets the Service Redundancy Protocol (SRP) Sx monitor failure information.

<b>Product</b>	All products that support Interchassis Session Recovery (ICSR)
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<b>srp reset-diameter-fail</b>
<b>Usage Guidelines</b>	This command resets the Sx monitor failure information.

## srp terminate-post-process

Forcibly terminates post-switchover processing by primary and backup chassis configured for Interchassis Session Recovery (ICSR) support employing Service Redundancy Protocol (SRP).

<b>Product</b>	All products that support ICSR
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<b>srp terminate-post-process [ -noconfirm ]</b>  <b>-noconfirm</b> Executes the command without any additional prompt and confirmation from the user.
<b>Usage Guidelines</b>	Use this command to force the termination of post-switchover processing.

**Example**

```
srp terminate-post-process
```

## srp validate-configuration

Initiates a configuration validation check from the active chassis via Service Redundancy Protocol (SRP).

**Product** All products that support Interchassis Session Recovery (ICSR)

**Privilege** Security Administrator, Administrator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **srp validate-configuration**

**Usage Guidelines** Validates the configuration for an active chassis.

### Example

The following command initiates a configuration validation check from the active chassis:

```
srp validate configuraiton
```

## srp validate-switchover

Validates that both the active and standby chassis are ready for a planned Service Redundancy Protocol (SRP) switchover.

**Product** All products that support Interchassis Session Recovery (ICSR)

**Privilege** Security Administrator, Administrator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **srp validate-switchover**

**Usage Guidelines** Validates that both the active and standby chassis are ready for a planned SRP switchover.

### Example

The following example performs SRP readiness validation on both ICSR chassis:

```
srp validate switchover
```

# ssh

Connects to a remote host using a secure shell (SSH) interface.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator, Operator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
ssh { host_name | host_ip_address } [ port port_num ] [ user user_name ]
```

***host\_name* | *host\_ip\_address***

Identifies the remote node with which to attempt connection.

*host\_name*: specifies the remote node using its logical host name which must be resolved via DNS lookup. This is an alphanumeric string of 1 through 127 characters.

*host\_ip\_address*: specifies the remote node using its assigned IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

***port port\_num***

Specifies a specific port for connection as an integer from 1 through 65535. Default = 22

***user user\_name***

Specifies the user name attempting connection as an alphanumeric string from 1 through 1024 characters.

---

**Usage Guidelines**

SSH connects to a remote network element using a secure interface.

**Example**

The following connects to remote host *remoteABC* as user *user1*.

```
ssh remoteABC user user1
```

The following connects to remote host *10.2.3.4* without any default user.

```
ssh 10.2.3.4
```

The following connects to remote host *10.2.3.4* via port *2047* without any default user.

```
ssh 10.2.3.4 port 2047
```

## start crypto security-association

Initiates Internet Key Exchange (IKE) negotiations.

<b>Product</b>	PDSN HA GGSN
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec  The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<b>start crypto security-association</b> <i>cryptomap</i>  <b>cryptomap</b>  Specifies the name of an existing crypto map policy to use when starting the IKE negotiations as an alphanumeric string of 1 through 127 characters.
<b>Usage Guidelines</b>	Use this command to start IKE negotiations for IPsec.

**Example**

The following command starts the IKE negotiations using the parameters set in the crypto map named *cryptomap1*:

```
start crypto security-association cryptomap1
```

## statistics-collection

This command allows to dynamically enable collection of Charging, Firewall or Post-processing ruledef statistics.

<b>Product</b>	ACS
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec  The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<b>statistics-collection active-charging</b> { { <b>all</b>   <b>charging</b>   <b>firewall</b>   <b>post-processing</b> } { <b>callid</b> <i>call_id</i>   <b>imsi</b> <i>imsi_number</i> } } [ <b>no</b> ] <b>statistics-collection active-charging</b> { <b>callid</b> <i>call_id</i>   <b>imsi</b> <i>imsi_number</i> }  <b>no</b>  If previously configured, deletes the specified rule expression from the current ruledef.



**all | charging | firewall | post-processing**

- **all**: Specifies to collect all ruledef statistics.
- **charging**: Specifies to collect charging ruledef statistics.
- **firewall**: Specifies to collect firewall ruledef statistics.
- **post-processing**: Specifies to collect post-processing ruledef statistics.

**callid *call\_id***

Specifies a call identification number as an eight-byte hexadecimal number.

**imsi *imsi\_number***

Specifies the IMSI number to match.

*imsi\_number* must be a sequence of digits.

**Usage Guidelines**

Use this command to dynamically enable collection of ruledef statistics — Charging, Firewall or Post-processing. By default, the statistics will not be maintained. If the command is not configured, statistics collection will not be enabled and the following error message will be displayed in the **show active-charging sessions full** CLI — "statistics collection disabled; not collecting <charging/firewall/postprocessing> ruledef stats".

**Example**

The following command will collect firewall ruledef statistics with call ID set to *004c9961*:

```
statistics-collection active-charging firewall callid 004c9961
```

## system packet-dump

Initiates a packet dump on an SF or CF card in a VPC-DI system.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
system packet-dump { di-net card slot_num | port service_port } [ bond { a | b } | direction { both-rxtx | rx | rxtx | tx } | duration seconds | packet-type { ipv4 | ipv6 } | pcapfile-size size | pcapfile-split-value | protocol { icmpv4 | icmpv6 | tcp | udp } | to file filename ]
```

**di-net card *slot\_num***

Specifies the card from 1 through *n*.

**port *card\_port/port\_num***

Specifies the ethernet interface based on the card number from 1 through *n* and port number from 1 through 50, for example 3/1.

**bond { *a* | *b* }**

Specifies a slave for bonded interfaces.

**direction { both-rxtx | rx | rxtx | tx }**

Specifies a filter for the direction of the packets to capture, either receive (**rx**), transmit (**tx**), or both (**rxtx**). Use the **both-rxtx** option to capture both receive and transmit, but output each to separate files.

**duration *seconds***

Specifies the number of seconds from 1 through 600 for the packet dump. Default: 5 seconds

**packet-type { ipv4 | ipv6 }**

Specifies a filter for the type of the packets to capture, either **ipv4** or **ipv6**.

**pcapfile-size *size***

Specifies the maximum size for each packet capture (pcap) file from 10 to 800 megabytes. Default: 10 megabytes.

**pcapfile-split-val *value***

Specifies the number of pcap files to generate for a given capture from 0 to 10. Default: 0 (do not split files).

**protocol { icmpv4 | icmpv6 | tcp | udp }**

Specifies a filter for the protocol of the packets to capture, either **icmpv4**, **icmpv6**, **tcp**, or **udp**.

**to file { /flash | /hd-raid | /cdrom1 | /sftp } [/directory]/ *filename***

Specifies the output location and filename.

**Usage Guidelines**

Use this command to perform packet captures to troubleshoot issues within a VPC-DI deployment.

**Example**

The following command initiates a packet dump on card in slot 7, port 1, and output the dump to a file stored locally at /flash/example7-1.pcap

```
system packet-dump port 7/1 to file /flash/example7-1.pcap
```

## system ping

Initiates a ping test on the internal network between two VMs within the VPC-DI system.

<b>Product</b>	VPC-DI
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<p><b>system ping from card</b> <i>slot_num</i> <b>to card</b> <i>slot_num</i> [ <b>count</b> <i>number_of_packets</i>   <b>size</b> <i>bytes</i> ]</p> <p><b>from card</b> <i>slot_num</i> Specifies the card slot number from 1 through <i>n</i> from which the ping test originates.</p> <p><b>to card</b> <i>slot_num</i> Specifies the destination card slot number from 1 through <i>n</i>.</p> <p><b>count</b> <i>number_of_packets</i> Sets the number of ping packets from 1 through 10000 to be sent. Default: 5 packets</p> <p><b>size</b> <i>bytes</i> Sets the size of the ICMP Datagram in bytes from 40 to 18432. Default: 56</p>
<b>Usage Guidelines</b>	Use this command to perform ping tests to troubleshoot connectivity issues within a VPC-DI deployment.

**Example**

The following command initiates a ping test of 1000 packets from the card in slot 1 to the card in slot 9:

```
system ping from card 1 to card 9 count 1000
```

## system ssh

Manages the persistent ssh user keys used for the internal ssh sessions between cards (VMs) in a VPC-DI system.

<b>Product</b>	VPC-DI
<b>Privilege</b>	Security Administrator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>

**Syntax Description**

```
system ssh key { copy boot1 to card slot_num | create boot1 }
no system ssh key boot1 { all | card slot_num }
```

**no system ssh key boot1 { all | card *slot\_num* }**

Deletes the persistent ssh keys on a specific card or all cards in the VPC-DI system. Deletion of keys may be used to purge a VM of the persistent keys or prepare the system for using a different distribution method (ESC, OpenStack, attached ISO).

- **all** : Deletes the ssh keys on all cards in the VPC-DI system.
- **card *slot\_num*** : Deletes the ssh keys on the card specified by *slot\_num* .

**Note**

This command does not affect the VM until it is rebooted. It will continue to use the active key found during its boot.

**copy boot1 to card *slot\_num***

Transfers the persistent ssh keys (both public and private) in /boot1 on the active CF to another VM. That VM must be in a state to accept it by a user with console access placing it in receiver mode during its failed boot.

**create boot1**

Creates new persistent ssh keys (both public and private) and stores it in /boot1 on the active CF.

**Note**

This command does not affect the VM until it is rebooted. It will continue to use the active key found during its boot.

**Usage Guidelines**

Use this command to manage the internal ssh keypairs in a VPC-DI deployment. While StarOS provides sshd services for user CLI and SFTP sessions on the management VMs (CF), another set of sshd services run for the exclusive use of internal communication between all component VMs, such as for remote command execution and file transfers. This internal sshd is only used on the internal DI-network interface.

This command enables you to store and manage ssh keys on the VM's virtual hard disk drive (HDD). This provides an alternate option for storing ssh keypairs besides the other methods such as Cisco Elastic Services Controller (ESC), OpenStack, or a directly attached ISO. The /boot1 partition is only accessible by a security administrator.

Use the **show system ssh key status** command to display the fingerprint of the current public key in use, the origin of where the key was found, and the status of all online VMs.

**Example**

The following command copies the ssh keypairs from the active CF to the card in slot 12

```
system ssh key copy boot1 to card 12
```



## CHAPTER 18

# Exec Mode Commands (T-Z)

The Exec Mode is the initial entry point into the command line interface system. Exec mode commands are useful in troubleshooting and basic system monitoring.

### Command Modes

This section includes the commands **telnet** through **upgrade url-blacklisting database**.

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```



### Important

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

- [tcpdump kernel](#), on page 552
- [telnet](#), on page 552
- [telnet6](#), on page 553
- [terminal](#), on page 554
- [test alarm](#), on page 555
- [test ggsn vapn](#), on page 556
- [test ipcf bindmux](#), on page 556
- [test ipsec tunnel ip-pool](#), on page 557
- [test mobile tunnel](#), on page 558
- [timestamps](#), on page 559
- [traceroute](#), on page 560
- [traceroute6](#), on page 562
- [update active-charging](#), on page 563
- [update firewall policy](#), on page 566
- [update ip access-list](#), on page 566
- [update ipv6 access-list](#), on page 567
- [update ip-pool apn](#), on page 568
- [update local-user database](#), on page 569
- [update module](#), on page 570
- [update qos policy map](#), on page 570
- [update qos tft](#), on page 571

- [update security](#), on page 572
- [upgrade content-filtering](#), on page 573
- [upgrade database](#), on page 574
- [upgrade tethering-detection](#), on page 574
- [upgrade url-blockedlisting database](#), on page 575

## tcpdump kernel

Runs the tcpdump packet analyzer and prints out a description of the contents of packets on a specified network interface that match the boolean expression.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `tcpdump kernel` *string*

### *string*

Specifies an existing interface match string as an alphanumeric string of 0 through 80 characters.

**Usage Guidelines** Runs the tcpdump packet analyzer and prints out a description of the contents of packets on a specified network interface that match the boolean expression. This analyzer performs a sniff operation at the mc dma0 interface using the kernel BIA (Bump-in-the-API) as a filter. This allows sniffing of kernel traffic complete with midplane header.



**Important** The `tcpdump kernel` command is not available in Trusted builds.

### Example

The following command initiates a tcpdump for the default kernel interface:

```
tcpdump BPPP
```

## telnet

Connects to a remote host using the terminal-remote host protocol and a hostname or IPv4 address and port number.

<b>Product</b>	All
----------------	-----

<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<b>telnet</b> { <i>host_name</i>   <i>host_ipv4_address</i> } [ <b>port</b> <i>port_num</i> ]  <b><i>host_name</i> / <i>host_ipv4_address</i></b> Identifies the remote node with which to attempt connection. <i>host_name</i> : specifies the remote node using its logical host name which must be resolved via DNS lookup. <i>host_ipv4_address</i> : specifies the remote node using its assigned IP address entered using the IPv4 dotted-decimal notation.  <b>port <i>port_num</i></b> Specifies a specific port for connect connection as an integer from 1025 through 10000.
<b>Usage Guidelines</b>	Telnet to a remote node for maintenance activities and/or troubleshooting when unable to do so directly.

**Important**

**telnet** is not a secure method of connecting between two hosts. **ssh** should be used whenever possible for security reasons.

**Example**

The following connects to remote host *remoteABC*.

```
telnet remoteABC
```

The following connects to remote host *10.2.3.4* port *2047*.

```
telnet 10.2.3.4 port 2047
```

## telnet6

Connects to a remote host using the terminal-remote host protocol and a hostname or an IPv6 address and port number.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>

---

**Syntax Description** `telnet6 { host_name | host_ipv6_address } [ port port_num ]`

***host\_name* | *host\_ipv6\_address***

Identifies the remote node with which to attempt connection.

*host\_name*: specifies the remote node using its logical host name which must be resolved via DNS lookup.

*host\_ipv6\_address*: specifies the remote node using its assigned IP address entered using the IPv6 colon-separated-hexadecimal notation.

**port *port\_num***

Specifies a specific port for connect connection as an integer from 1025 through 10000.

---

**Usage Guidelines** Telnet to a remote node for maintenance activities and/or troubleshooting when unable to do so directly.



**Important**

`telnet6` is not a secure method of connecting between two hosts. `ssh` should be used whenever possible for security reasons.

---

**Example**

The following connects to remote host *remoteABC*.

```
telnet6 remoteABC
```

The following connects to remote host *FE80::172.30.67.89* port *2047*.

```
telnet6 FE80::172.30.67.89 port 2047
```

## terminal

Sets the number of rows or columns for display output.

---

**Product** All

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `terminal { length lines | width characters }`

**length *lines* | width *characters***

**length *lines***: sets the terminal length in number of lines (rows) of text from 5 to 4294967295 lines or the special value of 0 (zero). The value 0 sets the terminal length to infinity.

**width *characters***: sets the terminal width in number of characters from 5 to 512 characters.



**Usage Guidelines**

Set the length to 0 (infinite) when collecting the output of a command line interface session which is part of a scripted interface.

**Example**

The following sets the length then width in two commands.

```
terminal length 66
terminal width 160
```

The following command sets the number of rows of the terminal to infinity.

```
terminal length 0
```

## test alarm

Tests the alarm capabilities of the chassis.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
test alarm { audible | central-office { critical | major | minor } }
```

**audible | central-office { critical | major | minor }**

**audible:** Tests the internal alarm on the ASR 5500 System Status Card (SSC) for 10 seconds. The alarm status is returned to its prior state, such as if the audible alarm was enabled prior to the test, the alarm will again be enabled following the test.

**central-office { critical | major | minor }:** Tests the specified central office alarm type.

**Usage Guidelines**

Test the alarm capabilities of the chassis as periodic maintenance to verify the hardware for generation of the internal audible alarms is functional.

**Caution**

The use of test commands could adversely affect the operation of your system. It is recommended that they only be used under the guidance and supervision of qualified support representative.

**Example**

```
test alarm audible
test alarm central-office critical
test alarm central-office major
test alarm central-office minor
```

## test ggsn vapn

Tests for Virtual Access Point Names (VAPNs) in GGSN networks.

<b>Product</b>	GGSN
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `test ggsn vapn { msisdn range | imsi range }`

### msisdn range | imsi range

**msisdn range:** Tests VAPNs within a range of previously specified Mobile Subscribers Integrated Services Digital Network (MSISDN) identifiers.

**imsi range:** Tests VAPNs within a range of previously specified International Mobile Subscriber Identity (IMSI) numbers.

**Usage Guidelines** Test for the existence of VAPNs associated with MSISDN or IMSI numbers.



#### Caution

The use of test commands could adversely affect the operation of your system. It is recommended that they only be used under the guidance and supervision of qualified support representative.

### Example

```
test ggsn vapn msisdn range
test ggsn vapn imsi range
```

## test ipcf bindmux

Tests the status of the Intelligent Policy Control Function (IPCF) BindMux Manager instance and also starts or stops the BindMux Manager instance on the chassis.

<b>Product</b>	IPCF
<b>Privilege</b>	Security Administrator, Administrator, Operator
<b>Command Modes</b>	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**    `test ipcf bindmux [ start | stop ]`

**start**

Starts the IPCF BindMux Manager on the chassis. If already an instance of IPCF BindMux Manager is running it prompts accordingly.

**stop**

Stops the IPCF BindMux Manager instance running on the chassis.

**Usage Guidelines**

Use this command to test the status of IPCF BindMux Manager instance and also to start or stop the BindMux Manager instance on the chassis.

**Caution**

The use of test commands could adversely affect the operation of your system. It is recommended that they only be used under the guidance and supervision of qualified support representative.

---

**Example**

The following command stops the BindMux Manager instance running on the chassis:

```
test ipcf bindmux stop
```

## test ipsec tunnel ip-pool

Tests a specified IPsec tunnel associated with an IP pool name.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
test ipsec tunnel ip pool pool_name destination-ip ip_address }
```

***pool\_name*** destination-ip ***ip\_address***

**ip pool** *pool\_name*: Specifies the name of an existing IP pool as an alphanumeric string of 1 through 32 characters.

**destination-ip** *ip\_address*: Specifies a destination IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation

**Usage Guidelines**

Use this command to test a specified IPsec tunnel.

**Caution**

The use of test commands could adversely affect the operation of your system. It is recommended that they only be used under the guidance and supervision of qualified support representative.

**Example**

The following command test the IPsec tunnel associated with *pool3* with a destination IP address of *10.2.3.4*:

```
test ipsec tunnel ip pool pool3 destination-ip 10.2.3.4
```

## test mobile tunnel

Tests for the existence of a specified mobile tunnel.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
test mobile tunnel { callid call_id | imsi imsi_value | ipaddr ip_address | msid msid_num | nai nai_value }
```

**callid** *call\_id*

Specifies the exact call instance ID which is to have trace data logged.as a 4-byte hexadecimal number.

**imsi** *imsi\_value*

Specifies the International Mobile Subscriber Identity (IMSI) of the subscriber session to be monitored an integer from 1 though 15 characters.

**ipaddr** *ip\_address*

Specifies the IP address of the subscriber session to be monitored in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**msid** *msid\_num*

Specifies the mobile subscriber identification number to be monitored as 7 to 16 digits of an IMSI, MIN, or RMI.

**nai *nai\_value***

Specifies the mobile session Network Access Identifier as an alphanumeric string of 1 through 256 characters. The NAI is the user identity submitted by the client during network access authentication.

**Usage Guidelines**

Use this command to test a specified mobile tunnel.

**Caution**

The use of test commands could adversely affect the operation of your system. It is recommended that they only be used under the guidance and supervision of qualified support representative.

**Example**

The following command tests the subscriber session associated with IP address 192.64.66.9:

```
test mobile tunnel ipaddr 192.64.66.9
```

## timestamps

Enables or disables the generation of a timestamp in response to each command entered. The timestamp does not appear in any logs as it is a CLI output only. This command affects the current CLI session only. Use the **timestamps** command in the Global Configuration Mode to change the behavior for all future CLI sessions.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
[ no ] timestamps
```

**no**

Disables generation of timestamp output for each command entered. When omitted, the output of a timestamp for each entered command is enabled.

**Usage Guidelines**

Enable timestamps when logging a CLI session on a remote terminal such that each command will have a line of text indicating the time when the command was entered.

**Example**

The following command initiates time stamping of CLI commands as they are entered for this login session:

```
timestamps
```

# tracert

Collects information on the route data will take to a specified IPv4 host.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```




---

**Important**

Inspector privileges are granted for all variables except **count** and **port**. To initiate a tracert count or to target a specific port for a tracert, you must have a minimum privilege level of Operator.

---



---

**Syntax Description**

```
tracert { host_name | host_ip_address } [ count packets ] [ df ] [ maxttl
max_ttl ] [ minttl min_ttl ] [ port port_num ] [ size octet_count ] [ src {
src_host_name | src_host_ip_address } ] [ timeout seconds ] [ vrf vrf_name ] [ | {
grep grep_options | more } ]
```

### ***host\_name* | *host\_ip\_address***

Identifies the remote node to trace the route to.

*host\_name*: specifies the remote node using its logical host name which must be resolved via DNS lookup.

*host\_ip\_address*: specifies the remote node using its assigned IP address entered using the IPv4 dotted-decimal notation.

### **count *packets***

Specifies the number of UDP probe packets to send. Default: 3

### **df**

Indicates the packets for the tracing of the route should not be fragmented. If a packet requires fragmenting, it is dropped and the result is the ICMP response "Unreachable, Needs Fragmentation" is received.

### **maxttl *max\_ttl***

Specifies the maximum time to live for the route tracing packets as an integer from 1 through 255. *max\_ttl* must be greater than *min\_ttl* whether *min\_ttl* is specified or defaulted. Default: 30

The time to live (TTL) is the number of hops through the network; it is not a measure of time.

### **minttl *min\_ttl***

Specifies the minimum time to live for the route tracing packets as an integer from 1 through 255. *min\_ttl* must be less than *max\_ttl* whether *max\_ttl* is specified or defaulted. Default: 1

The time to live (TTL) is the number of hops through the network; it is not a measure of time.

**port *port\_num***

Specifies a specific port for connection as an integer from 1 through 65535. Default: 33434

**size *octet\_count***

Specifies the number of bytes for each packet as an integer from 40 through 32768. Default: 40

**src { *src\_host\_name* | *src\_host\_ip\_address* }**

Specifies an IP address to use in the packets as the source node. Default: originating system's IP address

*src\_host\_name*: specifies the remote node using its logical host name which must be resolved via a DNS lookup.

*src\_host\_ip\_address*: specifies the remote node using its assigned IP address specified entered using IPv4 dotted-decimal notation.

**timeout *seconds***

Specifies the maximum time (in seconds) to wait for a response from each route tracing packet as an integer from 2 through 100. Default: 5

**vrf *vrf\_name***

Specifies the name of an existing virtual routing and forwarding (VRF) context associated with this route as an alphanumeric string of 1 through 63 characters. Associates a Virtual Routing and Forwarding (VRF) context with this static ARP entry.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in this guide.

---

## Usage Guidelines

Trace an IPv4 route when troubleshooting network problems where certain nodes are having significant packet delays or packet loss. This can also be used to identify bottlenecks in the routing of data within the network.

### Example

The following command traces the route to remote host *remoteABC* and sends the output to the *more* command.

```
traceroute remoteABC | more
```

The following command traces the route to remote host *10.2.3.4*'s port *2047* waiting a maximum of 2 seconds for responses.

```
traceroute 10.2.3.4 port 2047 timeout 2
```

# tracert6

Collects information on the route data will take to a specified IPv6 host.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```




---

**Important**

Inspector privileges are granted for all variables except **count** and **port**. To initiate a traceroute count or to target a specific port for a traceroute, you must have a minimum privilege level of Operator.

---



---

**Syntax Description**

```
tracert6 { host_name | host_ipv6_address } [ count packets ] [ maxttl max_ttl ] [ port port_num ] [ size octet_count ] [ src { src_host_name | src_host_ipv6_address } ] [ timeout seconds ] [ vrf vrf_name ] [ | { grep grep_options | more } ]
```

### ***host\_name* | *host\_ipv6\_address***

Identifies the remote node to trace the route to.

*host\_name*: specifies the remote node using its logical host name which must be resolved via DNS lookup.

*host\_ipv6\_address*: specifies the remote node using its assigned IP address entered using the IPv6 colon-separated-hexadecimal notation.

### **count *packets***

Specifies the number of UDP probe packets to send. Default: 3

### **maxttl *max\_ttl***

Specifies the maximum time to live for the route tracing packets as an integer from 1 through 255. *max\_ttl* must be greater than *min\_ttl* whether *min\_ttl* is specified or defaulted. Default: 30

The time to live (TTL) is the number of hops through the network; it is not a measure of time.

### **port *port\_num***

Specifies a specific port for connection as an integer from 1 through 65535. Default: 33434

### **size *octet\_count***

Specifies the number of bytes for each packet as an integer from 40 through 32768. Default: 40



**src { *src\_host\_name* | *src\_host\_ipv6\_address* }**

Specifies an IP address to use in the packets as the source node. Default: originating system's IP address

*src\_host\_name*: specifies the remote node using its logical host name which must be resolved via a DNS lookup.

*src\_host\_ipv6\_address*: specifies the remote node using its assigned IP address specified entered using IPv6 colon-separated-hexadecimal notation.

**timeout *seconds***

Specifies the maximum time (in seconds) to wait for a response from each route tracing packet as an integer from 2 through 100. Default: 5

**vrf *vrf\_name***

Specifies the name of an existing virtual routing and forwarding (VRF) context associated with this route as an alphanumeric string of 1 through 63 characters.

**grep *grep\_options* | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in this guide.

---

### Usage Guidelines

Trace an IPv6 route when troubleshooting network problems where certain nodes are having significant packet delays or packet loss. This can also be used to identify bottlenecks in the routing of data within the network.

### Example

The following command traces the route to remote host *remoteABC* and sends the output to the *more* command.

```
traceroute6 remoteABC | more
```

The following command traces the route to remote host *2000:4A2B::1f3F*'s port *2047* waiting a maximum of 2 seconds for responses.

```
traceroute6 2000:4A2B::1f3F port 2047 timeout 2
```

## update active-charging

Updates specified active charging option(s) for the matching sessions.

---




### Product

ACS

PSF

NAT

TPO

<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec  The following prompt is displayed in the Exec mode:  [local]host_name#
<b>Syntax Description</b>	<pre>update active-charging { override-control rulebase-config   switch-to-fw-and-nat-policy fw_nat_policy_name   switch-to-rulebase rulebase_name   switch-to-tpo-policy tpo_policy_name } { all   callid call_id   fw-and-nat-policy fw_nat_policy_name   imsi imsi   ip-address ip_address   msid msid   rulebase rulebase_name   tpo-policy tpo_policy_name   username user_name } [ -noconfirm ] [   { grep grep_options   more } ]</pre> <p><b>override-control rulebase-config</b></p> <p>This keyword initiates batch processing of all active calls to apply Override Control (OC) or Inheritance after any rulebase changes, charging action changes and/or addition/deletion of ruledefs for all subscribers having OC or Inheritance feature enabled. Since this is the batch processing of all active calls, the command execution will be in the background even after the CLI command returns to the CLI prompt.</p> <hr/> <p> <b>Important</b> Override Control is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. For more information on the licensing requirements, contact your Cisco account representative. For more information on the command to enable this feature, refer to <i>ACS Rulebase Configuration Mode Commands</i> chapter in the <i>Command Line Interface Reference</i>.</p> <hr/> <p> <b>Important</b> In this release, both Inheritance and the Override Control features are supported. Note that these two features should not be enabled simultaneously. If by mistake, these two features are enabled, only Override Control is applied.</p> <hr/> <p>In 17 and later releases, this CLI command is used to apply the overridden or inherited values after any ruledef, charging action and rulebase changes performed through the CLI commands in the respective configuration modes. This CLI command is necessary because the configuration changes are reflected immediately on any new PDN session that gets established. However, for the existing PDN sessions established before the configuration change, explicit execution of this CLI command is necessary. This will get all the PDN sessions in system in sync with respect to the required configuration changes.</p> <hr/> <p> <b>Important</b> It is recommended that this CLI command is executed after all rulebase/charging action/ruledef changes are complete. So, this will help in one-time execution of the CLI to get all PDN sessions in sync.</p> <hr/> <p>Typically, this command is used whenever any rulebase, charging action or ruledef modification happens. Once this CLI command is executed, each subscriber will read the configuration and incorporate the rulebase or ruledef changes for Override Control. Until this CLI execution is complete, Inheritance or Override Control values will not be applied to the changes done in configuration for all existing calls. Charging and policy parameters configured at P-GW will apply during this period. Please follow recommended upgrade procedures to avoid this. For the upgrade procedure, contact your Cisco account representative.</p>

In release 17, the batch processing will complete in 15 to 20 minutes depending on the call load in the system. In 18 and later releases, batch processing will complete in 1 to 3 minutes depending on the call load in the system.

If the **override-control rulebase-config** command has been issued multiple times, batch processing will be restarted and the latest rulebase/charging action/ruledef changes will be applied to all the active calls.




---

**Important**

In release 17, there was no restriction on the usage of the CLI command "**update active-charging override-control rulebase-config**" on a standby chassis. In release 18 and later, this CLI command is not allowed to be executed on the standby chassis.

---

**switch-to-fw-and-nat-policy *fw\_nat\_policy\_name***

Specifies an existing Firewall-and-NAT policy to switch to as an alphanumeric string of 1 through 63 characters.

**switch-to-rulebase *rulebase\_name***

Specifies an existing rulebase to switch to as an alphanumeric string of 1 through 63 characters.

**switch-to-tpo-policy *tpo\_policy\_name***



---

**Important**

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

---

**all**

Updates rulebase/policy for all subscribers.

**callid *call\_id***

Updates rulebase/policy for the Call Identification number specified as an eight-digit hexadecimal number.

**fw-and-nat-policy *fw\_nat\_policy\_name***

Updates the rulebase/policy for sessions matching an existing Firewall-and-NAT policy specified as an alphanumeric string of 1 through 63 characters.

**imsi *imsi***

Updates rulebase/policy for International Mobile Subscriber Identification (IMSI) specified here.

*imsi* must be 3 digits of MCC (Mobile Country Code), 2 or 3 digits of MNC (Mobile Network Code), and the rest with MSIN (Mobile Subscriber Identification Number). The total should not exceed 15 digits. For example, 123-45-678910234 can be entered as 12345678910234.

**ip-address *iP\_address***

Updates rulebase/policy for the IP address specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**msid** *msid*

Updates rulebase/policy for an MSID specified as a string of 1 through 24 characters.

**rulebase** *rulebase\_name*

Updates rulebase/policy for sessions matching an existing rulebase specified as an alphanumeric string of 1 through 63 characters.

**tpo-policy** *tpo\_policy\_name***Important**


---

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

---

**username** *user\_name*

Updates rulebase/policy for user specified as an alphanumeric of characters and/or wildcard characters ('\$ and '\*') of 1 through 127 characters.

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the Regulating a Command's Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

**Usage Guidelines**

Use this command to change specified active charging option(s) for the matching sessions.

**Example**

The following command changes the rulebase for sessions using the rulebase named *standard* to use the rulebase named *super*:

```
update active-charging switch-to-rulebase super rulebase standard
```

## update firewall policy

This command is obsolete.

## update ip access-list

When you update an IP Access list, this command forces the new version of the access list to be applied to any subscriber sessions that are currently using that list.

<b>Product</b>	PDSN GGSN ASN-GW
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec  The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<pre><b>update ipv6 access-list</b> <i>list_name</i> <b>subscribers</b> [ <i>command_keyword</i> ] [ <i>filter_keywords</i> ] [-noconfirm] [verbose] ]</pre> <p><b><i>list_name</i></b> Specifies the name of an existing IP Access list that you want to apply to the subscriber as an alphanumeric string of 1 through 47 characters.</p> <p><b>[ <i>command_keyword</i> ] [ <i>filter_keywords</i> ]</b> These are the same command keywords and filter keywords available for the <b>show subscribers</b> command.</p> <p><b>-noconfirm</b> Executes the command without any additional prompt and confirmation from the user.</p> <p><b>verbose</b> Show detailed information.</p>
<b>Usage Guidelines</b>	Use this command to force existing subscriber sessions that are already using a specific IP Access list to have that IP Access list reapplied. This is useful when you edit an IP Access list and want to make sure that even existing subscriber sessions have the new changes applied.
	<p><b>Example</b></p> <p>To apply the IP Access list named <i>ACLlist11</i> to all existing subscribers that are already using that IP Access list, enter the following command:</p> <pre><b>update ip access-list ACLlist11 subscribers all</b></pre>

## update ipv6 access-list

When you update an IP Access list, this command forces the new version of the access list to be applied to any subscriber sessions that are currently using that list.

<b>Product</b>	PDSN GGSN
----------------	--------------

ASN-GW

**Privilege** Security Administrator, Administrator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `update ipv6 access-list list_name subscribers [ command_keyword ] [ filter_keywords ] [-noconfirm] [verbose] ]`

***list\_name***

Specifies the name of an existing IPv6 Access list that you want to apply to the subscriber as an alphanumeric string of 1 through 47 characters.

**[ *command\_keyword* ][ *filter\_keywords* ]**

These are the same command keywords and filter keywords available for the **show subscribers** command.

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

**verbose**

Show detailed information.

**Usage Guidelines** Use this command to force existing subscriber sessions that are already using a specific IPv6 Access list to have that IPv6 Access list reapplied. This is useful when you edit an IPv6 Access list and want to make sure that even existing subscriber sessions have the new changes applied.

**Example**

To apply the IPv6 Access list named *ACLv6List1* to all existing subscribers that are already using that IP Access list, enter the following command:

```
update ipv6 access-list ACLv6List1 subscribers all
```

## update ip-pool apn

Use this CLI command to update the VPN manager with the APN configuration changes.

**Product** CUPS

**Privilege** Security Administrator, Administrator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `update ip-pool apn { all | name apn_name }`

**all**

Specifies to update all the configured APNs to the VPN manager.

**name *apn\_name***

Specifies to update a specific APN configuration to the VPN manager.

---

**Usage Guidelines**

This CLI command triggers the `SX_ASSOCIATION_UPDATE` towards the UP and transfers all the allocated IP pool chunks for the newly added IP pools.

For additional information, refer to the *Dynamic APN and IP Pool Support* chapter.

**Example**

The following CLI command updates a specific APN configuration, *cisco.com*, to the VPN manager:

```
update ip-pool apn name cisco.com
```

## update local-user database

Updates the local user (administrative) database with current user information. Run this command immediately after creating, removing or editing administrative users.




---

**Important**

In a release 20.0 or higher Trusted build, this command is not available.

---



---

**Product** All

---

**Privilege** Security Administrator, Administrator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `update local-user database`

---

**Usage Guidelines** Use this command to update the local-user database with current information.

**Example**

The following command updates the local-user database:

```
update local-user database
```

## update module

Loads a specified plugin module from the Module Priority List with the lowest priority number. This will also copy the Module priority list onto the Version priority list. This function is associated with the patch process for accommodating dynamic software upgrades.

---

**Product** ADC

---

**Privilege** Security Administrator, Administrator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `update module plugin_name`

### *plugin\_name*

Specifies the name of an existing plugin module that you want to update as an alphanumeric string of 1 through 16 characters. If the named module is not known to the system, an error message is displayed.

---

**Usage Guidelines** Use this command to initiate an update of a new software plugin module. If it fails to load, the module with next highest priority will be loaded. If none of the modules are installed, the default patch which comes along with the StarOS build is automatically loaded. The specified module must have been previously unpacked/verified and configured via the **install plugin** and **plugin** commands respectively.

For additional information, refer to the *Plugin Configuration Mode Commands* chapter.

### Example

The following command updates the plugin module named *p2p*:

```
update module p2p
```

## update qos policy map

Updates QoS profile information based on specific subscriber policy maps.

---

**Product** All

---

**Privilege** Security Administrator, Administrator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```



**Syntax Description**

```
update qos policy-map map_name use-granted-profile-id id1 [ id2 ] [ id3 ]
subscribers [ command_keyword ] [ filter_keywords ] [ -noconfirm ] [ verbose ]
[ match-requested-profile-id ] [ | { grep grep_options | more } ]
```

***map\_name***

Specifies the name of an existing policy map as an alphanumeric string of 1 through 15 characters.

**use-granted-profile-id *id1* [ *id2* ] [ *id3* ]**

Specifies the profile IDs to update. Up to three different profile IDs can be specified.

Each profile ID is specified as a hexadecimal value from 0x0 and 0xFFFF.

**subscribers [ *command\_keyword* ] [ *filter\_keywords* ]**

These are the same command keywords and filter keywords available for the **show subscribers** command.

**[ **-noconfirm** ]**

Updates matching subscribers without prompting for confirmation.

**[ **verbose** ]**

Displays details for the profile updates.

**[ **match-requested-profile-id** ]**

Sends session-updates only to profile-ids matching the profile-ids in the requested list.

**grep *grep\_options* | **more****

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in this guide.

**Usage Guidelines**

Use this command to update subscriber session profile IDs based on the specified criteria.

**Example**

The following command updates profile IDs *0x3E* and *0x4C* for all subscriber sessions and sends session-updates with the IDs:

```
update qos policy-map test use-granted-profile-id 0x3E 0x4C subscribers
all match-requested-profile-id
```

## update qos tft

Updates the subscriber traffic flow template (TFT) associated with the flow ID and direction.

---

**Product** All

---

**Privilege** Security Administrator, Administrator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
update qos tft flow-id flow-id flow-dir { forward | reverse }
use-granted-profile-id id1 [ id2 ] [ id3 ] subscribers [ command_keyword ] [
filter_keywords ] [-noconfirm ] [ verbose ] [ match-requested-profile-id ]
[ | { grep grep_options | more }
```

#### **flow-id *flow-id***

Sends session updates only when the flow ID matches the flow-id and flow-direction. *flow-id* must be specified as an integer from 1 through 255.

#### **flow-dir { forward | reverse }**

Specifies the direction of the TFT flow.

#### **subscribers [ *command\_keyword* ] [ *filter\_keywords* ]]**

These are the same command keywords and filter keywords available for the **show subscribers** command.

---

**Usage Guidelines** Supports QoS updates based on subscriber TFTs.

#### **Example**

The following command update QoS for reverse flow 0, profile ID 0x0, all subscribers without prompting for confirmation:

```
update qos tft flow-id 0 flow-dir reverse use-granted-profile-id 0x0
subscribers all -noconfirm
```

## update security

Updates database information for the specified Talos Security Intelligence server.

---

**Product** All

---

**Privilege** Security Administrator, Administrator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**    `update security server talos-intelligence server_name [ force ]`

***server\_name***

Specifies an existing Talos Intelligence Server name to be updated. *server\_name* must be specified as a case-sensitive alphanumeric string from 1 through 31 characters.

**force**

Deletes the existing DB files before the Talos Intelligence server is queried. When this optional keyword is used, the latest files will always be downloaded and updated even if the system already has the most recent versions.

---

**Usage Guidelines**    Use this command to query the Talos Intelligence Server to determine if updated database files exist. If so, the files will be downloaded and updated.

## upgrade content-filtering

Upgrades the Static Rating Database (SRDB) for Category-based Content Filtering application.

---

**Product**    CF

---

**Privilege**    Security Administrator, Administrator

---

**Command Modes**    Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**    `upgrade content-filtering category { database | rater-pkg }`

**upgrade content-filtering category database**

Triggers the upgrade of the Category-based Content Filtering Static Rating Database (SRDB).

**upgrade content-filtering category rater-pkg**

Triggers manual upgrade of the Dynamic Content-Filtering Rater Package (**rater.pkg** file).

The **rater.pkg** file contains the models and feature counters that are used to return the dynamic content rating. The upgrade will trigger distribution of the **rater.pkg** to all the SRDBs.




---

**Important**    This command is customer specific. For more information, please contact your local sales representative.

---



---

**Usage Guidelines**    Use this command to load the Static Rating Database (SRDB) in to memory for Category-based Content Filtering application, and/or to load the *rater.pkg* file.

If the default directory of /cf does not exist on the flash, it will create the same. It also locates the recent full database and loads it into memory. This command also clears the old and excess incremental databases.




---

**Important** This command is not supported on all platforms.

---

**Example**

The following command upgrades the SRDB for the Category-based Content Filtering application:

```
upgrade content-filtering category database
```

## upgrade database

This command allows you to upgrade a specified database.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
upgrade database uidh [ all | wl-url-host-db ]
```

**uidh all**

Upgrades UIDH databases.

**uidh wl-url-host-db**

Upgrades URL Host databases.

**Usage Guidelines**

Use the following command to upgrade the UIDH whitelist URL database:

## upgrade tethering-detection

Upgrades the Tethering Detection feature's database(s).

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `upgrade tethering-detection database { all | os-signature | tac | ua-signature } [ -noconfirm ]`

**all**

Upgrades all Tethering Detection databases—OS, TAC and UA.

**os-signature**

Upgrades only the OS database.

**tac**

Upgrades only the TAC database.

**ua-signature**

Upgrades only the UA database.

**- noconfirm**

Executes the command without any prompts and confirmation from the user.

**Usage Guidelines**

Use this command to upgrade the database(s) used by the Tethering Detection feature.

This command upgrades the database(s) from file(s) kept in designated path. The name of the existing source file is prefixed with the word "new-". For example for OS DB, if the existing file name is "os-db", the upgrade file name is "new-os-db".

If there is a file named "new-xxx-db", it is verified that it is a valid Tethering Detection database and then loaded it into memory. If successful, the files is renamed "xxx-db" to "xxx-db-<number>" and then renamed "new-xxx-db" to "new-xxx-db".

For example, the command **upgrade tethering-database ua-signature -noconfirm** results in loading the file by name "new-ua-db" if it is present in the designated directory. In case of a successful upgrade, the previous version of the database is stored as backup in a file named "ua-db-1". Also, the newly uploaded database file is renamed as "ua-db".

Also see the **tethering-database** command in the *ACS Configuration Mode Commands* chapter.

**Example**

The following command upgrades all Tethering Detection databases:

```
upgrade tethering-detection database all -noconfirm
```

## upgrade url-blockedlisting database

Upgrades the URL blockedlisting database.

**Product**

CF

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

In releases prior to StarOS 21.26:

```
upgrade url-blacklisting database [ -noconfirm ]
```

From StarOS 21.26 and later releases:

```
upgrade url-blockedlisting database [ -noconfirm ]
```

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

---

**Usage Guidelines**

Use this command to upgrade and load a URL blacklisting database whenever required.

**Example**

In releases prior to StarOS 21.26:

The following command updates the URL blacklisting database:

```
upgrade url-blacklisting database
```

From StarOS 21.26 and later releases:

The following command updates the URL blockedlisting database:

```
upgrade url-blockedlisting database
```



# CHAPTER 19

## Exec Mode show Commands (A-C)

The Exec Mode is the initial entry point into the command line interface system. Exec mode **show** commands are useful in troubleshooting and basic system monitoring.

### Command Modes

This section includes the commands **show aaa** through **show css service**.

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```



### Important

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

- [show active-charging analyzer statistics](#), on page 580
- [show active-charging bandwidth-policy](#), on page 592
- [show active-charging charging-action](#), on page 592
- [show active-charging content-filtering category policy-id](#), on page 593
- [show active-charging content-filtering category statistics](#), on page 594
- [show active-charging content-filtering server-group](#), on page 596
- [show active-charging credit-control](#), on page 597
- [show active-charging dns-learnt-ip-addresses](#), on page 599
- [show active-charging edr-format](#), on page 600
- [show active-charging edr-udr-file](#), on page 601
- [show active-charging file-space-usage](#), on page 602
- [show active-charging firewall dos-protection](#), on page 603
- [show active-charging firewall statistics](#), on page 604
- [show active-charging firewall track-list](#), on page 605
- [show active-charging flow-control-counters](#), on page 606
- [show active-charging flow-kpi](#), on page 607
- [show active-charging flow-mappings](#), on page 608
- [show active-charging flows](#), on page 609
- [show active-charging fw-and-nat policy](#), on page 625
- [show active-charging group-of-objects](#), on page 626
- [show active-charging group-of-prefixed-urls](#), on page 627

- [show active-charging group-of-ruledefs](#), on page 628
- [show active-charging nat statistics](#), on page 629
- [show active-charging p2p-dynamic-rules](#), on page 631
- [show active-charging packet-filter](#), on page 631
- [show active-charging pcp-service](#), on page 632
- [show active-charging qos-group-of-ruledefs](#), on page 634
- [show active-charging regex](#), on page 635
- [show active-charging rulebase](#), on page 636
- [show active-charging ruledef](#), on page 637
- [show active-charging service](#), on page 639
- [show active-charging service-scheme](#), on page 640
- [show active-charging sessions](#), on page 641
- [show active-charging sessions credit-control server-unreachable](#), on page 655
- [show active-charging subscribers](#), on page 669
- [show active-charging subsystem](#), on page 670
- [show active-charging tcp-proxy statistics](#), on page 671
- [show active-charging tethering-detection](#), on page 673
- [show active-charging timedef](#), on page 674
- [show active-charging traffic-optimization counters sessmgr](#), on page 675
- [show active-charging traffic-optimization info](#), on page 676
- [show active-charging trigger-action](#), on page 676
- [show active-charging trigger-condition](#), on page 677
- [show active-charging udr-format](#), on page 678
- [show active-charging url-blockedlisting statistics](#), on page 679
- [show active-charging video detailed-statistics](#), on page 681
- [show active-charging xheader-format](#), on page 681
- [show administrators](#), on page 682
- [show alarm](#), on page 683
- [show alcap counters](#), on page 685
- [show alcap-service](#), on page 686
- [show alcap statistics](#), on page 687
- [show apn](#), on page 688
- [show apn counters ip-allocation](#), on page 689
- [show apn statistics](#), on page 690
- [show apn-profile](#), on page 693
- [show apn-remap-table](#), on page 694
- [show aps](#), on page 695
- [show asngw-service](#), on page 696
- [show asngw-service session](#), on page 698
- [show asngw-service session counters](#), on page 699
- [show asngw-service statistics](#), on page 701
- [show asnpc-service](#), on page 703
- [show asnpc-service session](#), on page 704
- [show asnpc-service session counters](#), on page 705
- [show asnpc-service session counters verbose](#), on page 706
- [show asnpc-service statistics](#), on page 708



- [show asnpc-service statistics verbose](#), on page 709
- [show banner](#), on page 710
- [show bcmcs counters](#), on page 711
- [show bcmcs statistics](#), on page 712
- [show bfd](#), on page 712
- [show boot](#), on page 713
- [show bssap+ statistics](#), on page 714
- [show bssgp statistics](#), on page 715
- [show bssgp status](#), on page 716
- [show build](#), on page 717
- [show bulkstats](#), on page 718
- [show ca-certificate](#), on page 725
- [show ca-crl](#), on page 725
- [show cae-group server](#), on page 726
- [show call-control-profile](#), on page 727
- [show call-home](#), on page 728
- [show camel-service](#), on page 729
- [show card](#), on page 730
- [show cbs counters](#), on page 731
- [show cbs sessions](#), on page 732
- [show cbs statistics](#), on page 733
- [show cbs-service](#), on page 735
- [show cdr](#), on page 736
- [show certificate](#), on page 737
- [show cgw-service](#), on page 737
- [show cli](#), on page 738
- [show clock](#), on page 739
- [show cloud configuration](#), on page 740
- [show cloud hardware](#), on page 741
- [show cloud monitor](#), on page 742
- [show cmp history](#), on page 743
- [show cmp outstanding-req](#), on page 744
- [show cmp statistics](#), on page 745
- [show confdmgr](#), on page 745
- [show configuration](#), on page 746
- [show configuration errors](#), on page 750
- [show congestion-control](#), on page 754
- [show connectedapps](#), on page 756
- [show content-filtering category database](#), on page 757
- [show content-filtering category policy-id](#), on page 758
- [show content-filtering category statistics](#), on page 759
- [show content-filtering category url](#), on page 760
- [show content-filtering server-group](#), on page 762
- [show context](#), on page 763
- [show cpu](#), on page 763
- [show crash](#), on page 765

- [show credit-control sessions](#), on page 766
- [show credit-control statistics](#), on page 767
- [show crypto blockedlist file](#), on page 767
- [show crypto group](#), on page 768
- [show crypto ikev1](#), on page 769
- [show crypto ikev2-ikesa security-associations](#), on page 771
- [show crypto ikev2-ikesa transform-set](#), on page 773
- [show crypto ipsec security-associations](#), on page 774
- [show crypto ipsec transform-set](#), on page 777
- [show crypto isakmp keys](#), on page 778
- [show crypto isakmp policy](#), on page 779
- [show crypto isakmp security-associations](#), on page 779
- [show crypto managers](#), on page 780
- [show crypto map](#), on page 782
- [show crypto statistics](#), on page 784
- [show crypto template](#), on page 785
- [show crypto vendor-policy](#), on page 786
- [show crypto permitlist file](#), on page 788
- [show cs-network](#), on page 788
- [show cs-network counters](#), on page 790
- [show cs-network statistics](#), on page 791
- [show css delivery-sequence](#), on page 792
- [show css server](#), on page 792
- [show css service](#), on page 792

## show active-charging analyzer statistics

Displays statistical information for protocol analyzers.

---

**Product** ACS

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show active-charging analyzer statistics** [ **name** *protocol\_name* [ **instance** *instance\_number* ] [ **verbose** ] ] [ | { **grep** *grep\_options* | **more** } ]

**name** *protocol\_name*

Displays detailed information for the specified protocol analyzer:

- **cdp**
- **dns**

- file-transfer
- ftp
- h323
- http
- icmp
- icmpv6
- imap
- ip
- ipv6
- mms
- p2p [ **application** *p2p\_list* | **protocol-group** *group\_list* | **duration** [ **audio** { **application** *p2p\_audio\_duration\_list* } | **video** { **application** *p2p\_video\_duration\_list* } ] ] [ **wide** [ **all** ] ] : Peer-to-peer analyzer.

**p2p application** *p2p\_list*: The supported applications are:

- 8tracks
- abcnetworks
- actionvoip
- actsync
- adobeconnect
- aimini
- amazoncloud
- amazonmusic
- amazonvideo
- antsp2p
- apple-push
- apple-store
- applejuice
- applemaps
- ares
- armagettron
- avi
- badoo
- baidumovie

- battlefld
- bbm
- beatport
- betternet
- bitcasa
- bittorrent
- bittorrent-sync
- blackberry-store
- blackberry
- blackdialer
- box
- callofduty
- chikka
- cisco-jabber
- citrix
- clubbox
- clubpenguin
- crackle
- crossfire
- crunchyroll
- cyberghost
- dblink
- deezer
- didi
- directconnect
- dish-anywhere
- disneymovies
- dofus
- dramafever
- dropbox
- edonkey
- espn

- **expressvpn**
- **facebook**
- **facetime**
- **fandor**
- **fasttrack**
- **feidian**
- **fiesta**
- **filetopia**
- **filmontv**
- **flash**
- **flickr**
- **florensia**
- **foursquare**
- **fox-sports**
- **freenet**
- **friendster**
- **fring**
- **funshion**
- **gadu\_gadu**
- **gamekit**
- **gmail**
- **gnutella**
- **go90**
- **goober**
- **google-music**
- **google-push**
- **google**
- **googleplay**
- **googleplus**
- **gotomeeting**
- **gtalk**
- **guildwars**

- **halflife2**
- **hamachivpn**
- **hayu**
- **hbogo**
- **hbonow**
- **heytell**
- **hgtv**
- **hike-messenger**
- **hls**
- **hotspotvpn**
- **hulu**
- **hyves**
- **iax**
- **icall**
- **icecast**
- **icloud**
- **idrive**
- **igo**
- **iheartradio**
- **imesh**
- **imessage**
- **imgur**
- **imo**
- **instagram**
- **oplayer**
- **iptv**
- **irc**
- **isakmp**
- **iskoot**
- **itunes**
- **jabber**
- **jap**

- **jumblo**
- **kakaotalk**
- **kik-messenger**
- **kontiki**
- **kugoo**
- **kuro**
- **linkedin**
- **livestream**
- **lync**
- **magicjack**
- **manolito**
- **mapfactor**
- **mapi**
- **maplestory**
- **meebo**
- **mgcp**
- **mlb**
- **mojo**
- **monkey3**
- **mozy**
- **msn**
- **msrp**
- **mute**
- **mypeople**
- **myspace**
- **nateontalk**
- **naverline**
- **navigon**
- **nbc-sports**
- **netmotion**
- **newsy**
- **nick**

- **nimbuzz**
- **nokia-store**
- **octoshape**
- **off**
- **ogg**
- **oist**
- **oovoo**
- **opendrive**
- **openft**
- **openvpn**
- **orb**
- **oscar**
- **outlook**
- **paltalk**
- **pando**
- **pandora**
- **path**
- **pbs**
- **pcanywhere**
- **periscope**
- **pinterest**
- **plingm**
- **poco**
- **popo**
- **pplive**
- **ppstream**
- **ps3**
- **qq**
- **qqgame**
- **qqlive**
- **quake**
- **quic**



- quicktime
- radio-paradise
- radius
- rdp
- rdt
- regram
- rfactor
- rhapsody
- rmstream
- rodi
- rynga
- samsung-store
- scydo
- secondlife
- shoutcast
- showtime
- silverlight
- siri
- skinny
- skydrive
- skype
- slacker-radio
- slingbox
- slingtv
- smartvoip
- snapchat
- softether
- sopcast
- soribada
- soulseek
- soundcloud
- spark

- **spdy**
- **speedtest**
- **spike**
- **splashfighter**
- **spotify**
- **ssdp**
- **starz**
- **stealthnet**
- **steam**
- **stun**
- **sudaphone**
- **svtplay**
- **tagged**
- **talkatone**
- **tango**
- **teamspeak**
- **teamviewer**
- **telegram**
- **thunder**
- **tinder**
- **tmo-tv**
- **tor**
- **truecaller**
- **truphone**
- **tumblr**
- **tunein-radio**
- **tunnelvoice**
- **turbovpn**
- **tvants**
- **tvland**
- **tvuplayer**
- **twitch**

- **twitter**
- **ultrabac**
- **ultrasurf**
- **univision**
- **upc-phone**
- **usenet**
- **ustream**
- **uusee**
- **vchat**
- **veohtv**
- **vessel**
- **vevo**
- **viber**
- **vine**
- **voipdiscount**
- **vopium**
- **vpnmaster**
- **vpnpx**
- **voxer**
- **vtok**
- **vtun**
- **vudu**
- **warcft3**
- **waze**
- **webex**
- **wechat**
- **whatsapp**
- **wii**
- **windows-azure**
- **windows-store**
- **winmx**
- **winny**

- **wmstream**
- **wofkungfu**
- **wofwarcraft**
- **wuala**
- **xbox**
- **xdcc**
- **xing**
- **yahoo**
- **yahoomail**
- **yiptv**
- **youku**
- **yourfreetunnel**
- **youtube**
- **zattoo**

**p2p protocol-group** *group\_list*: The following P2P protocol groups are supported:

- generic
- anonymous-access
- business
- communicator
- cloud
- e-store
- e-mail
- e-news
- internet-privacy
- filesharing
- gaming
- p2p-filesharing
- p2p-anon-filesharing
- remote-control
- social-nw-gaming
- social-nw-generic
- social-nw-videoconf
- standard
- streaming

**wide** [ **all** ]: Displays all available P2P statistics in a single wide line. The **all** keyword displays all available P2P statistics without suppressing zeroes.

- **pop3**
- **pptp**

- rtcp
- rtp
- rtsp
- sdp
- secure-http
- sip
- smtp
- tcp
- tftp
- udp
- wsp
- wtp

**[ instance *instance\_number* ]**

Displays the ACS/Session Manager information for specific instances.

*instance\_number* must be an integer from 1 through 65535.

**verbose**

Specifies to display detailed (all available) information. If not specified, concise information is displayed.

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Use this command to display statistic information for active charging protocol analyzers.

**Example**

The following command displays detailed statistic information for all P2P protocol analyzers:

```
show active-charging analyzer statistics name p2p verbose
```

The following command displays detailed statistic information for all TCP protocol analyzers:

```
show active-charging analyzer statistics name tcp verbose
```



---

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

# show active-charging bandwidth-policy

Displays information on bandwidth policies configured in a service.

**Product** ACS

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

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **show active-charging bandwidth-policy** { **all** | **name** *bandwidth\_policy\_name* } [ | { **grep** *grep\_options* | **more** } ]

## **all**

Displays information for all bandwidth policies configured in the service.

## **name** *bandwidth\_policy\_name*

Displays detailed information for an existing bandwidth policy specified as an alphanumeric string of 1 through 63 characters.

## | { **grep** *grep\_options* | **more** }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines** Use this command to view information on bandwidth policies configured in a service.

## **Example**

The following command displays detailed information for the bandwidth policy named *standard*:

```
show active-charging bandwidth-policy name standard
```

# show active-charging charging-action

Displays information for charging actions configured in the Active Charging Service (ACS).

**Product** ACS

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

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show active-charging charging-action { { { all | name charging_action_name }
[ service name acs_service_name ] } | statistics [ name charging_action_name ]
} [ | { grep grep_options | more } ]
```

**all**

Displays information for each configured charging action.

**name *charging\_action\_name***

Displays detailed information for an existing charging action specified as an alphanumeric string of 1 through 63 characters.

**statistics**

Displays statistical information for all configured charging actions.

**service name *acs\_service\_name***

Displays information for all or a specific charging action in the specified ACS. *acs\_service\_name* is an alphanumeric string of 1 through 15 characters.

**{ { grep *grep\_options* | more } }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display information for charging actions configured in a service.

**Example**

The following command displays a detailed information for all charging actions:

```
show active-charging charging-action all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging content-filtering category policy-id

Displays Content Filtering (CF) category policy definitions.

**show active-charging content-filtering category statistics**

---

**Product** CF

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show active-charging content-filtering category policy-id { all | id policy\_id } [ | { grep grep\_options | more } ]****all**

Displays definitions of all Content Filtering category policies.

**id policy\_id**

Displays definitions of an existing Content Filtering category policy specified as an integer from 1 through 4294967295.

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines** Use this command to view Content Filtering category definitions for a specific/all Policy IDs.**Example**

The following command displays Content Filtering category definitions for policy ID 3:

```
show active-charging content-filtering category policy-id id 3
```



---

**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show active-charging content-filtering category statistics

Displays category-based content filtering statistics.

---

**Product** CF

---

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

---

**Command Modes** Exec



The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show active-charging content-filtering category statistics [ rulebase { name rulebase_name | all } ] [ verbose ] [ | { grep grep_options | more } ]
```

**rulebase { name *rulebase\_name* | all }**

Displays category-based content filtering statistics, either for all or for a specific rulebase.

- **name *rulebase\_name***: Specifies an existing rulebase as an alphanumeric string of 1 through 63 characters.
- **all**: Displays category-based content filtering statistics for each rulebase in the ACS.

### verbose

Specifies to display detailed (all available) information. If not specified, concise information is displayed.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to view category-based content filtering statistics for a specific rulebase, or cumulative statistics for all rulebases in the ACS.



**Note** From Release 21.4, the following changes are made to the output of this show command:

- The "Total number of successful Cache lookups" field is excluded.
- The > **50ms** value is excluded from the "Time taken for rating" field.
- The following sub-fields are added to the "Time taken for rating" field:
  - 50-100ms
  - 100-200ms
  - 200-300ms
  - 300ms

### Example

The following command displays category-based content filtering statistics for the rulebase named *consumer*:

```
show active-charging content-filtering category statistics rulebase name  
consumer
```

The following command displays cumulative category-based content filtering statistics for all rulebases in verbose mode:

```
show active-charging content-filtering category statistics verbose
```



**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging content-filtering server-group

Displays information for Content Filtering Server Group (CFSG) configured in the service.

### Product

CF

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show active-charging content-filtering server-group [ name cfsg_name |
statistics [ name cfsg_name [ acsmgr instance instance_number [ priority priority
] ] | verbose ] [ | { grep grep_options | more } ]
```

#### **name** *cfsg\_name*

Specifies name of an existing CFSG as an alphanumeric string of 1 through 63 characters.

#### **acsmgr instance** *instance\_number*

Specifies the manager instance as an integer from 1 through 65535.

#### **priority** *priority*

Specifies the priority of the server for which statistics has to be displayed as an integer from 1 through 65535.

#### **verbose**

Specifies to display detailed (all available) information, for each ICAP server connection at each instance. If not specified, concise information is displayed.

#### **| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view CFSG information/statistics.

**show active-charging content-filtering server-group name** *cfsg\_name*: The output of this command displays detailed information for the specified CFSG.

**show active-charging content-filtering server-group statistics name** *cfsg\_name*: The output of this command displays cumulative statistics for the specified CFSG. This will include all the instances and all the servers configured in the CFSG.

**show active-charging content-filtering server-group statistics name** *cfsg\_name* **acsmgr instance** *instance\_number*: The output of this command displays the cumulative statistics of all the ICAP server connections on the specified manager instance.

**show active-charging content-filtering server-group statistics name** *cfsg\_name* **acsmgr instance** *instance\_number* **priority** *priority*: The output of this command displays the statistics for the specified ICAP server connection on the specified manager instance.

**show active-charging content-filtering server-group statistics verbose**: The output of this command displays statistics of each ICAP server connection at each instance.

**Example**

The following command displays information for the CFSG named *test12*:

```
show active-charging content-filtering server-group name test12
```

The following command displays detailed information for all CFSGs:

```
show active-charging content-filtering server-group statistics verbose
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

# show active-charging credit-control

Displays statistics for Diameter/RADIUS Prepaid Credit Control Service in the Active Charging Service (ACS).

**Product**

ACS

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show active-charging credit-control { misc-info max-backpressure [ all |
  facility sessmgr instance instance_number ] | statistics [ group group_name
  | server { all | ip-address ip_address [ port port_num ] | name server_name }
  ] | session-states [ rulebase rulebase_name ] [ content-id content_id ] } [ |
  { grep grep_options | more } ]
```

**misc-info max-backpressure [ all | facility sessmgr instance *instance\_number* ]**

Displays miscellaneous information including the maximum backpressure hit count for all active session managers.

- **all**: Displays the max-backpressure count from all session manager instances.
- **facility sessmgr instance *instance\_number***: Displays logged events for specific facility. That is, it will display the maximum backpressure count on that specific session manager instance.

The session manager instance number must be an integer ranging from 1 through 65535 characters.

**statistics [ group *group\_name* | server { all | ip-address *ip\_address* [ port *port\_num* ] | name *server\_name* ] ]**

Displays prepaid credit control statistics.

- **group *group\_name***: Displays statistics for an existing credit control group specified as an alphanumeric string of 1 through 63 characters.
- **server { all | ip-address *ip\_address* [ port *port\_num* ] | name *server\_name* }**: Displays statistics for the specified credit control server.
  - **all**: Displays all available statistics including host statistics.
  - **ip-address *ip\_address***: Displays available statistics for the specified server's address.
  - **port *port\_num***: Displays available statistics for the specified server's port number.
  - **name *server\_name***: Displays the credit control statistics for the specified server.

**session-states [ rulebase *rulebase\_name* ] [ content-id *content\_id* ]**

Displays prepaid CCA session status based on rulebase and/or content ID.

- **rulebase *rulebase\_name***: Displays the Credit Control Application (CCA) session state counts for an existing rulebase specified as an alphanumeric string of 1 through 63 characters.
- **content-id *content\_id***: Displays CCA session state counts for a content ID of a credit control service specified as an integer from 1 through 65535.

**{ *grep grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view statistics for Diameter/RADIUS prepaid credit control service in the ACS.

**Example**

The following command shows ACS statistics of configured Diameter or RADIUS Credit Control Application:

```
show active-charging credit-control statistics
```



**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging dns-learnt-ip-addresses

Displays DNS learnt IP address statistics for the DNS Snooping feature.

**Product** ACS

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

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **show active-charging dns-learnt-ip-addresses statistics { sessmgr { all | instance *sessmgr\_instance\_number* } [ verbose ] | summary } [ | { grep *grep\_options* | more } ]**

**sessmgr { all | instance *sessmgr\_instance\_number* } [ verbose ]**

Displays information for all or the specified Session Manager (SessMgr) instance.

- **all**: Displays information for all SessMgr instances.
- **instance *sessmgr\_instance\_number***: Displays information for a SessMgr instance specified as an integer from 1 through 65535.
- **verbose**: Displays detailed statistics for specified criteria. Use this keyword to view the learnt IP addresses.

### summary

Displays summary information.

**{ { grep *grep\_options* | more } }**

Specifies that the output of this command is to be piped (sent) to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines** Use this command to view statistics for the DNS Snooping feature related DNS learnt-ip-addresses.

This command displays the number of learnt IP entries per rule line. It displays on a service level the number of resolved (learnt) IP addresses per rule line per rulebase (once if a rule line is used multiple times in the same rulebase as it is shared across rulebase) per destination context per SessMgr instance. It also displays the number of entries flushed due to TTL expiry. The field `entries_replaced` gives the number of entries replaced (same IP returned again) in the pool due to a DNS response by same/another subscriber for same domain-name, wherein the TTL of the entry will be replaced.

IPv4-overflows will start incrementing when the maximum limit of 51200 across system is reached OR limit of 200 per pattern is reached.

IPv6-overflows will start incrementing when maximum limit of 25600 across system is reached OR limit of 100 per pattern is reached.

Limits are:

- Maximum of 51,200 IPv4 entries per instance shared across IPv4 all pools.
- Maximum of 200 IPv4 entries per pool (pool is same as discussed before (per rule-line pattern)).
- Maximum of 25,600 IPv6 entries per instance shared across all IPv6 pools.
- Maximum of 100 IPv6 entries per pool.

In releases prior to 14.0, this CLI command **show active-charging dns-learnt-ip statistics sessmgr all** displayed all the configured patterns and rulebase names for each of the pattern entry, even though the pattern has not learnt any IP address. When a large number of DNS snooping ruledefs are configured (configured as ip server-domain name under ruledef configuration), the memory allocated for sending this information exceeded the message size limit for messenger calls and hence the crash was observed.

To avoid the crash occurring, in 14.0 and later releases, the output of the CLI command **show active-charging dns-learnt-ip statistics sessmgr all** is modified to display only the patterns for which at least one IPv4/IPv6 address is learnt as all other information is available from the configuration. Also for each of the patterns this CLI command will not be displaying rulebase name as it can be printed once.

### Example

The following command displays summary statistics for DNS learnt IP addresses:

```
show active-charging dns-learnt-ip-addresses statistics summary
```



#### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging edr-format

Displays information about Event Data Record (EDR) formats configured in the Active Charging Service (ACS).

#### Product

ACS

#### Privilege

Security Administrator, Administrator, Operator, Inspector

#### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

#### Syntax Description

```
show active-charging edr-format [ statistics ] [ all | name edr_format_name ] [ | { grep grep_options | more } ]
```

**all**

Displays information for all EDR formats.

**statistics**

Displays statistics for all or an existing EDR format.

If neither **all** nor **name** is specified, summarized statistics over all EDR formats is displayed.

**name *edr\_format\_name***

Displays information for an existing EDR format specified as an alphanumeric string of 1 through 63 characters.

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display information for EDR format(s) in the ACS.

**Example**

The following command displays all configured EDR formats in the ACS.

```
show active-charging edr-format all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging edr-udr-file

Displays CDR flow control information. This command also displays the Event Data Record (EDR) and Usage Data Record (UDR) file information.

**Product**

ACS

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show active-charging edr-udr-file { flow-control-counters [ verbose ] |
statistics } [ | { grep grep_options | more } ]
```

**flow-control-counters [ verbose ]**

Displays the counters for dropped EDR/UDR records. These counters are for when CDRMOD uses flow control to stop ACS/Session Managers from sending the records.

**verbose** displays detailed information.

**statistics****Important**

This keyword is obsolete. The option is now supported through the **show cdr** command.

Displays EDR and UDR file statistics.

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view CDR flow control information.

**Example**

The following command displays EDR and UDR files statistics:

```
show active-charging edr-udr-file statistics
```

The following command displays CDR flow control information:

```
show active-charging edr-udr-file flow-control-counters
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging file-space-usage

Displays the file space used by Charging Data Record (CDR) and Event Data Record (EDR) files.

**Product**

ACS

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```



**Syntax Description** `show active-charging file-space-usage [ | { grep grep_options | more } ]`

`| { grep grep_options | more }`

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines** Use this command to view CDR/EDR file space usage information. The context in which this command is used is not relevant.

### Example

The following command displays CDR/EDR file space usage:

```
show active-charging file-space-usage
```

## show active-charging firewall dos-protection

Displays the list of servers involved in any IP Sweep attacks.

**Product** PSF

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

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `show active-charging firewall dos-protection ip-sweep server-list { all | instance instance_num } [ | { grep grep_options | more }`

**all**

Displays the IP Sweep server list for all instances.

**instance** *instance\_num*

Displays statistics for the specified ACS Manager instance.

*instance\_num* must be an integer from 1 through 65535.

`| { grep grep_options | more }`

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display the list of servers involved in any IP Sweep attacks.

**Example**

The following command displays the IP Sweep server list for all instances:

```
show active-charging firewall dos-protection ip-sweep server-list all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging firewall statistics

Displays Active Charging Stateful Firewall statistics.

**Product**

PSF

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show active-charging firewall statistics [ callid call_id | domain-name
domain_name | nat-realm nat_realm_name | protocol { icmp | icmpv6 | ip | ipv6
| other | tcp | udp } | username user_name ] [ acsmgr instance instance_number
] [ verbose ] [ wide ] [ | { grep grep_options | more } ]
```

**acsmgr instance** *instance\_number*

Specifies the ACS/Session Manager instance ID as an integer from 1 through 65535.

**callid** *call\_id*

Specifies the call identification number as an 8-digit hexadecimal number.

**domain-name** *domain\_name*

Specifies the domain name as an alphanumeric string of 1 through 127 characters.

**nat-realm** *nat\_realm\_name*

Specifies the NAT realm name as an alphanumeric string of 1 through 31 characters.

**protocol** { **icmp** | **ip** | **other** | **tcp** | **udp** }

Specifies the protocol:

- **icmp**: ICMPv4

- **icmpv6**
- **ip**: IPv4
- **ipv6**
- **other**: Protocols other than TCP, UDP, and ICMPv4/ICMPv6.
- **tcp**
- **udp**

**username** *user\_name*

Specifies the user name as an alphanumeric string of 1 through 127 characters.

**verbose**

Specifies to display detailed (all available) information. If not specified, concise information is displayed.

**wide**

Displays all available information in a single wide line.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view Stateful Firewall statistics. If you are in the local context, statistics for all contexts are displayed. Otherwise, only statistics of your current context are displayed.

**Example**

The following command displays Stateful Firewall statistics:

```
show active-charging firewall statistics
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

# show active-charging firewall track-list

Displays the list of servers being tracked for involvement in any Denial-of-Service (DOS) attacks.

**Product**

PSF

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show active-charging firewall track-list attacking-servers [ | { grep
grep_options | more } ]
```

```
| { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view details of servers being tracked for involvement in any DOS attack.

**Example**

The following command displays the list of servers being tracked for involvement in any DOS attacks:

```
show active-charging firewall track-list attacking-servers
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging flow-control-counters

Displays information for dropped EDR and UDR records.

**Product**

ACS

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show active-charging flow-control-counters [ verbose ] [ | { grep
grep_options | more } ]
```

**verbose**

Specifies to display detailed (all available) information. If not specified, concise information is displayed.

**{ { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to view EDR-UDR flow control information—for dropped EDR and UDR records.

### Example

The following command displays detailed EDR-UDR flow control information:

```
show active-charging flow-control-counters verbose
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging flow-kpi

Displays information about the cumulative KPI for ECS rule(s) across session managers.

### Product

ACS

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show active-charging flow-kpi sessmgr { all | instance instance_id } [ | {  
  grep grep_options | more } ]
```

#### all

Displays the KPI information for all rules.

#### instance *instance\_id*

Displays information for all rules based on session manager instance, specified as an integer ranging from 1 through 65535.

**{ { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view the cumulative KPI for ECS rule(s) across session managers.

This command is added in support of the Flow Recovery feature, that requires a separate feature license.

**Example**

The following command displays the KPI information for all rules:

```
show active-charging flow-kpi all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging flow-mappings

Displays information about all the active flow mappings based on the applied filters.

**Product**

PSF  
NAT

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show active-charging flow-mappings [ all | call-id call_id | [ nat {
not-required | required [ nat-realm nat_realm_name ] } | trans-proto { tcp
| udp } ] + [ | { grep grep_options | more } ]
```

**all**

Displays all the available active-charging flow-mapping information.

**call-id *call\_id***

Displays detailed information for a call ID specified as an 8-digit hexadecimal number.

**nat { required [ nat-realm *string* ] not-required }**

Displays the active charging flow mappings for which NAT is enabled or disabled.

**trans-proto { tcp | udp }**

Displays the transport layer.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to view the Active Charging flow-mapping details.

### Example

The following command displays the total number of Active Charging flow-mappings:

```
show active-charging flow-mappings all
```

The following command displays the flow-mappings for which NAT is enabled and the NAT-realm used is *natpool3*:

```
show active-charging flow-mappings nat required nat-realm natpool3
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging flows

Displays information for active charging flows.

### Product

ACS

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show active-charging flows { all | [ callid call_id ] [ connected-time [ <
| > | greater-than | less-than ] seconds ] [ control-connection { ftp |
pptp | rtsp | sip | tftp } ] [ flow-id flow_id ] [ full ] [ idle-time [ <
| > | greater-than | less-than ] seconds ] [ firewall { not-required |
required } ] [ imsi imsi_value ] [ ip-address [ server | subscriber ] [ <
| > | IPv4 | greater-than | less-than ] address ] [ msisdn msisdn_num ] [ nat
{ not-required | required [ nat-ip nat_ip_address ] [ binding-info ] } ] [
pacing-bitrate [ < | > | = | greater-than | less-than | equal-to ] number
[ port-number [ server | subscriber ] [ < | > | IPv4 | greater-than |
less-than ] number ] [ rx-bytes [ < | > | greater-than | less-than ] number
] [ rx-packets [ < | > | greater-than | less-than ] number ] [ session-id
session_id ] [ summary ] [ trans-proto { icmp | tcp | udp } ] [ tx-bytes
[ < | > | greater-than | less-than ] number ] [ tx-packets [ < | > |
```

```
greater-than | less-than ] number ] [ type flow_type ] [ username user_name ]
} [ | { grep grep_options | more } ]
```

**all**

Displays information for all active charging flows.

**callid *call\_id***

Displays the specific Call Identification Number. *call\_id* must be an eight digit hexadecimal number.

**connected-time [ < | > | greater-than | less-than ] seconds**

Displays information for flows filtered by connected time period.

- **< seconds**: Displays flows that have been connected less than the specified number of seconds.
- **> seconds**: Displays flows that have been connected more than the specified number of seconds.
- **greater-than seconds**: Displays flows that have been connected more than the specified number of seconds.
- **less-than seconds**: Displays flows that have been connected less than the specified number of seconds.

*seconds* is an integer from 0 through 4294967295.

**control-connection { ftp | pptp | rtsp | sip | tftp }**

Displays information for control connection of flows.

- **ftp**: Displays control connection information for the FTP flow.
- **pptp**: Displays control connection information for the PPTP flow.
- **rtsp**: Displays control connection information for the RTSP flow.
- **sip**: Displays control connection information for the SIP flow.
- **tftp**: Displays control connection information for the TFTP flow.

**firewall { not-required | required }**

Displays information for flows filtered by Firewall required or not required setting.

- **not-required**: Sessions with Firewall processing are not required.
- **required**: Sessions with Firewall processing are required.

**flow-id *flow\_id***

Displays concise information for specified active charging flow ID.

**full**

Displays all available information for the specified flows.



**idle-time [ < | > | greater-than | less-than ] seconds**

Displays information for flows filtered by idle time period.

- **< seconds**: Displays flows that have been idle less than the specified number of seconds.
- **> seconds**: Displays flows that have been idle more than the specified number of seconds.
- **greater-than seconds**: Displays flows that have been idle more than the specified number of seconds.
- **less-than seconds**: Displays flows that have been idle less than the specified number of seconds.

*seconds* is an integer from 0 through 4294967295.

**imsi *imsi\_value***

Displays information for an International Mobile Subscriber Identity (IMSI). *imsi\_value* must be a sequence of digits and/or wild characters.

**ip-address [ server | subscriber ] [ < | > | IPv4 | greater-than | less-than ] address**

Displays information for flows filtered by IPv4 IP address.

- **server**: Specifies the IP address for a specific server.
- **subscriber**: Displays subscriber details for the IP address specified in IPv4 dotted-decimal format.
- **< address**: Specifies an IPv4 IP address that is less than *address*.
- **> address**: Specifies an IPv4 IP address that is greater than *address*.
- **greater-than address**: Specifies an IPv4 IP address that is greater than *address*.
- **less-than address**: Specifies an IPv4 IP address that is less than *address*.

*address* is an IP address expressed in IPV4 dotted-decimal notation.

**msisdn *msisdn\_num***

Displays information for the mobile user identified by the Mobile Subscriber ISDN Number (MSISDN). *msisdn\_num* must be a numeric string of 1 to 15 digits.

**nat { not-required | required [ nat-ip *nat\_ip\_address* [ nat-port *nat\_port* ] ] [ binding-info ] }****Important**

The **nat** keyword and options are only available in StarOS 8.3 and later releases.

Displays information for flows filtered by Network Address Translation (NAT) required or not required setting.

- **not-required**: Sessions with NAT processing are not required.
- **required**: Sessions with NAT processing are required.
- **nat-ip *nat\_ip\_address***: Sessions using the NAT IP address expressed in IPv4 dotted-decimal notation.

- **nat-port** *nat\_port*: Sessions using the specified NAT IP address and NAT port number specified as an integer from 0 through 65535.
- **binding-info**: Displays the NAT binding information of the NATed flow.

**pacing-bitrate [ < | > | = | greater-than | less-than | equal-to ] *number***

Displays information on video flows filtered by a video pacing bit rate specified an integer from 1 to 256000000.

- *< number*: Specifies a number that is less than the specified video pacing bit rate.
- *> number*: Specifies a number that is greater than the specified video pacing bit rate.
- *= number*: Specifies a number that is equal to the specified video pacing bit rate.
- **greater-than** *number*: Specifies a number that is greater than the specified video pacing bit rate.
- **less-than** *number*: Specifies a number that is less than the specified video pacing bit rate.
- **equal-to** *number*: Specifies a number that is equal to the specified video pacing bit rate.

**port-number [ server | subscriber ] [ < | > | IPv4 | greater-than | less-than ] *\_number***

Displays information on flows filtered by port number.

- **server**: Specifies the port-number for a specific server.
- **subscriber**: Specifies subscriber details for this port-number, and must be an integer from 0 through 65535.
- *< number*: Specifies a port number that is less than the specified port-number.
- *> number*: Specifies a port number that is greater than the specified port-number.
- **greater-than** *number*: Specifies a port number that is greater than the specified port-number.
- **less-than** *number*: Specifies a port number that is less than the specified port-number.

**rx-bytes [ < | > | greater-than | less-than ] *number***

Displays information on flows filtered by the number of bytes received in the flow.

- *< number*: Specifies the number of bytes that is less than the specified rx-bytes.
- *> number*: Specifies number of bytes that is greater than the specified rx-bytes.
- **greater-than** *number*: Specifies number of bytes that is greater than the specified rx-bytes.
- **less-than** *number*: Specifies number of bytes that is less than the specified rx-bytes.

*number* must be an integer from 0 through 18446744073709551615.

**rx-packets [ < | > | greater-than | less-than ] *number***

Displays information on flows filtered by the number of packets received in the flow.

- **greater-than** *number*: Specifies the number of packets that is greater than the specified rx-packets.

- **less-than** *number*: Specifies the number of packets that is less than the specified rx-packets.

*number* must be an integer from 0 through 18446744073709551615.

#### **session-id** *session\_id*

Displays detailed information for specific active charging session ID.

#### **summary**

Displays summary information for defined sessions, based on defined parameters.

#### **trans-proto** { **icmp** | **tcp** | **udp** }

Displays information on flows filtered by the transport protocol.

- **icmp**: ICMP protocol type flow
- **tcp**: TCP protocol type flow
- **udp**: User Datagram Protocol (UDP) flows

#### **tx-bytes** [ < | > | **greater-than** | **less-than** ] *number*

Displays information on flows filtered by the number of bytes received in the flow.

- < *number*: Specifies the number of bytes that is less than the specified tx-bytes.
- > *number*: Specifies number of bytes that is greater than the specified tx-bytes.
- **greater-than** *number*: Specifies number of bytes that is greater than the specified tx-bytes.
- **less-than** *number*: Specifies number of bytes that is less than the specified tx-bytes.

*number* must be an integer from 0 through 18446744073709551615.

#### **tx-packets** [ < | > | **greater-than** | **less-than** ] *number*

Displays information on flows filtered by the number of packets received in the flow.

- **greater-than** *number*: Specifies the number of packets that is greater than the specified tx-packets.
- **less-than** *number*: Specifies the number of packets that is less than the specified tx-packets.

*number* must be an integer from 0 through 18446744073709551615.

#### **type** *flow\_type*

Displays information on flows filtered by flow type of application protocol.

*flow\_type* must be one of the following:

- **dns**
- **ftp**
- **http**

- **icmp**
- **icmpv6**
- **imap**
- **ip**
- **ipv6**
- **mms**
- **p2p** [ **application** *p2p\_list* [ **traffic-type** *traffic\_type* ] | **protocol-group** *group\_list* ]: Peer-to-peer analyzer.

**p2p application** *p2p\_list*: P2P protocol type flows include one or more of the following applications:

- **8tracks**
- **abcnetworks**
- **actionvoip**
- **actsync**
- **adobeconnect**
- **aimini**
- **amazoncloud**
- **amazonmusic**
- **amazonvideo**
- **antisp2p**
- **apple-push**
- **apple-store**
- **applejuice**
- **applemaps**
- **ares**
- **armagettron**
- **avi**
- **badoo**
- **baidumovie**
- **battlefld**
- **bbm**
- **beatport**
- **betternet**

- bitcasa
- bittorrent
- bittorrent-sync
- blackberry-store
- blackberry
- blackdialer
- box
- callofduty
- chikka
- cisco-jabber
- citrix
- clubbox
- clubpenguin
- crackle
- crossfire
- crunchyroll
- cyberghost
- ddrlink
- deezer
- didi
- directconnect
- dish-anywhere
- disneymovies
- dofus
- dramafever
- dropbox
- edonkey
- espn
- expressvpn
- facebook
- facetime
- fandor

- fasttrack
- feidian
- fiesta
- filetopia
- filmontv
- flash
- flickr
- florensia
- foursquare
- fox-sports
- freenet
- friendster
- fring
- funshion
- gadu\_gadu
- gamekit
- gmail
- gnutella
- go90
- goober
- google-music
- google-push
- google
- googleplay
- googleplus
- gotomeeting
- gtalk
- guildwars
- halflife2
- hamachivpn
- hayu
- hbogo

- hbonow
- heytell
- hgtv
- hike-messenger
- hls
- hotspotvpn
- hulu
- hyves
- iax
- icall
- icecast
- icloud
- idrive
- igo
- iheartradio
- imesh
- imessage
- imgur
- imo
- instagram
- iplayer
- iptv
- irc
- isakmp
- iskoot
- itunes
- jabber
- jap
- jumblo
- kakaotalk
- kik-messenger
- kontiki

- kugoo
- kuro
- linkedin
- livestream
- lync
- magicjack
- manolito
- mapfactor
- mapi
- maplestory
- meebo
- mgcp
- mlb
- mojo
- monkey3
- mozy
- msn
- msrp
- mute
- mypeople
- Myspace
- nateontalk
- naverline
- navigon
- nbc-sports
- netmotion
- newsy
- nick
- nimbuzz
- nokia-store
- octoshape
- off



- **ogg**
- **oist**
- **oovoo**
- **opendrive**
- **openft**
- **openvpn**
- **orb**
- **oscar**
- **outlook**
- **paltalk**
- **pando**
- **pandora**
- **path**
- **pbs**
- **pcanywhere**
- **periscope**
- **pinterest**
- **plingm**
- **poco**
- **popo**
- **pplive**
- **ppstream**
- **ps3**
- **qq**
- **qqgame**
- **qqlive**
- **quake**
- **quic**
- **quicktime**
- **radio-paradise**
- **radius**
- **rdp**

- rdt
- regram
- rfactor
- rhapsody
- rmstream
- rodi
- rynga
- samsung-store
- scydo
- secondlife
- shoutcast
- showtime
- silverlight
- siri
- skinny
- skydrive
- skype
- slacker-radio
- slingbox
- slingtv
- smartvoip
- snapchat
- softether
- soapcast
- soribada
- soulseek
- soundcloud
- spark
- spdy
- speedtest
- spike
- splashfighter

- **spotify**
- **ssdp**
- **starz**
- **stealthnet**
- **steam**
- **stun**
- **sudaphone**
- **svtplay**
- **tagged**
- **talkatone**
- **tango**
- **teamspeak**
- **teamviewer**
- **telegram**
- **thunder**
- **tinder**
- **tmo-tv**
- **tor**
- **truecaller**
- **truphone**
- **tumblr**
- **tunein-radio**
- **tunnelvoice**
- **turbovpn**
- **tvants**
- **tvland**
- **tvuplayer**
- **twitch**
- **twitter**
- **ultrabac**
- **ultrasurf**
- **univision**

- **upc-phone**
- **usenet**
- **ustream**
- **uusee**
- **vchat**
- **veohtv**
- **vessel**
- **vevo**
- **viber**
- **vine**
- **voipdiscount**
- **vopium**
- **vpnmaster**
- **vpn**
- **voxer**
- **vtok**
- **vtun**
- **vudu**
- **warcft3**
- **waze**
- **webex**
- **wechat**
- **whatsapp**
- **wii**
- **windows-azure**
- **windows-store**
- **winmx**
- **winny**
- **wmstream**
- **wofkungfu**
- **wofwarcraft**
- **wuala**

- **xbox**
- **xdcc**
- **xing**
- **yahoo**
- **yahoomail**
- **yiptv**
- **youku**
- **yourfreetunnel**
- **youtube**
- **zattoo**

**traffic-type** *traffic\_type*: P2P protocol flows include the following traffic type classifications:



---

**input** The traffic type for a P2P protocol may vary depending on the P2P protocol.

---

- **ads**
- **audio**
- **file-transfer**
- **im**
- **video**
- **voipout**
- **unclassified**

**p2p protocol-group** *group\_list*: The following P2P protocol groups are supported:

- generic
- anonymous-access
- business
- communicator
- cloud
- e-store
- e-mail
- e-news
- internet-privacy
- filesharing
- gaming
- p2p-filesharing
- p2p-anon-filesharing

- remote-control
- social-nw-gaming
- social-nw-generic
- social-nw-videoconf
- standard
- streaming
- **pop3**
- **pptp**
- **rtcp**
- **rtp**
- **rtsp**
- **secure-http**
- **sip**
- **smtp**
- **tcp**
- **tftp**
- **udp**
- **unknown**: Unknown type of protocol type flow not listed here.
- **wsp-connection-less**
- **wsp-connection-oriented**

**username** *user\_name*

Specifies the user name as a sequence of characters and/or wildcard characters (\$ and \*). *user\_name* must be an alphanumeric string of 1 through 127 characters.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Use this command to display charging flow type information.

**Example**

The following command displays a detailed flow information for a session ID of *test*:

```
show active-charging flows session-id test
```

The following command displays a detailed flow information for a P2P type session:

```
show active-charging flows full type p2p
```

The following command displays a detailed information for a P2P type flow:

```
show active-charging flows type p2p
```




---

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show active-charging fw-and-nat policy

Displays Firewall-and-NAT Policy information.




---

**Important**

This command is only available in StarOS 8.1, and in StarOS 9.0 and later. For more information on this command please contact your local service representative.

---



---

**Product**

ACS  
PSF  
NAT

---

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
show active-charging fw-and-nat policy { { { all | name fw_nat_policy_name }
[ service name acs_service_name ] } | { statistics { all | name
fw_nat_policy_name } } } [ | { grep grep_options | more } ]
```

**all**

Displays information for all Firewall-and-NAT policies configured, optionally all in a specified service.

**name fw\_nat\_policy\_name**

Displays detailed information for an existing Firewall-and-NAT policy specified as an alphanumeric string of 1 through 63 characters.

**service name acs\_service\_name**

Displays information for all or the specified Firewall-and-NAT policy in the specified ACS.

*acs\_service\_name* must be the name of the active-charging service, and must be an alphanumeric string of 1 through 15 characters.

**statistics**

Displays statistics for all or the specified Firewall-and-NAT policy.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view Firewall-and-NAT Policy information.

**Example**

The following command displays detailed information for the Firewall-and-NAT policy named *standard*:

```
show active-charging fw-and-nat policy name standard
```

## show active-charging group-of-objects

Displays information for ACS group-of-objects.

**Product**

ACS

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show active-charging group-of-objects { all | name group_of_objects_name } [
| { grep grep_options | more } ]
```

**all**

Displays details of all group-of-objects configured in the system.

**name *group\_of\_objects\_name***

Displays details for the specified group-of-objects.

*group\_of\_objects\_name* must be the name of a group-of-objects, and must be an alphanumeric string of 1 through 63 characters.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.



For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to view information for all/specific group-of-objects.

### Example

The following command displays information for a group-of-objects named *test*.

```
show active-charging group-of-objects name test
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging group-of-prefixed-urls

D displays information on group of prefixed URLs configured in an Active Charging Service (ACS).

### Product

ACS

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show active-charging group-of-prefixed-urls { all | name prefixed_url_group
} [ service name acs_service_name ] [ | { grep grep_options | more } ]
```

#### all

Displays information for all group of prefixed URLs configured in an ACS.

#### name *prefixed\_url\_group*

Displays detailed information for the group of prefixed URLs specified as an alphanumeric string of 1 through 63 characters.

#### service name *acs\_service\_name*

Displays information for all or the specified group of prefixed URLs in the specified ACS. *acs\_service\_name* must be the name of the ACS expressed as alphanumeric string of 1 through 15 characters.

#### { grep *grep\_options* | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter

### Usage Guidelines

Use this command to view information on group of prefixed URLs configured in the ACS.

### Example

The following command displays for the group of prefixed URLs named *test123*:

```
show active-charging group-of-prefixed-urls name test123
```

## show active-charging group-of-ruledefs

Displays information for all groups or a specified group of ruledefs configured in the Active Charging Service (ACS).

### Product

ACS

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show active-charging group-of-ruledefs { { all | name group_of_ruledefs_name
} [ service name acs_service_name ] | statistics name group_of_ruledefs_name }
[ | { grep grep_options | more } ]
```

#### all

Displays information for all groups of ruledefs configured, optionally all in a specified ACS.

#### name *group\_of\_ruledefs\_name*

Displays detailed information for an existing group of ruledefs specified as an alphanumeric string of 1 through 63 characters.

#### service name *acs\_service\_name*

Displays information for all groups or the specified group of ruledefs within the ACS. *acs\_service\_name* must be the name of the ACS, and must be an alphanumeric string of 1 through 15 characters.

#### statistics name *group\_of\_ruledefs\_name*

Displays statistics for an existing group of ruledefs specified as an alphanumeric string of 1 through 63 characters.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to view information on group of ruledefs configured in a ACS.

### Example

The following command displays information on all groups of ruledefs configured:

```
show active-charging group-of-ruledefs all
```

## show active-charging nat statistics

Displays Network Address Translation (NAT) realm statistics.

### Product

NAT

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show active-charging nat statistics [ instance instance_number | nat-realm  
nat_realm_name [ summary ] | unsolicited-pkts-server-list [ instance  
instance_number ] ] [ | { grep grep_options | more } ]
```

### show active-charging nat statistics

When issued in the local context, this command displays statistics for all NAT realms in all contexts. When issued in a specific context, this command displays statistics for all NAT realms in that context.

### show active-charging nat statistics instance *instance\_number*

When issued in the local context, this command displays statistics for the specified ACS/Session Manager instance in all contexts. When issued in a specific context, this command displays statistics for the specified ACS/Session Manager instance in that context.

### show active-charging nat statistics nat-realm *nat\_realm\_name*

When issued in the local context, this command displays statistics for the specified NAT realm in all contexts. When issued in a specific context, this command displays statistics for the specified NAT realm in that context.

**show active-charging nat statistics unsolicited-pkts-server-list instance *instance\_num***

When issued in the local context, this command displays statistics for unsolicited packets in all contexts. When issued in a specific context, this command displays statistics for unsolicited packets that context.

*instance\_number* must be an integer from 1 through 65535.

**nat-realm *nat\_realm\_name***

Specifies the NAT realm's / NAT realm group's name.

*nat\_realm\_name* must be an alphanumeric string of 1 through 31 characters.

**instance *instance\_number***

Displays statistics for the specified ACS/Session Manager instance.

*instance\_number* must be an integer from 1 through 65535.

**summary**

When the *nat\_realm\_name* specified is a "pool group" and the **summary** option is used, summary statistics of all pools in the pool group are displayed.

When the *nat\_realm\_name* specified is a pool and the **summary** option is not used, all available statistics for the specified pool are displayed.

When the *nat\_realm\_name* specified is a "pool group" and the **summary** option is not used, all available statistics of each pool in the specified "pool group" are displayed.

**unsolicited-pkts-server-list**

Displays statistics with the list of servers from where most number of unsolicited packets are received for the specified ACS/Session Manager instance.

**| { *grep grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view NAT realm statistics.

**Example**

The following command when issued in the local context, displays NAT realm statistics for NAT realms named *test135* in all contexts:

```
show active-charging nat statistics nat-realm test135
```

## show active-charging p2p-dynamic-rules

This command is under development for a future release and is not supported in this release. This command displays P2P Dynamic signature file information.

**Product** ADC

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

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **show active-charging p2p-dynamic-rules** [ **verbose** ] [ **acsmgr instance** *instance\_number* ] [ | { **grep** *grep\_options* | **more** } ]

**acsmgr instance** *instance\_number*

Specifies the ACS/Session Manager instance ID as an integer from 1 through 65535.

**verbose**

Displays P2P Dynamic rule statistics in detail.

| { **grep** *grep\_options* | **more** }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines** Use this command to view P2P Dynamic signature file statistics/information.

**Example**

The following command displays P2P Dynamic rule information:

```
show active-charging p2p-dynamic-rules
```

## show active-charging packet-filter

Displays information on packet filters configured in an Active Charging Service (ACS).

**Product** ACS

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

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show active-charging packet-filter { all | name packet_filter_name } [ service
name acs_service_name ] [ | { grep grep_options | more } ]
```

**all**

Displays information for all packet filters configured, optionally all configured in an ACS.

**name** *packet\_filter\_name*

Displays detailed information for an existing packet filter specified as an alphanumeric string of 1 through 63 characters.

**service name** *acs\_service\_name*Displays information for all filters or the specified packet filter in the specified ACS. *acs\_service\_name* must be the name of the ACS specified as an alphanumeric string of 1 through 15 characters.| { **grep** *grep\_options* | **more** }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.**Usage Guidelines**

Use this command to view information on packet filters configured in an ACS.

**Example**The following command displays information for the packet filter *filter12*:

```
show active-charging packet-filter name filter12
```

## show active-charging pcp-service

Displays statistics for Port Control Protocol (PCP) service in the Active Charging Service (ACS).

**Important**

This command is customer specific. For more information contact your Cisco account representative.

**Product**

ACS

NAT

PSF

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show active-charging pcp-service { all | name pcp_service_name | statistics
[ instance instance_number | name pcp_service_name | wide ] } [ | { grep
grep_options | more } ]
```

**all**

Displays information for all PCP services configured in the service.

**name pcp\_service\_name**

Displays information for an existing PCP service specified as an alphanumeric string of 1 through 63 characters.

**statistics [ instance instance\_number | name pcp\_service\_name | wide ]**

Displays statistical information for all configured PCP services.

- **instance instance\_number**: Displays statistics for the specified ACS/Session Manager instance.
- **name pcp\_service\_name**: Displays statistics for the specified PCP service.
- **wide**: Displays all available information in a single wide line.

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.**Usage Guidelines**

Use this command to view statistics for PCP service in the ACS.

**show active-charging pcp-service statistics**: The output of this command displays statistics for all PCP services in all contexts when issued in the local context. When issued in a specific context, this command displays statistics for all PCP services in that context.**show active-charging pcp-service instance instance\_number**: When issued in the local context, this command displays statistics for the specified ACS/Session Manager instance in all contexts. When issued in a specific context, this command displays statistics for the specified ACS/Session Manager instance in that context.**show active-charging pcp-service name pcp\_service\_name**: The output of this command displays the statistics for the specified PCP service.**Example**The following command displays PCP service statistics for a PCP service named *pcp1*:

```
show active-charging pcp-service statistics name pcp1
```




---

**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show active-charging qos-group-of-ruledefs

Displays information for ACS QoS-group-of-ruledefs.

<b>Product</b>	ACS
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **show active-charging qos-group-of-ruledefs** { **all** | **name** *qos\_group\_of\_ruledefs\_name* } [ | { **grep** *grep\_options* | **more** } ]

### all

Displays details of all qos-group-of-ruledefs configured in the system.

### name *qos\_group\_of\_ruledefs\_name*

Displays details for the specified qos-group-of-ruledefs.

*qos\_group\_of\_ruledefs\_name* must be the name of a qos-group-of-ruledefs, and must be an alphanumeric string of 1 through 63 characters.

### | { **grep** *grep\_options* | **more** }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines** Use this command to view details of all/specific qos-group-of-ruledefs.

### Example

The following command displays of a qos-group-of-ruledefs named *test*.

```
show active-charging qos-group-of-ruledefs name test
```




---

**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

---



# show active-charging regex

Displays regular expression (regex) related statistics and information.

---

**Product**

ACS

---

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
show active-charging regex { statistics { memory | ruledef } { all | instance instance_number | summary } | status { all | instance instance_number } } [ | { grep grep_options | more } ]
```

**statistics { memory | ruledef } { all | instance instance\_number | summary }**

Displays regex-related statistics.

- **memory**: Displays regex memory related statistics.
- **ruledef**: Displays regex ruledef related statistics.
- **all**: Displays specified statistics for all Session Manager instances.
- **instance instance\_number**: Displays specified statistics for specified Session Manager instance. *instance\_number* must be an integer from 1 through 65535.
- **summary**: Displays summary information for specified parameter.

**status { all | instance instance\_number }**

Displays status information of regex engines.

- **all**: Displays status for all regex engines.
- **instance instance\_number**: Displays status of regex engine for specified Session Manager instance. *instance\_number* must be an integer from 1 through 65535.

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Use this command to view regular expression (regex) related statistics and status of regex engines.

**Example**

The following command displays status information of all regex engines:

```
show active-charging regex status all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging rulebase

Displays information for ACS rulebases.

**Product**

ACS

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show active-charging rulebase { { { all | name rulebase_name } [ service
name acs_service_name ] } | statistics [ name rulebase_name ] } [ | { grep
grep_options | more } ]
```

**all**

Displays details of all rulebases configured in the system.

**name *rulebase\_name***

Displays details of an existing rulebase specified as an alphanumeric string of 1 through 63 characters.

**service name *acs\_service\_name***

Displays details of all or the specified rulebase configured in the specified ACS. *acs\_service\_name* must be the name of the ACS, and must be an alphanumeric string of 1 through 15 characters.

**statistics**

Displays statistical information for all or the specified rulebase.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view various statistics for a specific charging rulebase.

**Example**

The following command displays active charging rulebase statistics.

```
show active-charging rulebase statistics
```

The following command displays configurations and statistics for a rulebase named *rulebase\_1*.

```
show active-charging rulebase name rulebase_1
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging ruledef

Displays information for ACS ruledefs.

**Product**

ACS  
PSF

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show active-charging ruledef { all | charging | firewall | name ruledef_name
| post-processing | routing | statistics [ all { charging | firewall [
wide ] | post-processing | tpo } | name ruledef_name [ wide ] ] | tpo } [ |
{ grep grep_options | more } ]
```

**all**

Displays information for all ruledefs configured in the ACS.

**charging**

Displays information for all Charging ruledefs configured in the ACS.

**firewall**

Displays information for all Stateful Firewall ruledefs configured in the ACS.

**name *ruledef\_name***

Displays detailed information for an existing ruledef specified as an alphanumeric string of 1 through 63 characters.

**post-processing**

Displays information for all post-processing ruledefs configured in the ACS.

**routing**

Displays information for all Routing ruledefs configured in the ACS.

**service *service\_name***

This keyword is obsolete.

**statistics [ all { charging | firewall [ wide ] | post-processing | tpo } | name *ruledef\_name* [ wide ] ]**

Displays statistical information for all/specified ruledefs configured in the ACS. If none of the optional arguments are supplied, statistics totaled for all ruledefs will be displayed.

- **all**: Displays statistics for all ruledefs of the specified type configured in the ACS.
- **charging**: Displays statistics for all Charging ruledefs configured in the ACS.
- **firewall**: Displays statistics for all Firewall ruledefs configured in the service.
- **post-processing**: Displays statistics for all Post-processing ruledefs configured in the ACS.
- **tpo**




---

**Important** The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

---

- **name *ruledef\_name***: Displays statistics for an existing ruledef specified as an alphanumeric string of 1 through 63 characters.
- **wide**: Displays all available information in a single wide line.

**tpo**


---

**Important** The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

---

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view information for ruledefs configured in the ACS.

**Example**

The following command displays ACS ruledef statistics.

```
show active-charging ruledef statistics
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging service

Displays detailed information about an Active Charging Service (ACS).

**Product**

ACS

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show active-charging service { all | name acs_service_name } [ | { grep
grep_options | more } ]
```

**all**

Displays information for all configured ACSs.

**name acs\_service\_name**

Displays detailed information for the ACS specified as an alphanumeric string of 1 through 15 characters.

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view ACS details.

**Example**

The following command displays details for the ACS named *test1*.

```
show active-charging service name test1
```



**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging service-scheme

Displays statistics and information on active subscribers.

<b>Product</b>	ACS
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **show active-charging service-scheme** { **all** | **name** *serv\_scheme\_name* | **statistics** [ **name** *serv\_scheme\_name* ] } [ **service name** *service\_name* ] [ | { **grep** *grep\_options* | **more** } ]

### **all**

Displays information for all service schemes configured in a service.

### **name** *serv\_scheme\_name*

Displays detailed information for a specific service scheme.

*serv\_scheme\_name* must be an alphanumeric string of 1 through 63 characters.

### **statistics** [ **name** *serv\_scheme\_name* ]

Displays the related statistics for the service-scheme.

**name** *serv\_scheme\_name* must be the name of a service-scheme and must be an alphanumeric string of 1 through 63 characters.

### **service** *service\_name*

Displays service and configuration counters for the specific active charging service.

*service\_name* must be an alphanumeric string of 1 through 15 characters.

### | { **grep** *grep\_options* | **more** }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view subscriber statistics and information on dynamic updates to charging parameters per call ID.

**Example**

The following command displays all service-scheme statistics for the configured service-scheme *ss1*:

```
show active-charging service-scheme statistics name ss1
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging sessions

Displays statistics for Active Charging Service (ACS) sessions.

**Product**

ACS

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show active-charging sessions [ full [ wide ] | wf1 | summary ] [
filter_keyword + ] + [ all ] [ | { grep grep_options | more } ]
```

**full [ wide ]**

Displays all available information for the specified session.

Optionally all available information can be displayed in a single wide line.

**summary**

Displays active sessions count and packet and bytes statistics.

**wf1**

Displays all available information including MSISDN and rulebase in a single wide line.

**display-dynamic-charging-rules**

Displays information for the dynamic charging rules configured per session under Gx interface support.

**dynamic-charging**

Displays information for dynamic charging sessions.

***filter\_keyword***

The following keywords are filters that modify or filter the output of the Command Keywords. Not all filters are available for all command keywords. Multiple filter keywords can be entered on a command line.

When multiple filter keywords are specified, the output conforms to all of the filter keywords specifications.

For example, if you enter the following command:

**show active-charging sessions full active-charging-service acs\_!**

Counters for active charging sessions active in ACS *acs\_1* with full details is displayed. Information for all other services is not displayed.

**acsmgr instance *instance\_number***

Displays session information for a specific ACS/Session Manager instance.

**active-charging-service *acs\_service\_name***

Displays session information for the ACS specified as an alphanumeric string of 1 through 15 characters.

**all**

Displays session information for all active charging sessions.

**cae-readdressing**

Displays the Content Adaptation Engine (CAE) re-addressing session information for active charging sessions.

**callid**

Specifies the call identification number.

**display-dynamic-charging-rules**

Displays dynamic charging rules configured.

**dynamic-charging**

Displays session information for all dynamic charging sessions.

**firewall { not-required | required }**

Displays session information for sessions with Firewall Processing required or not required, as specified.

**flows { active | idle | total } [ < | = | > | equal-to | greater-than | less-than ] { bytes }**

Displays information for all active charging flows filtered by all information, active, or idle sessions.

- < *bytes* or **less-than** *bytes*: Specifies filtering of flows that is less than the specified number of bytes.
- > *bytes* or **greater-than** *bytes*: Specifies filtering of flows that is greater than the specified number of bytes.
- = *bytes* or **equal-to** *bytes*: Specifies filtering of flows that is equal to the specified number of bytes.



*bytes* must be an integer from 0 through 18446744073709551615.

#### **fw-and-nat policy *fw\_nat\_policy\_name***

Displays information for the Firewall-and-NAT Policy specified as an alphanumeric string of 1 through 63 characters.

#### **imsi**

Specifies the International Mobile Subscriber Identity (IMSI) of the subscriber session.

#### **ip-address**

Specifies the IP address for the specific charging service.

#### **max-flows { < | = | > | equal-to | greater-than | less-than } { *bytes* }**

Displays information for the maximum flows made by the session.

- < *bytes* or **less-than** *bytes*: Specifies filtering of maximum flows that is less than the specified number of bytes.
- > *bytes* or **greater-than** *bytes*: Specifies filtering of maximum flows that is greater than the specified number of bytes.
- = *bytes* or **equal-to** *bytes*: Specifies filtering of maximum flows that is equal to the specified number of bytes.

*bytes* must be an integer from 0 through 18446744073709551615.

#### **msid**

Displays active charging session information for a specific subscriber's Mobile Station Identification (MSID) number.

#### **msisdn *msisdn\_number***

Displays active charging session information for a specific subscriber's Mobile Station Integrated Services Digital Network (MSISDN) number.

*msisdn\_number* must be an integer with a maximum of 15 digits.

#### **ipv4**

Displays active charging session information with IPv4 Firewall enabled/disabled.

#### **ipv6**

Displays active charging session information with IPv6 Firewall enabled/disabled.

#### **nat { not-required | required [ nat-realm *nat\_realm\_name* ] } [ ipv4 | ipv6 ]**

Displays session information for sessions with NAT required or not required, as specified.

**nat-realm** *nat\_realm\_name* specifies the name of a NAT realm as an alphanumeric string of 1 through 63 characters.

**ipv4:** Displays active-charging sessions for which NAT44 processing is required.

**ipv6:** Displays active-charging sessions for which NAT64 processing is required.

#### **rulebase**

Displays information for a rulebase that is configured in an active charging session.

#### **rx-data**

Displays the bytes received in the session.

#### **session-id**

Displays detailed session information for a specific session identification.

#### **transrating**

Displays the transrating sessions.

#### **tx-data**

Displays the bytes sent in the session.

#### **type**

Displays session information for specified DNS application type(s).

- **dns**
  - **ftp**
  - **h323**
  - **http**
  - **icmp**
  - **icmpv6**
  - **imap**
  - **ip**
  - **ipv6**
  - **mms**
  - **p2p** [ **application** *p2p\_list* [ **traffic-type** *traffic\_type* ] | **protocol-group** *group\_list* ]: Displays session information for a P2P application type and P2P protocol group.
- p2p application** *p2p\_list*: The supported P2P applications are:
- **8tracks**
  - **abcnetworks**
  - **actionvoip**
  - **actsync**

- **adobeconnect**
- **aimini**
- **amazoncloud**
- **amazonmusic**
- **amazonvideo**
- **antisp2p**
- **apple-push**
- **apple-store**
- **applejuice**
- **applemaps**
- **ares**
- **armagetron**
- **avi**
- **badoo**
- **baidumovie**
- **battlefld**
- **bbm**
- **beatport**
- **betternet**
- **bitcasa**
- **bittorrent**
- **bittorrent-sync**
- **blackberry-store**
- **blackberry**
- **blackdialer**
- **box**
- **callofduty**
- **chikka**
- **cisco-jabber**
- **citrix**
- **clubbox**
- **clubpenguin**

- crackle
- crossfire
- crunchyroll
- cyberghost
- dblink
- deezer
- didi
- directconnect
- dish-anywhere
- disneymovies
- dofus
- dramafever
- dropbox
- edonkey
- espn
- expressvpn
- facebook
- facetime
- fandor
- fasttrack
- feidian
- fiesta
- filetopia
- filmontv
- flash
- flickr
- florensia
- foursquare
- fox-sports
- freenet
- friendster
- fring

- **funshion**
- **gadu\_gadu**
- **gamekit**
- **gmail**
- **gnutella**
- **go90**
- **goober**
- **google-music**
- **google-push**
- **google**
- **googleplay**
- **googleplus**
- **gotomeeting**
- **gtalk**
- **guildwars**
- **halflife2**
- **hamachivpn**
- **hayu**
- **hbogo**
- **hbonow**
- **heytell**
- **hgtv**
- **hike-messenger**
- **hls**
- **hotspotvpn**
- **hulu**
- **hyves**
- **iax**
- **icall**
- **icecast**
- **icloud**
- **idrive**

- igo
- iheartradio
- imesh
- imessage
- imgur
- imo
- instagram
- iplayer
- iptv
- irc
- isakmp
- iskoot
- itunes
- jabber
- jap
- jumblo
- kakaotalk
- kik-messenger
- kontiki
- kugoo
- kuro
- linkedin
- livestream
- lync
- magicjack
- manolito
- mapfactor
- mapi
- maplestory
- meebo
- mgcp
- mlb

- **mojo**
- **monkey3**
- **mozy**
- **msn**
- **msrp**
- **mute**
- **mypeople**
- **myspace**
- **nateontalk**
- **naverline**
- **navigon**
- **nbc-sports**
- **netmotion**
- **newsy**
- **nick**
- **nimbuzz**
- **nokia-store**
- **octoshape**
- **off**
- **ogg**
- **oist**
- **oovoo**
- **opendrive**
- **openft**
- **openvpn**
- **orb**
- **oscar**
- **outlook**
- **paltalk**
- **pando**
- **pandora**
- **path**

- pbs
- pcanywhere
- periscope
- pinterest
- plingm
- poco
- popo
- pplive
- ppstream
- ps3
- qq
- qqgame
- qqlive
- quake
- quic
- quicktime
- radio-paradise
- radius
- rdp
- rdt
- regram
- rfactor
- rhapsody
- rmstream
- rodi
- rynga
- samsung-store
- scydo
- secondlife
- shoutcast
- showtime
- silverlight



- siri
- skinny
- skydrive
- skype
- slacker-radio
- slingbox
- slingtv
- smartvoip
- snapchat
- softether
- sopcast
- soribada
- soulseek
- soundcloud
- spark
- spdy
- speedtest
- spike
- splashfighter
- spotify
- ssdp
- starz
- stealthnet
- steam
- stun
- sudaphone
- svtplay
- tagged
- talkatone
- tango
- teamspeak
- teamviewer

- telegram
- thunder
- tinder
- tmo-tv
- tor
- truecaller
- truphone
- tumblr
- tunein-radio
- tunnelvoice
- turbovpn
- tvants
- tvland
- tvuplayer
- twitch
- twitter
- ultrabac
- ultrasurf
- univision
- upc-phone
- usenet
- ustream
- uusee
- vchat
- veohtv
- vessel
- vevo
- viber
- vine
- voipdiscount
- vopium
- vpnmaster

- **vpn**
- **voxe**
- **vtok**
- **vtun**
- **vudu**
- **warcft3**
- **waze**
- **webex**
- **wechat**
- **whatsapp**
- **wii**
- **windows-azure**
- **windows-store**
- **winmx**
- **winny**
- **wmstream**
- **wofkungfu**
- **wofwarcraft**
- **wuala**
- **xbox**
- **xdcc**
- **xing**
- **yahoo**
- **yahoomail**
- **yiptv**
- **youku**
- **yourfreetunnel**
- **youtube**
- **zattoo**

**traffic-type** *traffic\_type*: P2P protocol flows include the following traffic type classifications:




---

**important** The traffic type for a P2P protocol may vary depending on the P2P protocol.

---

- **ads**
- **audio**
- **file-transfer**
- **im**
- **video**
- **voipout**
- **unclassified**

**p2p protocol-group** *group\_list*: The following P2P protocol groups are supported:

- generic
- anonymous-access
- business
- communicator
- cloud
- e-store
- e-mail
- e-news
- internet-privacy
- filesharing
- gaming
- p2p-filesharing
- p2p-anon-filesharing
- remote-control
- social-nw-gaming
- social-nw-generic
- social-nw-videoconf
- standard
- streaming
- **pop3**
- **pptp**
- **rtcp**
- **rtp**
- **rtsp**
- **secure-http**
- **sip**

- **smtp**
- **tcp**
- **tftp**
- **udp**
- **unknown**
- **wsp-connection-less**
- **wsp-connection-oriented**

**username**

Displays session information for a specific user name.

**dynamic-charging**

Displays all the sessions having received at least one Gx message from Session Manager/IMS Authorization.

**{ { grep *grep\_options* | more } }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Use this command to display the configuration information for an active charging session.

**Example**

The following command displays full information of an active charging session.

```
show active-charging sessions full all
```

The following command displays an active charging session summary.

```
show active-charging sessions summary
```



---

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

# show active-charging sessions credit-control server-unreachable

Displays the details of sessions that are currently in server-unreachable state i.e. Gy Assume Positive state.

---

**Product**

ACS

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

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **show active-charging sessions credit-control server-unreachable** [ *filter\_keyword* + ] [ | { **grep** *grep\_options* | **more** } ]

#### ***filter\_keyword***

The following keywords are filters that modify or filter the output of the Command Keywords. Not all filters are available for all command keywords. Multiple filter keywords can be entered on a command line.

When multiple filter keywords are specified, the output conforms to all of the filter keywords specifications.

For example, if you enter the following command:

**show active-charging sessions credit-control server-unreachable active-charging-service acs\_1**

Counters for active charging sessions active in ACS *acs\_1* are displayed. Information for all other services is not displayed.

#### ***acsmgr instance\_number***

Displays session information for a specific ACS/Session Manager instance.

#### ***active-charging-service acs\_service\_name***

Displays session information for the ACS specified as an alphanumeric string of 1 through 15 characters.

#### ***callid***

Specifies the call identification number.

#### ***credit-control***

Displays credit control information.

#### ***dynamic-charging***

Displays session information for all dynamic charging sessions.

#### ***firewall { not-required | required }***

Displays session information for sessions with Firewall Processing required or not required, as specified.

#### ***flows { active | idle | total } [ < | = | > | equal-to | greater-than | less-than ] { bytes }***

Displays information for all active charging flows filtered by all information, active, or idle sessions.

- *< bytes* or **less-than bytes**: Specifies filtering of flows that is less than the specified number of bytes.
- *> bytes* or **greater-than bytes**: Specifies filtering of flows that is greater than the specified number of bytes.

- = *bytes* or **equal-to** *bytes*: Specifies filtering of flows that is equal to the specified number of bytes.

*bytes* must be an integer from 0 through 18446744073709551615.

#### **fw-and-nat policy *fw\_nat\_policy\_name***

Displays information for the Firewall-and-NAT Policy specified as an alphanumeric string of 1 through 63 characters.

#### **imsi**

Specifies the International Mobile Subscriber Identity (IMSI) of the subscriber session.

#### **ip-address**

Specifies the IP address for the specific charging service.

#### **max-flows { < | = | > | equal-to | greater-than | less-than } { *bytes* }**

Displays information for the maximum flows made by the session.

- < *bytes* or **less-than** *bytes*: Specifies filtering of maximum flows that is less than the specified number of bytes.
- > *bytes* or **greater-than** *bytes*: Specifies filtering of maximum flows that is greater than the specified number of bytes.
- = *bytes* or **equal-to** *bytes*: Specifies filtering of maximum flows that is equal to the specified number of bytes.

*bytes* must be an integer from 0 through 18446744073709551615.

#### **msid**

Displays active charging session information for a specific subscriber's Mobile Station Identification (MSID) number.

#### **rulebase**

Displays information for a rulebase that is configured in an active charging session.

#### **rx-data**

Displays the bytes received in the session.

#### **session-id**

Displays detailed session information for a specific session identification.

#### **tx-data**

Displays the bytes sent in the session.

**type**

Displays session information for specified DNS application type(s).

- dns
  - ftp
  - h323
  - http
  - icmp
  - icmpv6
  - imap
  - ip
  - ipv6
  - mms
  - **p2p** [ **application** *p2p\_list* [ **traffic-type** *traffic\_type* ] | **protocol-group** *group\_list* ]: Displays session information for a P2P application type and P2P protocol group.
- p2p application** *p2p\_list*: The supported P2P applications are:

- 8tracks
- abcnetworks
- actionvoip
- actsync
- adobeconnect
- aimini
- amazoncloud
- amazonmusic
- amazonvideo
- antsp2p
- apple-push
- apple-store
- applejuice
- applemaps
- ares
- armagettron
- avi



- **badoo**
- **baidumovie**
- **battlefld**
- **bbm**
- **beatport**
- **betternet**
- **bitcasa**
- **bittorrent**
- **bittorrent-sync**
- **blackberry-store**
- **blackberry**
- **blackdialer**
- **box**
- **callofduty**
- **chikka**
- **cisco-jabber**
- **citrix**
- **clubbox**
- **clubpenguin**
- **crackle**
- **crossfire**
- **crunchyroll**
- **cyberghost**
- **ddlink**
- **deezer**
- **didi**
- **directconnect**
- **dish-anywhere**
- **disneymovies**
- **dofus**
- **dramafever**
- **dropbox**

- edonkey
- espn
- expressvpn
- facebook
- facetime
- fandor
- fasttrack
- feidian
- fiesta
- filetopia
- filmontv
- flash
- flickr
- florensia
- foursquare
- fox-sports
- freenet
- friendster
- fring
- funshion
- gadu\_gadu
- gamekit
- gmail
- gnutella
- go90
- goober
- google-music
- google-push
- google
- googleplay
- googleplus
- gotomeeting

- **gtalk**
- **guildwars**
- **halflife2**
- **hamachivpn**
- **hayu**
- **hbogo**
- **hbonow**
- **heytell**
- **hgtv**
- **hike-messenger**
- **hls**
- **hotspotvpn**
- **hulu**
- **hyves**
- **iax**
- **icall**
- **icecast**
- **icloud**
- **idrive**
- **igo**
- **iheartradio**
- **imesh**
- **imessage**
- **imgur**
- **imo**
- **instagram**
- **oplayer**
- **iptv**
- **irc**
- **isakmp**
- **iskoot**
- **itunes**

- jabber
- jap
- jumblo
- kakaotalk
- kik-messenger
- kontiki
- kugoo
- kuro
- linkedin
- livestream
- lync
- magicjack
- manolito
- mapfactor
- mapi
- maplestory
- meebo
- mgcp
- mlb
- mojo
- monkey3
- mozy
- msn
- msrp
- mute
- mypeople
- myspace
- nateontalk
- naverline
- navigon
- nbc-sports
- netmotion

- **newsy**
- **nick**
- **nimbuzz**
- **nokia-store**
- **octoshape**
- **off**
- **ogg**
- **oist**
- **oovoo**
- **opendrive**
- **openft**
- **openvpn**
- **orb**
- **oscar**
- **outlook**
- **paltalk**
- **pando**
- **pandora**
- **path**
- **pbs**
- **pcanywhere**
- **periscope**
- **pinterest**
- **plingm**
- **poco**
- **popo**
- **pplive**
- **ppstream**
- **ps3**
- **qq**
- **qqgame**
- **qqlive**

- quake
- quic
- quicktime
- radio-paradise
- radius
- rdp
- rdt
- regram
- rfactor
- rhapsody
- rmstream
- rodi
- rynga
- samsung-store
- scydo
- secondlife
- shoutcast
- showtime
- silverlight
- siri
- skinny
- skydrive
- skype
- slacker-radio
- slingbox
- slingtv
- smartvoip
- snapchat
- softether
- sopcast
- soribada
- soulseek

- soundcloud
- spark
- spdy
- speedtest
- spike
- splashfighter
- spotify
- sstp
- starz
- stealthnet
- steam
- stun
- sudaphone
- svtplay
- tagged
- talkatone
- tango
- teamspeak
- teamviewer
- telegram
- thunder
- tinder
- tmo-tv
- tor
- truecaller
- truphone
- tumblr
- tunein-radio
- tunnelvoice
- turbovpn
- tvants
- tvland

- tvuplayer
- twitch
- twitter
- ultrabac
- ultrasurf
- univision
- upc-phone
- usenet
- ustream
- uusee
- vchat
- veohTV
- vessel
- vevo
- viber
- vine
- voipdiscount
- vopium
- vpnmaster
- vpnx
- voxer
- vtok
- vtun
- vudu
- warcft3
- waze
- webex
- wechat
- whatsapp
- wii
- windows-azure
- windows-store



- winmx
- winny
- wmstream
- wofkungfu
- wofwarcraft
- wuala
- xbox
- xdcc
- xing
- yahoo
- yahoomail
- yiptv
- youku
- yourfreetunnel
- youtube
- zattoo

**traffic-type** *traffic\_type*: P2P protocol flows include the following traffic type classifications:



---

**Input** The traffic type for a P2P protocol may vary depending on the P2P protocol.

---

- ads
- audio
- file-transfer
- im
- video
- voipout
- unclassified

**p2p protocol-group** *group\_list*: The following P2P protocol groups are supported:

- generic
- anonymous-access
- business
- communicator

- cloud
- e-store
- e-mail
- e-news
- internet-privacy
- filesharing
- gaming
- p2p-filesharing
- p2p-anon-filesharing
- remote-control
- social-nw-gaming
- social-nw-generic
- social-nw-videoconf
- standard
- streaming
- **pop3**
- **pptp**
- **rtcp**
- **rtp**
- **rtsp**
- **secure-http**
- **sip**
- **smtp**
- **tcp**
- **tftp**
- **udp**
- **unknown**
- **wsp-connection-less**
- **wsp-connection-oriented**

### username

Displays session information for a specific user name.

**{ { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display the configuration information for an active charging session.

**Example**

The following command displays full information of an active charging session.

```
show active-charging sessions full all
```

The following command displays an active charging session summary.

```
show active-charging sessions summary
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging subscribers

Displays statistics and information on active subscribers.

**Product**

ACS

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show active-charging subscribers callid call_id charging-updates [ statistics
] [ charging-action [ name charging_action_name ] | qos-group [ name
qos_group_of_ruledefs_name ] | session ] [ | { grep grep_options | more } ]
```

**callid *call\_id***

Specifies a call identification number.

*call\_id* must be an eight digit HEX number.

```
charging-updates [ statistics ] [ charging-action [ name charging_action_name ] | qos-group [ name
qos_group_of_ruledefs_name ] | session ]
```

Displays charging-update statistics for subscriber.

- **statistics**: Displays statistics related to dynamic updates to charging parameters.
- **charging-action** [ **name** *charging\_action\_name* ]: Displays charging-updates for activated charging-actions or specified charging action.

*charging\_action\_name* must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters in length.

- **qos-group** [ **name** *qos\_group\_of\_ruledefs\_name* ]: Displays charging-updates for activated QoS groups or the specified QoS-group-of-ruledefs.

*qos\_group\_of\_ruledefs\_name* must be the name of a QoS-group-of-ruledefs, and must be an alphanumeric string of 1 through 63 characters in length.

- **session**: Displays charging-updates for the session.

### | { **grep** *grep\_options* | **more** }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to view subscriber statistics and information on dynamic updates to charging parameters per call ID.

### Example

The following command displays all statistics related to dynamic updates to charging parameters for call ID *ca50ea54*:

```
show active-charging subscribers callid ca50ea54 charging-updates
statistics
```

The following command displays information on charging updates for call ID *ca50ea54* and ACS charging action named *test12*:

```
show active-charging subscribers callid ca50ea54 charging-updates
charging-action name test12
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging subsystem

Displays service and configuration counters for the ACS.

### Product

ACS

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show active-charging subsystem { all | facility acsmgr { all | instance
instance_number } [ rulebase name rulebase_name ] | sip } [ | { grep grep_options
| more } ]
```

**all**

Displays ACS subsystem information.

**facility acsmgr [ all | instance *instance\_number* ]**

Displays logged events for all ACS/Session Managers or for a specific instance.

*instance\_number* must be an integer from 1 through 65535.

**rulebase name *rulebase\_name***

Displays rulebase statistics for the specified rulebase.

*rulebase\_name* must be the name of a rulebase, and must be an alphanumeric string of 1 through 63 characters.

**sip**

Displays SIP related statistics.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view ACS/Session Manager information.

**Example**

The following command displays ACS subsystem information:

```
show active-charging subsystem all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging tcp-proxy statistics

Displays TCP Proxy statistics.

**Product**

ACS

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show active-charging tcp-proxy statistics [ all | dynamic-disable |
ip-layer | proxy-fac | rulebase rulebase_name | socket-migration | tcp-layer
] [ verbose ] [ | { grep grep_options | more } ]
```

**all**

Displays all TCP Proxy statistics aggregated over all rulebases, including for both IP and TCP layers.

**dynamic-disable**

Displays statistics for dynamic disabling of TCP Proxy.

**ip-layer**

Displays TCP Proxy statistics for IP layer.

**proxy-fac**

Displays TCP Proxy Flow Admission Control statistics.

**rulebase *rulebase\_name***

Displays TCP Proxy statistics for the rulebase specified as an alphanumeric string of 1 through 63 characters.

**socket-migration**

Displays TCP Proxy statistics for socket migration.

**tcp-layer**

Displays TCP Proxy statistics for TCP layer.

**verbose**

Displays detailed TCP Proxy statistics.

**{ grep *grep\_options* | more }**

Specifies that the output of this command is to be piped (sent) to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view TCP Proxy statistics.

**Example**

The following command displays detailed TCP proxy statistics for the rulebase named *test14*:

```
show active-charging tcp-proxy statistics rulebase test14 verbose
```

## show active-charging tethering-detection

Displays information/statistics pertaining to Tethering Detection databases.

---

**Product** ACS

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show active-charging tethering-detection { database [ os-signature | tac | ua-signature ]+ [ sessmgr { all | instance instance_number } ] [ | { grep grep_options | more } ] | statistics }`

**database [ os-signature | tac | ua-signature ]+ [ sessmgr { all | instance *instance\_number* } ]**

Displays information pertaining to the specified Tethering Detection database(s).

- **os-signature**: Displays Tethering Detection OS (Operating System) database information.
- **tac**: Displays Tethering Detection TAC (Transaction Authorization Code) database information.
- **ua-signature**: Displays Tethering Detection UA (User Agent) database information.
- **+**: Indicates that more than one of the preceding keywords can be entered in a single command.
- **sessmgr { all | instance *instance\_number* }**: Displays SessMgr Tethering Detection database status.
  - **all**: Displays status for all SessMgr instances.
  - **instance *instance\_number***: Displays status for the SessMgr instance specified as an integer from 1 through 10000.

### statistics

Displays Tethering Detection related statistics.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines** Use this command to view information/statistics pertaining to Tethering Detection databases.

**Example**

The following command displays information pertaining to Tethering Detection UA and OS databases:

```
show active-charging tethering-detection database ua-signature os-signature
```

The following command displays information pertaining to all Tethering Detection databases:

```
show active-charging tethering-detection database
```

## show active-charging timedef

Displays the details of timeslots configured in specified time definition(s).

**Product**

ACS

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show active-charging timedef { all | name timedef_name } [ service name
acs_service_name ] [ | { grep grep_options | more } ]
```

**all**

Displays information for all timedefs configured in the service.

**name *timedef\_name***

Displays detailed information for the timedef specified as an alphanumeric string of 1 through 63 characters.

**service name *acs\_service\_name***

Displays information for all or a specific timedef configured in the specified ACS. *acs\_service\_name* must be the name of the active-charging service, and must be an alphanumeric string of 1 through 15 characters.

**| { **grep** *grep\_options* | **more** }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view details of timeslots configured in specified timedef(s) that have been configured for the Time-of-Day Activation/Deactivation of Rules feature.



**Example**

The following command displays timeslot details of all timedefs configured in the ACS:

```
show active-charging timedef all
```

## show active-charging traffic-optimization counters sessmgr

Displays cumulative Traffic Optimization statistics from Cisco Ultra Traffic Optimization engine.

**Important**

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

**Product**

P-GW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show active-charging traffic-optimization counters sessmgr { all | instance
  number }
```

**counters**

Displays aggregate flow counters/statistics from Cisco Ultra Traffic Optimization engine.

**all**

Displays all session manager (sessmgr) statistics specific to Traffic Optimization.

**instance *number***

Displays the statistics for a session manager instance.

**Usage Guidelines**

Use this command to display cumulative Traffic Optimization statistics from Cisco Ultra Traffic Optimization engine.

**Example**

The following command displays all sessmgr Traffic Optimization statistics from Cisco Ultra Traffic Optimization engine:

```
show active-charging traffic-optimization counters sessmgr all
```

## show active-charging traffic-optimization info

Displays version, mode, and configuration values of Cisco Ultra Traffic Optimization engine.

---

**Product**

P-GW

---

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

**show active-charging traffic-optimization info**

**traffic-optimization**

Displays all Traffic Optimization options.

**info**

Displays Cisco Ultra Traffic Optimization engine information.

---

**Usage Guidelines**

Use this command to display version, mode, and configuration values of Cisco Ultra Traffic Optimization engine. The output of configured values is based on Cisco Ultra Traffic Optimization engine. Only the relevant information for each Cisco Ultra Traffic Optimization engine is displayed as part of this CLI output.

**Example**

The following command displays detailed statistics about the version, mode, and configuration values of Cisco Ultra Traffic Optimization engine:

```
show active-charging traffic-optimization info
```

## show active-charging trigger-action

Displays information about the trigger actions configured in a service.

---

**Product**

ACS

---

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

**show active-charging trigger-action { all | name *trigger\_action\_name* [ service *acs\_service\_name* ] } [ | { **grep** *grep\_options* | more } ]**

**all**

Displays information for all trigger actions configured in a service.

**name *trigger\_action\_name***

Displays information for the specified trigger action.

*trigger\_action\_name* must be specified as an alphanumeric string of 1 through 63 characters.

**service *acs\_service\_name***

Displays service and configuration counters for the specified active charging service.

*acs\_service\_name* must be specified as an alphanumeric string of 1 through 63 characters.

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view information about trigger actions configured in a service.

**Example**

The following command displays the information for all trigger actions:

```
show active-charging trigger-action all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging trigger-condition

Displays information about the trigger conditions configured in a service.

**Product**

ACS

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show active-charging trigger-condition { { all | name trigger_condn_name [
service acs_service_name ] } | statistics [ name trigger_condn_name ] } [ | {
grep grep_options | more } ]
```

**all**

Displays information for all trigger conditions configured in a service.

**name *trigger\_condn\_name***

Displays information for the specified trigger condition.

*trigger\_condn\_name* must be specified as an alphanumeric string of 1 through 63 characters.

**statistics**

Displays statistical information for all configured trigger conditions.

**service *acs\_service\_name***

Displays service and configuration counters for the specified active charging service.

*acs\_service\_name* must be specified as an alphanumeric string of 1 through 63 characters.

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view information about trigger conditions configured in a service.

**Example**

The following command displays the information for all trigger conditions:

```
show active-charging trigger-condition all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging udr-format

Displays information about UDR formats configured in an Active charging Service (ACS).

**Product**

ACS

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

<b>Syntax Description</b>	<pre>show active-charging udr-format { all   name udr_fromat_name } [   { grep grep_options   more } ]</pre> <p><b>all</b></p> <p>Displays information for all UDR formats.</p> <p><b>name <i>udr_fromat_name</i></b></p> <p>Displays information for an existing UDR format specified as an alphanumeric string of 1 through 63 characters.</p> <p><b>{ grep <i>grep_options</i>   more }</b></p> <p>Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.</p> <p>For details on the usage of <b>grep</b> and <b>more</b>, refer to the <i>Regulating a Command's Output</i> section of the <i>Command Line Interface Overview</i> chapter.</p>
<b>Usage Guidelines</b>	Use this command to display information for UDR format(s) in an ACS.

**Example**

The following command displays all configured UDR formats in an ACS.

```
show active-charging udr-format all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show active-charging url-blockedlisting statistics

Displays URL Blockedlisting statistics.

<b>Product</b>	CF
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec
<b>Syntax Description</b>	<p>The following prompt is displayed in the Exec mode:</p> <pre>[local]host_name#</pre> <p>In releases prior to StarOS 21.26:</p> <pre>show active-charging url-blacklisting statistics [ rulebase { all   name rulebase_name } ] [ verbose ] [   { grep grep_options   more } ]</pre> <p>From StarOS 21.26 and later releases:</p>

```
show active-charging url-blockedlisting statistics [ rulebase { all |
name rulebase_name } ] [ verbose ] [ | { grep grep_options | more } ]
```

### **rulebase { all | name *rulebase\_name* }**

Displays URL Blockedlisting statistics for all or a specific rulebase.

- **all**: Displays URL Blockedlisting statistics for all configured rulebases.
- **name *rulebase\_name***: Displays URL Blockedlisting statistics for the rulebase specified as an alphanumeric string of 1 through 63 characters.

### **verbose**

Displays detailed URL Blockedlisting statistics.

### **| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

## Usage Guidelines

Use this command to view URL Blockedlisting hits and misses statistics.

### Example

In releases prior to StarOS 21.26:

The following command displays cumulative URL Blacklisting statistics:

```
show active-charging url-blacklisting statistics
```

The following command displays URL Blacklisting statistics for the rulebase *rulebase\_1*:

```
show active-charging url-blacklisting statistics rulebase name rulebase_1
```

From StarOS 21.26 and later releases:

The following command displays cumulative URL Blockedlisting statistics:

```
show active-charging url-blockedlisting statistics
```

The following command displays URL Blockedlisting statistics for the rulebase *rulebase\_1*:

```
show active-charging url-blockedlisting statistics rulebase name rulebase_1
```




---

### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

# show active-charging video detailed-statistics

Displays detailed statistics for TCP video flows. The command options enable you to collect statistical data for video per UE device type, per radio access type, and per video container type.



## Important

In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

## Product

MVG

## Privilege

Security Administrator, Administrator, Operator, Inspector

## Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

## Syntax Description

```
show active-charging video detailed-statistics [ container { flv | mp4 |  
others } | rat { cdma | gprs | hspa | lte | others | umts | wlan } | ue  
{ android | ios | laptop | others } ]
```

### **container { flv | mp4 | others }**

Displays detailed statistics for TCP video flows based on the specified container file format.

### **rat { cdma | gprs | hspa | lte | others | umts | wlan }**

Displays detailed statistics for TCP video flows based on the specified radio access type.

### **ue { android | ios | laptop | others }**

Displays detailed statistics for TCP video flows based on the specified UE device type.

## Usage Guidelines

Use this command to display detailed statistics about video usage. Use the command options to display detailed statistics based on the UE device type, radio access type, or container file format.

### Example

The following command displays detailed statistics about video usage based on the UE device type *ios*:

```
show active-charging video detailed-statistics ue ios
```

# show active-charging xheader-format

Displays x-header format configurations for an Active Charging Service (ACS).

**Important**

This is a customer-specific command. Please contact your local sales representative for more information.

**Product**

ACS

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show active-charging xheader-format { all | name xheader_format } [ | { grep grep_options | more } ]
```

**all**

Displays information for all x-header formats configured.

**name *xheader\_format***

Displays information for the x-header format specified as an alphanumeric string of 1 through 63 characters.

**| { *grep grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view details of x-header formats configured in an ACS.

**Example**

The following command displays information for the x-header format named *test12*:

```
show active-charging xheader-format test12
```

## show administrators

Displays information regarding all CLI users currently connected to the system.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:



```
[local]host_name#
```

---

**Syntax Description** `show administrators [ session id ] [ | { grep grep_options | more } ]`

**session id**

Indicates the output is to contain additional information about the CLI user session including the assigned session ID.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines** This command displays a list of administrative users that have command line interface sessions active.

**Example**

The following command displays a list of administrative users with active command line interface sessions:

```
show administrators
```

The following command displays the list along with CLI user session IDs:

```
show administrators session id
```

## show alarm

Displays alarm information.

---

**Product** All

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show alarm { all | audible | central-office | facility | outstanding [ all | chassis | port slot/port | slot slot ] [ verbose ] | statistics } [ | { grep grep_options | more } ]`

**all**

Displays the state of all alarms in one screen.

**audible**

Displays the state of the internal audible alarm on the SMC (ASR 5000) or SSC (ASR 5500).

**central-office**

Displays the state of the CO Alarm contacts on the SPIO (ASR 5000) or SSC (ASR 5500).

**facility**

Displays the state of the facility (audible and CO) alarms.

**outstanding [ all | chassis | port *slot/port* | slot *slot* ] [ verbose ]**

Displays information on currently outstanding alarms.

- **all**: Displays all alarm information.
- **chassis**: Displays chassis/power/fan alarms.
- **port *slot/port***: Shows the alarm information for the specified port.
- **slot *slot***: Shows the alarm information for the card in the specified slot.
- **verbose**: Displays more verbose output, including the internal alarm ID

**statistics**

Displays basic statistics on the alarming subsystem, including the current number of outstanding alarms of different severities and a cumulative total of alarms generated.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

View alarms to verify system status or to periodically check the general health of the system.

**Important**

This command is not supported on all platforms.

**Example**

The following command displays all alarms that are currently outstanding:

```
show alarm outstanding all
```

The following command displays more detailed information on all alarms that are currently outstanding:

```
show alarm outstanding all verbose
```

The following command displays alarm statistics:

```
show alarm statistics
```




---

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show alcap counters




---

**Important**

In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

---

Displays the Access Link Control Application Part (ALCAP) protocol message counters related to ALCAP protocol sessions associated with a Home-NodeB Gateway (HNB-GW) service instance configured and running on a system.

---

**Product**

HNBGW

---

**Privilege**

Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
show alcap counters [ alcap-service alcap_svc_name [ aal2-node aal2_node_name
[ aal2-path aal2_path_id ] ] ] [ | { grep grep_options | more } ]
```

**name** *alcap\_svc\_name*

Specifies the name of the ALCAP service for which ALCAP protocol session counters are to be displayed.

**aal2-node** *aal2-node*

Specifies the name of the ATM Adaptation Layer 2 (AAL2) node for which protocol session counters will be filtered.

**aal2-path** *aal2\_path\_id*

Specifies the identity number of the AAL2 path on a specific ATM Adaptation Layer 2 (AAL2) node for which ALCAP protocol counters will be filtered.

| { **grep** *grep\_options* | **more** }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *Command Line Interface Overview* chapter.

### Usage Guidelines

This command is used to display the sessions statistics and counters for ALCAP service.

### Example

The following command displays the ALCAP protocol session counters for ALCAP service named as *alcap\_hnb\_svc1*:

```
show alcap counters alcap-service alcap_hnb_svc1
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show alcap-service



### Important

In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Displays the Access Link Control Application Part (ALCAP) session statistics of an ALCAP service associated with a Home-NodeB Gateway (HNB-GW) service instance configured and running on a system.

### Product

HNBGW

### Privilege

Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show alcap-service { all | name alcap_svc_name [ aal2-node aal2_node_name [
aal2-path aal2_path_id [ aal2-channel aal2_channel_num ] ] | endpoint
aal2_endpoint_name ] } [ | { grep grep_options | more } ]
```

#### **name** *alcap\_svc\_name*

Specifies the name of the ALCAP service for which service statistics are to be displayed.

#### **aal2-node** *aal2-node*

Specifies the name of the ATM Adaptation Layer 2 (AAL2) node that will be used to filter the display of the ALCAP service statistics.

**aal2-path** *aal2\_path\_id*

Specifies the identity number of the AAL2 path on a specific ATM Adaptation Layer 2 (AAL2) node that will be used to filter the display of the ALCAP service statistics.

**aal2-channel** *aal2\_channel\_num*

Specifies the AAL2 channel number of the AAL2 path on a specific ATM Adaptation Layer 2 (AAL2) node that will be used to filter the display of the ALCAP service statistics.

**endpoint** *atm\_endpoint\_name*

Specifies the ATM endpoint name that will be used to filter the display of the ALCAP service statistics for a specific ATM endpoint.

**Usage Guidelines**

This command is used to clear the sessions statistics and counters for ALCAP service.

**Example**

The following command displays the service statistics of ALCAP service named as *alcap\_hnb\_svc1*:

```
show alcap-service name alcap_hnb_svc1
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show alcap statistics

**Important**

In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Displays the session statistics related to Access Link Control Application Part (ALCAP) protocol sessions associated with a Home-NodeB Gateway (HNB-GW) service instance configured and running on a system.

**Product**

HNBGW

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show alcap statistics [ alcap-service alcap_svc_name [ aal2-node aal2_node_name
[ aal2-path aal2_path_id ] ] ] [ verbose ] [ | { grep grep_options | more }
]
```

**name *alcap\_svc\_name***

Specifies the name of the ALCAP service for which statistics are to be displayed.

**aal2-node *aal2-node***

Specifies the name of the ATM Adaptation Layer 2 (AAL2) node for which ALCAP service related statistics will be displayed.

**aal2-path *aal2\_path\_id***

Specifies the identity number of the AAL2 path on a specific ATM Adaptation Layer 2 (AAL2) node for which ALCAP service statistics counters will be displayed.

**{ *grep grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *Command Line Interface Overview* chapter of the *Command Line Interface Reference*.

**Usage Guidelines**

This command is used to display the sessions statistics and counters for ALCAP service.

**Example**

The following command displays the service session statistics counters for ALCAP service named as *alcap\_hnb\_svc1*:

```
show alcap counters alcap-service alcap_hnb_svc1
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

# show apn

Displays configuration information for either a specific or all configured Access Point Names (APNs).

**Product**

GGSN  
P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**    `show apn { all | name apn_name } [ | { grep grep_options | more } ]`

**all**

Displays information on all APNs configured on the system.

**name *apn\_name***

Displays information for an APN specified as an alphanumeric string of 1 through 62 characters that is case sensitive.

**{ **grep** *grep\_options* | **more** }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more** options, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

This command is used to verify the configuration of one or all APNs for monitoring or troubleshooting purposes. The output is a concise listing of APN parameter settings.

If this command is executed from within the local context with the **all** keyword, information for all APNs configured on the system will be displayed.

**Example**

The following command displays configuration information for all APNs:

```
show apn all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show apn counters ip-allocation

Displays cumulative statistics of IP allocation method for calls set up so far, per Access Point Name (APN) basis.

**Product**

GGSN  
P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `show apn counters ip-allocation [ all | name apn_name ] [ | { grep grep_options | more } ]`

**all**

Displays statistics for all APNs.

**name *apn\_name***

Displays statistics for the APN specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**| { **grep** *grep\_options* | **more** }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

This command is used to display the cumulative IP allocation counters on a per APN basis. Output of this command gives the user clear idea of how many sessions in each APN have used a particular type of ip-allocation method.

If this command is issued from within the local context, the statistics displayed will be cumulative for all APNs configured on the system regardless of context. If no APN name is specified and the command is executed from a context with multiple APNs configured, the output will be cumulative for all APNs in the context.

**Example**

The following command displays statistics for all APN on a system:

```
show apn counter ip-allocation all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show apn statistics

Displays statistics for either a specific Access Point Name (APN) or all configured APNs. Also can be used to display APN statistics at the ARP/QCI level.

**Product**

GGSN  
P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator, Operator, Inspector



**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show apn statistics [ all | name apn_name ] qci { all | 1-9 | non-std [ gbr | non-gbr ] } arp { all | 1-15 } ] [ | { grep grep_options | more } ]
```

**all**

Displays statistics for all APNs.

**name *apn\_name***

Displays statistics for the APN specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**qci**

Enables the configuration of ARP priority level statistics for the specified QCI.

**Important**

ARP Granularity and Per QCI Packet Drop Counters is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

**all**

Configures the collection of ARP priority level statistics for all QCIs.

**Important**

ARP Granularity and Per QCI Packet Drop Counters is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

**1-9**

Configures the collection of ARP priority level statistics for a specific QCI 1 through 9.

**Important**

ARP Granularity and Per QCI Packet Drop Counters is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

**non-std**

Configures collection of ARP priority level statistics for non-standard non-guaranteed bit rate (GBR) QCIs.

**Important**

ARP Granularity and Per QCI Packet Drop Counters is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

**non-gbr**

Configures the collection of ARP priority level statistics for non-standard non-GBR QCIs.

**Important**

ARP Granularity and Per QCI Packet Drop Counters is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

**gbr**

Configures the collection of ARP priority level statistics for non-standard GBR QCIs.

**Note**

ARP Granularity and Per QCI Packet Drop Counters is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

**arp**

Configures the collection of ARP priority level statistics for the specified ARP.

**Important**

ARP Granularity and Per QCI Packet Drop Counters is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

**1-15**

Configures ARP priority level statistics for a specified ARP of 1 through 15.

**Important**

ARP Granularity and Per QCI Packet Drop Counters is a license-controlled feature. Contact your Cisco account or support representative for licensing details.

**{ *grep* *grep\_options* | *more* }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

This command is used to view statistics for one or all APNs within a context for monitoring or troubleshooting purposes.

If this command is issued from within the local context, the statistics displayed will be cumulative for all APNs configured on the system regardless of context. If no APN name is specified and the command is executed from a context with multiple APNs configured, the output will be cumulative for all APNs in the context.

**Example**

The following command displays statistics for an APN named *isp2*:

```
show apn statistics name isp2
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show apn-profile

Displays information for configured Access Point Name (APN) profiles.

**Product**

MME  
SGSN

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show apn-profile { all | full { all | name apn_name } | name apn_name } [ |  
{ grep grep_options | more } ]
```

**all**

Lists all APN profiles configured on the system.

**full { all | name *apn\_name* }**

**full**: Displays all information in the APN profile(s).

**all**: Displays full information for all APN profiles configured on the system.

**name** *apn\_name*: Displays full information for an APN profile specified as an alphanumeric string of 1 through 64 characters.

**name *apn\_name***

Displays information for an APN profile specified as an alphanumeric string of 1 through 64 characters.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display information for APN profiles configured on the system. APN profiles are configured through the global configuration mode and in the APN profile configuration mode. For more information regarding APN profile commands, refer to the *APN Profile Configuration Mode Commands* chapter.

**Example**

The following command displays all available information for an APN profile named *apn-prof3*:

```
show apn-profile full name apn-prof3
```

## show apn-remap-table

Displays information for Access Point Name (APN) remap tables configured on the system.

**Product**

MME  
SGSN

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show apn-remap-table { all | full { all | name remap_table_name } | name remap_table_name } [ | { grep grep_options | more } ]
```

**all**

Lists all APN remap tables configured on the system.

**full { all | name *remap\_table\_name* }**

**full**: Displays a full set (all) of available information for the configured APN remap table(s).

**all**: Displays the full set of available information for all APN remap tables configured on the system.

**name *remap\_table\_name***: Displays the full set of available information for an existing APN remap table specified as alphanumeric string of 1 through 64 characters.

**name *remap\_table\_name***

Displays information for an existing APN remap table specified as an alphanumeric string of 1 through 64 characters.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display information for APN remap tables configured on the system. APN remap tables are configured through the Global Configuration mode and in the APN remap table configuration mode. For more information regarding APN remap table commands, refer to the *APN Remap Table Configuration Mode Commands* chapter.

### Example

The following command displays all available information for an APN remap table named *remap-table12*:

```
show apn-remap-table full name remap-table12
```

## show aps

Displays information for configured Automatic Protection Switching (APS) parameters.

### Product

SGSN

### Privilege

Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show aps { all | card-stats slot_number [ clear ] | info slot_number/port_number
  | port-stats slot_number/port_number [ clear ] | port-status } [ | { grep
  grep_options | more } ]
```

#### all

Lists APS information for all cards configured with APS.

#### card-statsslot\_number[ clear ]

Displays the APS statistics for the identified card. If the **clear** keyword is included with the command, the APS statistics for the specified card are cleared (reset to zero).

*slot\_number* is an integer that identifies the chassis slot holding the card.

#### infoslot\_number/port\_number

Displays APS information for a specific port.

*slot\_number/port\_number*: The first number must be an integer that identifies the chassis slot holding the specified card. The slot number must be followed by a slash '/', which must be followed immediately by the port number - an integer from 1 to 4 depending upon the type of card.

**port-statsslot\_number/port\_number [ clear ]**

Displays APS statistics for a specific port. If the **clear** keyword is included with the command then the APS statistics for the specified port are cleared (reset to zero).

*slot\_number/port\_number*: The first number must be an integer from 1 to 48 to identify the chassis slot holding the specified card. The slot number must be followed by a slash '/', which must be followed immediately by the port number - an integer from 1 to 4 depending upon the type of card.

**port-statusslot\_number/port\_number**

Displays APS status information for a specific port.

*slot\_number/port\_number*: The first number must be an integer from 1 to 48 to identify the chassis slot holding the specified card. The slot number must be followed by a slash '/', which must be followed immediately by the port number - an integer from 1 to 4 depending upon the type of card.

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display APS redundancy configuration, APS card and port status, and APS card and port statistics. APS is configured at the card level. For details on configuring APS, refer to the *Card Configuration Mode Commands* chapter in this reference.

**Important**

APS is only relevant for the CLC2 and OLC2 line cards supporting SONET/SDH.

**Example**

The following command displays all available APS configuration information for a specific port 1 on the line card in slot 27:

```
show aps info 27/1
```

# show asngw-service

Displays information about selected Access Service Network Gateway (ASN-GW) calls/services.

**Product**

ASN-GW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show asngw-service { all | name service_name | session | statistics } [
bs-status [ address ip_address | filter { all | icmp-monitored | no-calls
| summary | up } ] ] [ | { grep grep_options | more } ]
```

**all**

Displays information for all configured ASN-GW services.

**name *service\_name***

Displays information only for an existing ASN-GW service in the current context specified as an alphanumeric string of 1 through 63 characters.

**session**

Displays information about configured ASN-GW sessions. See the **show asngw-service session** command

**statistics**

Total of collected information for specific protocol since the last **restart** or **clear** command.

```
bs-status { address ip_address | filter { all | icmp-monitored | no-calls | summary | up } }
```

Displays the ASN base station (BS) status based on IP address and various filters.

**address *ip\_address*** specifies the IP address of ASN base station whose status is requested. *ip\_address* must be entered in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**filter { all | icmp-monitored | no-calls | summary | up }**: Filters the requested BS's status on the basis of following criteria:

- **all**: Displays the status of all ASN base stations.
- **icmp-monitored**: Displays the status of ASN base stations that are monitored through ICMP ping messages.
- **no-calls**: Displays the status of an ASN base station that has no active calls.
- **summary**: Displays a summary of the status of requested ASN base stations.
- **up**: Displays the of status of ASN base stations that are in active state.

```
{ { grep grep_options | more } }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view information for selected configured ASN-GW services.

**Example**

The following command displays available information for all active ASN-GW services.

```
show asngw-service all
```



**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show asngw-service session

Displays statistics for specific Access Service Network Gateway (ASN-GW) sessions.

### Product

ASN-GW

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show asngw-service session [ all | anchor-only [ full ] | callid call_id |
  counters | full | ip-address ipv4_address | msid msid_number | non-anchor-only
  [ full ] | peer-address ipv4_address | summary | username user_name ] [ | {
  grep grep_options | more } ]
```

#### all

Displays all related information for all active ASN-GW service sessions.

#### anchor-only

Displays all available information for all active ASN-GW service sessions on an anchor ASN-GW only.

#### callid *call\_id*

Displays available information for the call identification number specified as an 8-digit hexadecimal number.

#### full

Displays all available information for the associated display or filter keyword.

#### ip-address *ipv4\_address*

Specifies the IP address of the subscriber in IPv4 dotted-decimal notation.

#### msid *msid\_number*

Displays available information for the specific mobile station identification number (MSID).

#### non-anchor-only

Displays all available information for all active ASN-GW service sessions on a non-anchor ASN-GW only.



**peer-address *ipv4\_address***

Specifies the Ip address of an IP peer in dotted-decimal notation.

**summary**

Displays summary of available information for associated display or filter keyword (previous keyword).

**username *user\_name***

Specifies the name of a user within current context as an alphanumeric string of 1 through 127 characters.

**{ *grep grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view configuration information for an ASN-GW session.

**Example**

The following command displays all available ASN-GW sessions.

```
show asngw-service session all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show asngw-service session counters

Displays statistics for specific Access Service Network Gateway (ASN-GW) sessions.

**Product**

ASN-GW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show asngw-service session counters [ [ function-type { auth-relay |
context-transfer | data-path | handoff | im-operation | ms-state-change |
paging | qos } ] ] [ anchor-only | callid call_id | ip-address ipv4_address |
msid msid_number | non-anchor-only | peer-address ipv4_address | username user_name
] [ r4-only | r6-only | verbose ] [ | { grep grep_options | more } ]
```

**anchor-only**

Displays all available information for all active anchor sessions in an ASN-GW service.

**callid *call\_id***

Displays available information for the call identification number specified as an 8-digit hexadecimal number.

**function-type { *auth-relay* | *context-transfer* | *data-path* | *handoff* | *im-operation* | *ms-state-change* | *paging* | *qos* }**

Displays the counters for specific type of functions in an ASN-GW session.

**auth-relay:** Displays information about authentication relay messages.

**context-transfer:** Displays information about context-transfer messages.

**data-path:** Displays information about data-path registration messages.

**handoff:** Displays information about hand-off messages.

**im-operations:** Displays information about idle mode state operation messages.

**ms-state-change:** Displays information about MS state change messages.

**paging:** Displays information about paging messages.

**qos:** Displays information about RR messages.

**ip-address *ipv4\_address***

Specifies the IP address of the subscriber in IPv4 dotted-decimal notation.

**msid *msid\_number***

Displays available information for the specific mobile station identification (MSID) number.

**non-anchor-only**

Displays all available information for all active non-anchor sessions in an ASN-GW service.

**peer-address *ipv4\_address***

Specifies the IP address of an IP peer in IPv4 dotted-decimal notation.

**r6-only**

Displays all available counters for R6 interface in an ASN-GW session.

**r4-only**

Displays all available counters for R4 interface in an ASN-GW session.

**username *user\_name***

Displays available session information for the specific WiMAX user in ASN-GW service session.

*user\_name* is an alphanumeric string of 1 through 127 characters.

**verbose**

Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view the counters of an ASN-GW session.

**Example**

The following command displays the counters for data path type function.

```
show asngw-service session counters function-type data-path
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show asngw-service statistics

Displays statistics for all Access Service Network Gateway (ASN-GW) sessions.

**Product**

ASN-GW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show asngw-service statistics [ function-type { auth-relay |
context-transfer | data-path | handoff | im-operations | ms-state-change
| paging | qos | capability } ] [ name service_name | r4-only | r6-only |
verbose | peer-address ipv4_address ] [ peer-id id ] [ verbose ] [ { grep
grep_options | more } ]
```

**function-type**

Displays information about selected function type on R4 or R6 interface.

**function-type** { **auth-relay** | **context-transfer** | **data-path** | **handoff** | **im-operations** | **ms-state-change** | **paging** | **qos** | **capability** } [ **r4-only** | **r6-only** ]

Displays the counters for specific type of functions in an ASN-GW session.

**auth-relay**: Displays information about authentication relay messages.

**context-transfer**: Displays information about context-transfer messages.

**data-path**: Displays information about data-path registration messages.

**handoff**: Displays information about hand-off messages.

**im-operations**: Displays information about idle mode state operation messages.

**ms-state-change**: Displays information about MS state change messages.

**paging**: Displays information about paging messages.

**qos**: Displays information about RR messages.

**capability**: Displays the capability negotiation between the ASNGW and the base station.

**r4-only**: Displays information about selected function on R4 interface.

**r6-only**: Displays information about selected function on R6 interface.

**name** *service\_name*

Displays information for an existing service specified as an alphanumeric string of 1 through 63 characters.

**r4-only**

Displays statistics of R4 interface in ASN-GW services.

**r6-only**

Displays statistics of R6 interface in ASN-GW services.

**peer-address** *ipv4\_address*

Specifies the IP address of an IP Peer in IPv4 dotted-decimal notation.

**peer-id** < *id* >

Display the statistics based on the 6-byte BSID or ASNGW ID in addition to the IPv4 address.

**verbose**

Specifies that the output should display all available information. If this option is not specified then the output will be the standard level which is the concise mode.

[ { **grep** *grep\_options* | **more** } ]

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display ASN-GW statistics.

**Example**

The following command displays information about selected MS-State-Change function.

```
show asngw-service statistics function-type ms-state-change
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show asnpc-service

Displays information about selected Access Service Network Paging Controller and Location Registry (ASN PC/LR) services.

**Product**

ASN-GW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show asnpc-service { all | id | name service_name | session | statistics }
[ | { grep grep_options | more } ]
```

**all**

Displays information for all configured ASN PC services.

**paging-group**

Displays all the configured paging-groups and associated paging nodes, and the offset count. For a specific paging group, enter the paging group id number.

**name *service\_name***

Displays information only for an existing ASN PC service specified as an alphanumeric string of 1 through 63 characters.

**session**

Displays information about configured ASN PC sessions.

**statistics**

Total of collected information for specific protocol since last restart or clear command.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to view information for selected configured ASN PC services.

### Example

The following command displays available information for all active ASN PC services.

```
show asnpc-service all
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show asnpc-service session

Displays statistics for specific Access Service Network Paging Controller (ASN PC) service sessions.

### Product

ASN-GW

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show asnpc-service session [ all | callid call_id | counters | full | msid
  msid_number | peer-address ipv4_address | summary ] [ | { grep grep_options |
  more } ]
```

#### all

Displays all related information for all active ASN PC service sessions.

#### callid *call\_id*

Displays available information for the call identification number specified as an 8-digit hexadecimal number.

#### full

Displays all available information for the associated display or filter keyword.

**msid** *msid\_number*

Displays available information for the specific mobile station identification (MSID) number.

**peer-address** *ipv4\_address*

Specifies the IP address of an IP peer in IPv4 dotted-decimal notation.

**summary**

Displays summary of available information for associated display or filter keyword (previous keyword).

**{ grep** *grep\_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view configuration information for an ASN PC session.

**Example**

The following command displays all available ASN PC session counters in verbose mode.

```
show asnpc-service session all
```

The following command displays full ASN PC session counters in verbose mode.

```
show asnpc-service session full
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show asnpc-service session counters

Displays session counters for Access Service Network Paging Controller (ASN PC) service sessions.

**Product**

ASN-GW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show asngw-service session counters [ all | callid call_id | msid msid_number
| peer-address ipv4_address | verbose ] ] [ | { grep grep_options | more } ]
```

**all**

Displays all available counters for all ASN PC service sessions.

**callid *call\_id***

Displays available information for the call identification number specified as an 8-digit hexadecimal number.

**msid *msid\_number***

Displays available information for the specific mobile station identification (MSID) number.

**peer-address *ipv4\_address***

Specifies the IP address of an IP peer in IPv4 dotted-decimal notation.

**verbose**

Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

**| { *grep grep\_options* | *more* }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view the counters of an ASN PC session.

**Example**

The following command displays the counters for ASN PC service sessions in verbose mode.

```
show asnpc-service session counters verbose
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show asnpc-service session counters verbose

Displays session counters for Access Service Network Paging Controller (ASN PC) service sessions in complete detail.

**Product**

ASN-GW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec



The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show asngw-service session counters verbose [ function-type {
context-transfer | im-operations | ms-state-change | paging } ] [ all |
callid call_id | msid msid_number | peer-address ipv4_address ] [ | { grep
grep_options | more } ]
```

#### all

Displays all available counters for all ASN PC service sessions in verbose mode.

#### callid *call\_id*

Displays full information for the call identification number specified as an 8-digit hexadecimal number.

#### function-type { context-transfer | im-operations | ms-state-change | paging }

Displays the counters for specific type of functions in an ASN-GW session.

**context-transfer:** Displays information about context-transfer messages.

**im-operations:** Displays information about idle mode state operation messages.

**ms-state-change:** Displays information about MS state change messages.

**paging:** Displays information about paging messages.

#### msid *msid\_number*

Displays full information for the specific mobile station identification (MSID) number.

#### peer-address *ipv4\_address*

Specifies the IP address of an IP peer IPv4 dotted-decimal notation.

#### r4-only

Displays statistics of R4 interface in ASN PC services in verbose mode.

#### r6-only

Displays statistics of R6 interface in ASN PC services in verbose mode.

#### { grep *grep\_options* | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to view the counters of an ASN PC session in verbose mode.

**Example**

The following command displays the counters for data path type function.

```
show asnpc-service session counters verbose
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show asnpc-service statistics

Displays statistics for all ASN PC service sessions.

**Product**

ASN-GW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show asnpc-service statistics [ name service_name | peer-address ipv4_address
| verbose ] [ r4-only | r6-only [ | { grep grep_options | more } ]
```

**name *service\_name***

Specifies an existing service name as an alphanumeric string of 1 through 63 characters.

**peer-address *ipv4\_address***

Specifies the IP address of an IP peer in IPv4 dotted-decimal notation.

**verbose**

Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display ASN PC statistics.

**Example**

The following command displays information about ASN PC service in verbose mode.

```
show asnpc-service statistics verbose
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show asnpc-service statistics verbose

Displays statistics for all Access Service Network Paging Controller (ASN PC) service in verbose mode.

**Product**

ASN-GW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show asnpc-service statistics verbose [ function-type { context-transfer
| im-operations | ms-state-change | paging } ] | all | r4-only | r6-only
] [ | { grep grep_options | more } ]
```

**function-type { context-transfer | ms-state-change | paging }**

Displays the statistics for specific type of functions in an ASN PC service in verbose mode.

**context-transfer:** Displays information about context-transfer messages.

**im-operations:** Displays information about idle mode state operation messages.

**ms-state-change:** Displays information about MS state change messages.

**paging:** Displays information about paging messages.

**all**

Displays statistics of all ASN PC services in verbose mode.

**r4-only**

Displays statistics of R4 interface in ASN PC services.

**r6-only**

Displays statistics of R6 interface in ASN PC services.

```
{ grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display ASN PC service statistics in verbose mode.

### Example

The following command displays information about selected MS-State-Change function.

```
show asnpc-service statistics verbose function-type ms-state-change
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show banner

Displays the configured banner message for the current context.

### Product

All

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show banner { all | charging-service | motd | lawful-intercept | pre-login } [ | { grep grep_options | more } ]
```

#### all

Displays all banners configured for a service in a system including the enhanced charging service (ECS).

#### charging-service

Displays banner message configured for an enhanced charging service in the current context.

#### motd

Display the banner message that is configured for the current context.

#### lawful-intercept

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

**{ `grep` *grep\_options* | `more` }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines** Show the configured banner to verify the message of the day contents for possible change

### Example

The following command displays all current banner messages:

```
show banner all
```

## show bcmcs counters

Displays Broadcast and Multicast Service (BCMCS)-specific counters and statistics.

**Product** PDSN

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

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **show bcmcs counters { `all` | `callid` *call\_id* | `flow-id` *flow\_id* }**

### **all**

Displays BCMCS-specific counters and statistics for all multicast sessions.

### **callid** *call\_id*

Displays BCMCS-specific counters and statistics for a specific call ID.

### **flow\_id** *flow\_id*

Displays BCMCS-specific counters and statistics for a specific BCMCS flow, defined by a flow ID.

**Usage Guidelines** Use this command to view BCMCS-specific statistics. You may narrow the results of the command output by specifying a specific call ID or flow ID.

### Example

The following command displays all BCMCS counters:

```
show bcmcs counters all
```




---

**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show bcmcs statistics

Displays Broadcast and Multicast Service (BCMCS)-specific statistics for the current PDSN-service.

<b>Product</b>	PDSN
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `show bcmcs statistics [ pdsn-service service_name ]`

**pdsn-service service\_name**

Defines a specific PDSN service from which to gather BCMCS-specific statistics.

**Usage Guidelines** Shows several sets of BCMCS-specific statistics, and may be configured to show statistics only for a certain PDSN service.

**Example**

The following command displays BCMCS statistics for the PDSN service named *group\_1*:

```
show bcmcs statistics pdsn-service group_1
```




---

**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show bfd

Displays Bidirectional Forwarding Detection (BFD) neighbors and their current debug settings.

<b>Product</b>	PDSN
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**    `show bfd { debugging | neighbors }`

**show bfd debugging**

Displays current BFD options for peer control messaging.

**show bfd neighbors**

Displays summary information for BFD-enabled neighbors.

---

**Usage Guidelines**    Show the configuration of BFD-enabled neighbors and the current debug settings.

**Example**

The following command displays information for BFD-enabled neighbors:

```
show bfd neighbors
```




---

**Important**    Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show boot

Displays information on the current boot image in use.

---

**Product**    All

---

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

---

**Command Modes**    Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**    `show boot [ initial-config | { grep grep_options | more } ]`

**initial-config**

Identifies the OS image, configuration file, and boot priority used during the initial start up of the system.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**    Show the boot information in preparing for maintenance activities by verifying current boot data. The boot image in use may not be the same as the boot image stored on the SPC/SMC due to upgrades and pending

reboots. **show boot initial-config** displays the actual boot image and configuration file loaded during boot. This may or may not be the highest priority image and makes this command useful when comparing the loaded image to the priority list.




---

**Important** This command is not supported on all platforms.

---

### Example

The following command displays the boot system configuration priority list:

```
show boot
```

The following command displays the initial configuration after a system boot:

```
show boot initial-config
```

## show bssap+ statistics

Displays Base Station system Application Part (BSSAP+) protocol statistics for the Gs interface between the SGSN and the Mobile services Switching Centre, Visitor Location Register (MSC/VLR).

---

**Product** SGSN

---

**Privilege** Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show bssap+ statistics** [ **gs-service** *gs\_svc\_name* ] [ **vlr** { **isdn-number** *ISDN\_Num* | **name** *vlr\_name* } ] [ **verbose** ] [ | { **grep** *grep\_options* | **more** } ]

### **gs-service** *gs\_svc\_name*

Specifies the name of a specific Gs service to filter the BSSAP+ information as an alphanumeric string of 1 through 63 characters that is case sensitive.

### **vlr** { **isdn-number** *ISDN\_Num* | **name** *vlr\_name* }

Identifies a specific VLR (by name or ISDN number) to filter BSSAP+ information.

*vlr\_name* is the configured name of the VLR expressed.

*VLR\_num* is the configured E.164-type ISDN number for the VLR. Enter a numerical string of 1 to 15 digits.

### **verbose**

Indicates the output should provide as much information as possible. If this option is not specified then the output will be limited to a concise summary.



**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display the BSSAP+ statistics for the SGSN's Gs interface(s). Based on how the command is entered, this command displays collected BSSAP+ protocol statistics for the entire SGSN or for a specified Gs interface. Using the keywords of this command, the interface can be identified by defining a specific VLR connected to the SGSN or by identifying the Gs service to which the interface has been configured.

### Example

The following command displays all BSSAP+ information for the Gs interface configured for the Gs service named *gssvc1*.

```
show bssap+ statistics gs-service gssvc1 verbose
```



### Important

Descriptions for show command outputs are available in the *Statistics and Counters Reference*.

## show bssgp statistics

Displays base station subsystem GPRS protocol statistics for traffic between the base station subsystem (BSS) and the SGSN over the Gb interface.

### Product

SGSN

### Privilege

Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show bssgp statistics [ gprs-service gprs_svc_name | nse nse_id [ bvc bvc_id
[ sessmgr | verbose ] ] ] [ verbose ] [ | { grep grep_options | more } ]
```

#### **gprs-service *gprs\_svc\_name***

Specifies the name of an existing GPRS service for which the BSSGP information will be filtered as an alphanumeric string of 1 through 63 characters that is case-sensitive.

#### **nse *ID***

Enter this keyword to display the BSSGP statistics for the network service entity (NSE) specified as an integer from 0 through 65535.

**bvcbvc\_ID**

Enter this keyword to display the BSSGP statistics for the BSSGP virtual connection (BVC) specified as an integer from 0 through 6500.

**sessmgr instance sessmgr\_instance\_number**

Enter this keyword to display the BSSGP statistics for a session manager instance specified as an integer from 1 through 4294967295.

**verbose**

Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display the BSSGP statistics for a particular GPRS service or NSEI.

**Example**

The following command displays BSSGP statistics for the GPRS service named *gprs1*.

```
show bssgp statistics gprs-service gprs1
```

**Important**

Descriptions for show command outputs are available in the *Statistics and Counters Reference*.

# show bssgp status

Displays the traffic status through the BSSGP (base station subsystem GPRS protocol) layer between the base station subsystem (BSS) and the SGSN over the Gb interface.

**Product**

SGSN

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show bssgp status { bvc-bucket nsei nse_id bvci bvc_id | bvc-stat nsei nse_id
  bvci bvc_id } [ | { grep grep_options | more } ]
```

**bvc-bucket nseinse\_id bvci bvc\_id**

Displays traffic status for a specific BVC bucket identified by the NSEI (network service entity ID) and BVCI (BSSGP virtual connection ID).

*nse\_ID* is an integer from 0 through 65535.

*bvc\_ID* is an integer from 0 through 65000.

**bvc-stat nseinse\_id bvci bvc\_id**

Displays traffic status for a BVC identified by the NSEI (network service entity ID) and BVCI (BSSGP virtual connection ID).

*nse\_ID* is an integer from 0 through 65535.

*bvc\_ID* is an integer from 0 through 65000.

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display BVC status of the BSSGP layer for specified NSEI and BVCI.

**Example**

The following command displays BSSGP traffic status for the BVC bucket for NSEI 2556 BVCI 241.

```
show bssgp status bvc-bucket nsei 2556 bvci 241
```

**Important**

Descriptions for show command outputs are available in the *Statistics and Counters Reference*.

## show build

Displays detailed information about the currently active StarOS release build.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show build [ | { grep grep_options | more } ] ]
```

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For information on usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines** Use this command to display detailed information on the currently active StarOS release build.

### Example

The following command displays StarOS build information:

```
show build
```

## show bulkstats

Displays information on bulk statistics.

**Product** All

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

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **show bulkstats** [ [ **data** ] | [ **schemas** ] | [ **variables** [ *schema\_name* ] [ **obsolete** ] ] [ | { **grep** *grep\_options* | **more** } ] ]

### data

Displays collected bulk statistical data.

### schema

Displays the configuration of the statistics to be collected on a per-schema basis.



**Important** For information on available schemas, refer to the *Bulk Statistics Configuration Mode Commands* chapter.

### variables *schema\_name*

Displays all valid bulkstat schema statistics, or only the statistics for the specified schema.

*schema\_name* specifies the name of the schemas available on system. The following is the list of available schemas in this release.

- aal2

- alcap
- apn
- asngw
- asnpc
- bcmcs
- card
- closedrp
- common
- context
- cs-network-ranap
- cs-network-rtp
- cs-network-sccp
- cscf
- cscfintf
- dcca
- dcca-group
- diameter-acct
- diameter-auth
- diameter-acct
- dlci-util
- dpca
- ecs
- egtpc
- epdg
- fa
- flow-kpi
  
- fng
- gprs
- gtpc
- gtpu
- gtpu
- ha
- hnbgw-access




---

**Important** In Release 20, 21.0 and 21.1, HeNBGW is not supported. For more information, contact your Cisco account representative.

---

- hnbgw-network




---

**Important** In Release 20, 21.0 and 21.1, HeNBGW is not supported. For more information, contact your Cisco account representative.

---

- hnbgw-hnbap



---

**Important** In Release 20 and later, HNMGW is not supported. For more information, contact your Cisco account representative.

---

- hnmgw-hnbap-access-closed



---

**Important** In Release 20 and later, HNMGW is not supported. For more information, contact your Cisco account representative.

---

- hnmgw-hnbap-access-hybrid



---

**Important** In Release 20 and later, HNMGW is not supported. For more information, contact your Cisco account representative.

---

- hnmgw-hnbap-access-open



---

**Important** In Release 20 and later, HNMGW is not supported. For more information, contact your Cisco account representative.

---

- hnmgw-iubc-sabp



---

**Important** In Release 20 and later, HNMGW is not supported. For more information, contact your Cisco account representative.

---

- hnmgw-iubc-tcp



---

**Important** In Release 20 and later, HNMGW is not supported. For more information, contact your Cisco account representative.

---

- hnmgw-ranap



---

**Important** In Release 20 and later, HNMGW is not supported. For more information, contact your Cisco account representative.

---

- hnmgw-ranap-access-closed



---

**hpoint** In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

---

- hnbgw-ranap-access-hybrid



---

**hpoint** In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

---

- hnbgw-ranap-access-open



---

**hpoint** In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

---

- hnbgw-rtp



---

**hpoint** In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

---

- hnbgw-rtp-access-closed



---

**hpoint** In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

---

- hnbgw-rtp-access-hybrid



---

**hpoint** In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

---

- hnbgw-rtp-access-open



---

**hpoint** In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

---

- hnbgw-rua




---

**Important** In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

---

- hnbgw-rua-access-closed




---

**Important** In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

---

- hnbgw-rua-access-hybrid




---

**Important** In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

---

- hnbgw-rua-access-open




---

**Important** In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

---

- hnbgw-sabp




---

**Important** In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

---

- hnbgw-sabp-access-closed




---

**Important** In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

---

- hnbgw-sabp-access-hybrid




---

**Important** In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

---

- hnbgw-sabp-access-open






---

**Important** In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

---

- hnbgw-sctp




---

**Important** In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

---

- hsgw
- hss
- icnr
- imsa
- ippool
- ipsg
- lac
- lcs
- link-aggr
- lma
- lns
- mag
- map
- mipv6ha
- mme
- mvs
- nat-realm
- p2p
- pcc-af
- pcc-policy
- pcc-quota
- pcc-service
- pcc-sp-endpt
- pdg
- pdif
- pgw
- phsgw
- phspc
- port
- ppp
- ps-network-gtpu
- ps-network-ranap
- ps-network-sccp
- radius
- radius-group

- readdress-server
- rlf
- rlf-detailed
- rp
- rulebase
- samog
- sbc
- sccp
- sgs
- sgs-vlr
- sgsn
- sgtp
- sgw
- sls
- ss7link
- ss7rd
- system
- tai
- vlan-npu
- vpn
- wsg

### obsolete

This keyword shows obsolete (but still available) schema variables. An asterisk (\*) is displayed next to schema variables that have been obsoleted.

### { **grep** *grep\_options* | **more** }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For information on usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display information on bulk statistics supported by the system.

The **variable** keyword can be used to list statistics supported by the system either for all schemas, or for an individual schema.

The **schema** keyword can be used to display the configuration of settings for bulk statistics, including the schema.

The **data** keyword can be used to display bulk statistic data collected up to that point.

### Example

The following command displays bulk statistics data:

```
show bulkstats data
```

The following command displays bulk statistics schema configuration:

```
show bulkstats data schemas
```




---

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show ca-certificate

Displays information for Certificate Authority (CA) digital certificates configured on this system.

---

**Product** All

---

**Privilege** Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show ca-certificate { all | name *name* }**
**all**

Displays information about all the configured CA certificates.

**name *name***

Displays information about an existing configured CA certificate name specified as n alphanumeric string of 1 through 128 characters.

---

**Usage Guidelines** View information for CA certificates configured on this system.

**Example**

The following command displays information for a CA certificate named *cert-1*:

```
show ca-certificate name cert-1
```




---

**Important**

Output descriptions for some commands are available in the *Statistics and Counters Reference*.

---

## show ca-crl

Displays information for Certificate Authority (CA) Certificate Revocation List (CRL) configured on this system.

## show cae-group server

**Product** All

**Privilege** Inspector

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **show ca-crl { all | name name }**

### all

Displays information about all the configured CA-CRLs.

### name name

Displays information about an existing CA-CRL name specified as an alphanumeric string of 1 through 128 characters.

**Usage Guidelines** View information for CA-CRLs on this system.

### Example

The following command displays information for a CA-CRL named *crl-5*:

```
show ca-crl name crl-5
```



**Important** Output descriptions for some commands are available in the *Statistics and Counters Reference*.

## show cae-group server

Displays configuration information, including the name of the associated CAE group, for all CAEs or for a specific CAE. The CAE (Content Adaptation Engine) is an optional component of the Mobile Videoscape.



**Important** In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

**Product** MVG

**Privilege** Security Administrator, Administrator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**    **show cae-group server { all | name *cae\_name* }**

**all**

Shows the configuration information, including the associated CAE group, for all CAEs.

**name *cae\_name***

Shows the configuration information for a specific CAE.

**Usage Guidelines**

Use this command to display configuration information for all CAEs or for a specific CAE. This command can be issued from either the local context or the context in which the associated CAE group is defined.

**Example**

The following command displays configuration information for the CAE named *server\_1*:

```
show cae-group server name server_1
```

## show call-control-profile

Displays information for call control profiles configured on the system.

**Product**

MME  
SGSN

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

**show call-control-profile { all | full { all | name *profile\_name* } | name *profile\_name* } [ | { **grep** *grep\_options* | **more** } ]**

**all**

Lists all call-control profiles configured on the system.

**full { all | name *profile\_name* }**

**full**: Displays a full set (all) of available information in the call-control profile.

**all**: Displays a full set of available information for all call-control profiles configured on the system.

**name *profile\_name***: Displays full information for an existing call-control profile specified as an alphanumeric string of 1 through 64 characters.

**name *profile\_name***

Displays information for an existing call-control profile specified as an alphanumeric string of 1 through 64 characters.

**| { *grep grep\_options* | *more* }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display information for call-control profiles configured on the system. Call-control profiles are configured through the global configuration mode and in the call-control profile configuration mode. For more information regarding call-control profile commands, refer to the *Call-Control Profile Configuration Mode Commands* chapter.

**Example**

The following command displays all available information for a call-control profile named *call-prof2*:

```
show call-control-profile full name call-prof2
```

## show call-home

Displays information for Smart Call Home settings configured on the system.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show call-home [ alert-group | detail | mail-server status | profile [
all | name profile_name ] | statistics [ | { grep grep_options | more } ] ]
```

**alert-group**

Displays information for all alert groups configured on the system. It also indicates if an alert-group has been disabled by the user.

**detail**

Displays general information and alert-group settings for all configured call-home profiles.

**mail-server status**

Displays status information for call-home mail servers that are configured on the system.

**profile { all | name *profile\_name* }**

Displays all available information for all call-home profiles on the system or a specified call-home profile.

**all:** Displays all available information for all call-home profiles configured on the system.

**name *profile\_name*:** Displays all available information for an existing call-home profile specified as an alphanumeric string of 1 through 31 characters.

**name *profile\_name***

Displays information for a call-home profile specified as an alphanumeric string of 1 through 31 characters.

**statistics**

Displays statistical information for call-home statistics configured on the system.

**{ *grep grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display profile and notification policy information associated with the call-home profiles configured on the system. Call-home profiles are configured through the Context Configuration Mode and in the Call-home Configuration Mode. For more information regarding call-home commands, refer to the *Call Control Profile Configuration Mode Commands* chapter.

**Example**

The following command displays all available information for a call-home profile named *call-home-profl*:

```
show call-home profile name call-home-profl
```

## show camel-service

Displays configuration details for Customized Applications for Mobile networks Enhanced Logic (CAMEL) services configured for this SGSN.

**Product** SGSN

**Privilege** Inspector

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **show camel-service { all | name *service\_name* } [ | *grep grep\_options* | more ]**

**all**

Displays the configuration details for all configured CAMEL services.

**name**

Displays the configuration details for an existing CAMEL service specified as an alphanumeric string of 1 through 63 characters.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

View configuration information for CAMEL services.

**Example**

The following command displays the configuration information for a CAMEL service identified as *camel4sgsnTO*:

```
show camel-service name camel4sgsnTO
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

# show card

Displays various types of information for a card or all cards in the system.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show card { diag [ slot# ] | hardware [ slot# ] | info [ slot# ] | mappings
| table [ all ] } [ | { grep grep_options | more } ]
```

**diag**

Displays diagnostic results for a specific card or all cards.



**hardware**

Displays information about installed hardware.

**info**

Displays detailed information for a specific card or all cards

**mappings**

Displays mappings between front-installed application cards and rear-installed interface cards.



---

**Important** This keyword is only supported on the ASR 5000.

---

**table [all]**

Displays information about each card in tabular output. The **all** option includes empty slots in the output.

**slot#**

Specifies the slot number for a card as an integer from 1 through 48.

**{ { grep grep\_options | more } }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Use this command to view various types of information for all cards or a specified card.

**Example**

The following command displays diagnostic information for the card in slot 1:

```
show card diag 1
```



---

**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show cbs counters



---

**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

---

Displays counters associated with cell broadcasting service (CBS).

**Product**

HNBGW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show cbs counters [ cbs-service cbs_service_name ] [ | { grep grep_options | more } ]
```

**cbs-service *cbs\_service\_name***

Displays information for specific CBS service. *cbs\_service\_name* is a string of size 1 through 63.

**| { **grep** *grep\_options* | **more** }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

**Usage Guidelines**

Use this command to display the counters for CBS service

**Example**

The following command displays the counters for the CBS named *my\_service*:

```
show cbs counters cbc-service my_service
```

## show cbs sessions

**Important**

In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

This command displays the information for CBS sessions.

**Product**

HNBGW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show cbs sessions [ all ] [ cbc-address cbc_address | cbs-service
cbs_service_name ] [ [ full | summary ] [ cbc-address cbc_address | cbs-service
cbs_service_name ] ] [ | { grep grep_options | more } ]
```

**all**

Displays all CBS sessions.

**cbc-address *cbc\_address***

Specifies the IP address of a Cell Broadcast Center (CBC) in IPv4 dotted-decimal notation.

**cbs-service *cbs\_service\_name***

Displays information for a named CBS service. *cbs\_service\_name* is an alphanumeric string of 1 through 63 characters.

**full**

Displays all available session information.

**summary**

Displays summary information for CBS sessions

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

**Usage Guidelines**

Use this command to display the information for CBS sessions.

**Example**

The following command displays the full session information for CBS address *101.102.109.211*:

```
show cbs sessions full cbc-address 101.102.109.211
```

## show cbs statistics

**Important**

In Release 20 and later, HN BGW is not supported. This command must not be used for HN BGW in Release 20 and later. For more information, contact your Cisco account representative.

Displays CBS statistics.

**Product**

HN BGW

<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<p><b>show cbs statistics</b> [ <b>cbc-address</b> <i>cbc_address</i>   <b>cbs-service</b> <i>cbs_service_name</i> ] [ <b>sabp-only</b>   <b>tcp-only</b>   <b>verbose</b> ] [   { <b>grep</b> <i>grep_options</i>   <b>more</b> } ]</p> <p><b>cbc-address</b> <i>cbc_address</i> Designates the IP address of a CBC in IPv4 dotted-decimal notation.</p> <p><b>cbs-service</b> <i>cbs_service_name</i> Displays information for a named CBS service. <i>cbs_service_name</i> is an alphanumeric string of 1 through 63 characters.</p> <p><b>sabp-only</b> Displays Service Area Broadcast Protocol (SABP) statistics for the selected CBS Service.</p> <p><b>tcp-only</b> Displays TCP statistics for the selected CBS Service.</p> <p><b>verbose</b> Displays more detailed CBS statistics.</p> <p>  { <b>grep</b> <i>grep_options</i>   <b>more</b> } Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. Refer to <i>Regulating a Command's Output</i> section of the <i>Command Line Interface Overview</i> chapter for details on the usage of <b>grep</b> and <b>more</b>.</p>
<b>Usage Guidelines</b>	Use this command to display the statistics for CB service.

**Example**

The following command displays the SABP statistics for the CBC at *101.102.109.211*:

```
show cbs statistics cbc-address 101.102.109.211 sabp-only
```

# show cbs-service



**Important** In Release 20 and later, HNMGW is not supported. This command must not be used for HNMGW in Release 20 and later. For more information, contact your Cisco account representative.

Displays information for all or a specific CBS service.

---

**Product**

HNMGW

---

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
show cbs-service { all | name cbs_service_name } [ status ] [ | { grep grep_options | more } ]
```

**all**

Displays all CBS services.

**name***cbs\_service\_name*

Displays information for named CBS service. *cbs\_service\_name* is an alphanumeric string of 1 through 63 characters.

**status**

Display detailed status.

**{ | grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

---

**Usage Guidelines**

Use this command to display the information for all or a specific CBS service.

**Example**

The following command displays the detailed status of a CBS service with name *my\_service*:

```
show cbs-service name my_service status
```

# show cdr

Displays information about Charging Data Records (CDRs).

---

## Product

ACS

---

## Privilege

Security Administrator, Administrator, Operator, Inspector

---

## Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

## Syntax Description

```
show cdr { file-space-usage | statistics } [ | { grep grep_options | more } ]
```

### file-space-usage

Displays the amount of file space used by Charging Data Record (CDR) files.

### statistics

Displays CDR file statistics.

### | { grep *grep\_options* | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

## Usage Guidelines

Use this command to view CDR flow control information.

### Example

The following command displays CDR files statistics:

```
show cdr statistics
```

The following command displays the amount of file space used by the CDR files:

```
show cdr file-space-usage
```




---

### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

# show certificate

Displays information about the certificates configured on this system.

---

**Product** All

---

**Privilege** Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show certificate { all | name *name* }**

## **all**

Displays information about all the configured certificates on this system.

## **name *name***

Displays information of a specified certificate configured.

*name* must be the name of an existing certificate specified as an alphanumeric string of 1 through 128 characters.

---

**Usage Guidelines** View information for local node certificates on this system.

## **Example**

The following command displays information for a node certificate named *certificate-3*:

```
show certificate name certificate-3
```




---

**Important**

Output descriptions for some commands are available in the *Statistics and Counters Reference*.

---

# show cgw-service

Displays configuration and/or statistical information for CGW services on this system.

---

**Product** SaMOG

---

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

---

**Syntax Description** **show cgw-service { all | name *name* | statistics { all [ verbose ] [ | { grep *grep\_options* | more } ] | name *name* } } [ | { grep *grep\_options* | more } ]**

**all**

Displays all CGW services.

**name *name***

Displays information for an existing CGW service specified as an alphanumeric string of 1 through 63 characters.

**statistics**

Displays node level Statistics for CGW.

**verbose**

Specifies detailed statistics.

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to displays configuration and/or statistical information for CGW services on this system.

**Example**

The following command displays information for all CGW services:

```
show cgw-service all
```

# show cli

Displays current or historical information about command line interface (CLI) user session(s).

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show cli { configuration-monitor | history [ all | exclude-show ] | session
}
[ | { grep grep_options | more } ]
```



**configuration-monitor**

Displays information related to the **cli configuration-monitor** command, including the number of seconds remaining until the next configuration monitor check is performed.

**history [ all | exclude-show ]**

Displays CLI command history for this CLI session when another option is not selected.

**all**: Displays the CLI command history for all CLI sessions.

**exclude-show**: Excludes **show** commands.

**session**

Displays information about the current CLI session.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Displays current or historical CLI sessions. This command is useful when there is some unexpected output from a chassis and a check of current CLI users may reveal other in-progress activities that may have contributed to the anomaly.

**Example**

The following command displays information about all current CLI sessions:

```
show cli
```

# show clock

Displays the current system data and time.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show clock [ universal ] [ | { grep grep_options | more } ]
```

**universal**

Displays the date and time in universal coordinated time (UTC/GMT) format.

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Check the current time of a chassis to compare with network wide time or for logging purposes if network accounting and/or event records appear to have inconsistent timestamps.



### Important

This command is not supported on all platforms.

### Example

The following displays the system time in local time and UTC, respectively.

```
show clock
```

```
show clock universal
```

## show cloud configuration

Displays the contents of the configuration file.

### Product

VPC

### Privilege

Security Administrator, Administrator, Inspector, Operator

### Mode

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax

```
show cloud configuration
```

### Usage

This command dumps the contents of the configuration file to the screen. It displays the configuration file on the config disk or the local flash. Usually the user does not have direct access to these files. The local param file on the flash is defined during the VPC installation and the config disk is usually created by the orchestrator and then attached to the card.

**Example**

This command displays the hardware configuration associated with card number 1:

```
show cloud configuration
```

## show cloud hardware

Displays information regarding the configuration for each card or a specific card.

---

**Product**

VPC

---

**Privilege**

Security Administrator, Administrator, Inspector, Operator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show cloud hardware [iftask | optimum | test] [card_number]
```

**iftask**

Displays IFTASK information.

**optimum**

Displays the optimum configuration of the underlying VM hardware according to the available parameters. It provides information regarding the configured vCPU, memory size, huge page size, crypto hardware and the NIC.

**test**

Compares the configuration of the underlying VM hardware of a specific card or all cards in the VPC to the optimum configuration. It provides information regarding the configured vCPU, memory size, huge page size, crypto hardware and the NIC and indicates the optimum values for each parameter.

**card\_number**

Specifies the number of the card for which to display information. If no card number is specified, the command displays information for each of the running cards.

**Usage**

Displays the configuration of the underlying VM hardware for a specific card or all cards in the VPC. When no optional keywords are provided, the command displays information regarding the configured vCPU, memory size, huge page size, crypto hardware and the NIC.

**Example**

This command displays the hardware configuration associated with card number 1:

```
show cloud hardware test 1
```

This command displays the hardware configuration associated with card number 1:

```
show cloud hardware 1
```

This command displays the optimum hardware configuration for the associated VM hardware:

```
show cloud hardware optimum
```

## show cloud monitor

Displays VPC-DI network latency and packet loss statistics for all cards or a specific card in the VPC.

**Product**

VPC-DI

**Privilege**

Security Administrator, Administrator, Inspector, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show cloud monitor di-network {detail | summary} card_number
show cloud monitor controlplane [dst dst_slot ] [ src src_slot ]
show cloud monitor dataplane [dst dst_slot ] [ src src_slot ]
```

**detail**

Displays detailed information about the VPC-DI network.

**summary**

Displays summary information about the VPC-DI network.

**card\_number**

Specifies the number of the card for which to display information.

**controlplane**

Displays the most recent Control Plane monitor information.

**dataplane**

Displays the most recent Data Plane monitor information.

**dst *dst\_slot***

Specifies the slot to which the request was directed.

**src *src\_slot***

Specifies the slot that originated the request.

**Usage Guidelines**

Displays the configuration of the underlying VM hardware for a specific card or all cards in the VPC. It provides information regarding the configured vCPU, memory size, huge page size, crypto hardware and the NIC.

The **show cloud monitor controlplane [dst *dst\_slot*] [src *src\_slot*]** command displays the most recent Control Plane monitor information.

The **show cloud monitor dataplane [dst *dst\_slot*] [src *src\_slot*]** command displays the most recent Control Plane monitor information.

**Example**

This command displays summary monitored statistics for VPC-DI network communications from and to the third card in the VPC. The display shows the test packet loss rate for the past five minutes and past 60 minutes. If the rate is larger than 1%, the health status is marked as "Bad".

**show cloud monitor di-network summary 3**

Card 3 Test Results:

ToCard	Health	5MinLoss	60MinLoss
1	Good	0.0%	0.0%
2	Good	0.0%	0.0%
4	Bad	6.32%	5.36%
5	Good	0.0%	0.0%
6	Good	0.0%	0.0%

The following command displays slot 3 as the source slot from where the Control Plane monitor information originated.

Specifies the slot that originated the request.

**show cloud monitor controlplane src\_slot 3**

The following command displays slot 6 as the destination slot from where the most recent Data Plane monitor information was requested.

**show cloud monitor dataplane dst\_slot 6**

## show cmp history

Displays historical information for the last 100 Certificate Management Protocol v2 transactions.

**Product**

All products supporting IPsec CMPv2 features

**Important**

This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

**show cmp history**

**Usage Guidelines**

Display historical information for the last 100 Certificate Management Protocol v2 transactions.

**Example**

The following command displays CMPv2 transaction history:

```
show cmp history
```

## show cmp outstanding-req

Displays details regarding outstanding Certificate Management Protocol v2 requests.

**Product**

All products supporting IPSec CMPv2 features

**Important**

This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

**show cmp outstanding-req**

**Usage Guidelines**

Display information for outstanding Certificate Management Protocol v2 requests.

**Example**

The following command displays outstanding CMPv2 requests:

```
show cmp outstanding-req
```

## show cmp statistics

Displays statistics related to Certificate Management Protocol v2 functions.

---

### Product

All products supporting IPsec CMPv2 features




---

### Important

This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

---



---

### Privilege

Security Administrator

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

**show cmp statistics**

---

### Usage Guidelines

Display statistics related to Certificate Management Protocol v2 functions.

### Example

The following command displays CMPv2 statistics:

```
show cmp statistics
```

## show confdmgr

Displays information about the StarOS ConfD Manager (confdmgr) process and its association with NETCONF protocol. ConfD and NETCONF intercommunicate with the Cisco Network Service Orchestrator (NSO).

---

### Product

All

---

### Privilege

Security Administrator, Administrator, Operator

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax

```
show confdmgr [ confd { cdb | netconf | state } | model { bulkstats |
confd } | subscriptions ] [ | { grep grep_options | more } ]
```

**confd { cdb | netconf | state }**

Displays information about the ConfD engine based on the specified keyword:

- **cdb** - displays ConfD Configuration Database (CDB) information
- **netconf** - displays NETCONF state information
- **state** - displays current ConfD state information

**model { bulkstats | confd }**

Displays information about the ConfD model based on the specified keyword:

- **bulkstats** - bulk statistics configuration and operational data
- **confd** - server ConfD configuration

**subscriptions**

Displays ConfD CDB subscription information.

**{ { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Used this command to display useful in monitoring and troubleshooting NETCONF protocol.

**Example**

The following command displays ConfD subscription information.

```
show confdmgr subscriptions
```

# show configuration

Displays current configuration information for various subcomponents of the system.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show configuration [ active-charging service { all | name srvc_name } | apn
apn_name
```



```

| brief | bulkstats | card card_num | checksum | context name
| link-aggregation group group_number | obsolete-encryption | port slot/port
| rohc | showsecrets | srp | url url | verbose ] [ | { grep grep_options |
more } ]

show configuration active-charging service { all | name svrc_name } [ brief
| obsolete-encryption | showsecrets | verbose ]
show configuration apn apn_name [ obsolete-encryption | showsecrets | verbose
]
show configuration brief
show configuration bulkstats [ brief | verbose ]
show configuration card card_num [ brief | obsolete-encryption | showsecrets
| verbose ]
show configuration checksum [ brief | obsolete-encryption | showsecrets
| verbose ]
show configuration confd [ brief | verbose ]
show configuration context name [ brief | obsolete-encryption | radius |
showsecrets | verbose ]
show configuration link-aggregation group group_number
show configuration obsolete-encryption
show configuration port slot/port [ brief | obsolete-encryption | showsecrets
| verbose ]
show configuration rohc [ all | profile-name name ] [ brief | verbose ]
show configuration showsecrets [ obsolete-encryption ]
show configuration srp [ brief | checksum | obsolete-encryption |
showsecrets | verbose ]
show configuration url url
show configuration verbose [ obsolete-encryption | showsecrets ]

```

#### **active-charging service { all | name *svrc\_name* | statistics }**

Displays all active charging parameters for all services, or a specified service name expressed as an alphanumeric string of 1 through 15 characters, or service statistics.

#### **apn *apn\_name***

Specifies an APN for which to display the configuration information. All contexts are searched for this APN, and if a match found, the StarOS returns the configuration of this APN.

#### **brief**

Displays current configuration information in brief form.



#### **Important**

The **brief** keyword is only available in StarOS 20.0 and higher releases.

#### **bulkstats**

Displays the URL for the backup bulkstats configuration file if it has been configured.

**card *card\_num***

Specifies a card for which configuration information is to be displayed as an integer from 1 through 48 for the ASR 5000 or 1 through 20 for the ASR 5500.

**checksum**

Generates and displays a checksum value for the configuration data.

**confd**

Displays subset of configuration information for ConfD and NETCONF protocol. (ASR 5500 and VPC platforms only)

**context *name***

Specifies an existing context for which configuration information is to be displayed as an alphanumeric string of 1 through 79 characters.

**link-aggregation group *group\_number***

Displays the current configuration of the LAG specified by group number as an integer from 1 through 1023.

**obsolete-encryption**

Shows encrypted values using a weaker, obsolete encryption method (prior to release 12.2).

**Important**


---

The **obsolete-encryption** keyword is only available in StarOS 19.1 and prior releases.

---

**port *slot/port***

Displays configuration information for a port identified by its slot and port numbers.

**rohc [ all | profile-name *name***

Specifies that information for all robust header compression (RoHC) profiles or the named profile is to be displayed.

**showsecrets**

Displays encrypted and unencrypted secret keys saved in the configuration. If this keyword is not specified, secret keys are not displayed.

**Important**


---

This keyword is restricted to Administrator privilege or higher.

---

**Important**


---

The **showsecrets** keyword is only available in StarOS 19.1 and prior releases.

---

**srp**

Shows the Service Redundancy Protocol (SRP) configuration used for Interchassis Session Recovery (ICSR) deployments.

**url *url***

Default: configuration which is currently in use.

This keyword is not available to users with Operator level permissions. Specifies the location of the configuration data to use for information display. The *url* may refer to a local or a remote file and must be entered in the following format:

For the ASR 5000:

```
[ file: ]{ /flash | /pcmcia1 | /hd }[ /directory ]/file_name
tftp://{ host[ :port# ] }[ /directory ]/file_name
[ http: | ftp: | sftp: ]//[ username[ :password ]@ ] { host }[ :port# ] [ /directory
]/file_name
```

For the ASR 5500:

```
[ file: ]{ /flash | /usb1 | /hd }[ /directory ]/file_name
tftp://{ host[ :port# ] }[ /directory ]/file_name
[ http: | ftp: | sftp: ]//[ username[ :password ]@ ] { host }[ :port# ] [ /directory
]/file_name
```




---

**Important** FTP is not supported in StarOS 20.0 or higher Trusted Builds.

---




---

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

---

*directory* is the directory name.

*filename* is the actual file of interest.




---

**Important** Configuration files should be named with a **.cfg** extension.

---

*username* is the user to be authenticated.

*password* is the password to use for authentication.

*host* is the IP address or host name of the server.

*port#* is the logical port number that the communication protocol is to use.

**verbose**

Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

```
{ grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

View the current configuration to analyze recent changes. For additional information, refer to the Administration Guides for products installed on your system.

### Example

The following command displays the local in-use port configuration information for port *24/1* in verbose mode.

```
show configuration port 24/1 verbose
```

The following command displays the local in-use port configuration information for port *5/11* in verbose mode.

```
show configuration port 5/11 verbose
```

The following command displays the configuration of all RADIUS server groups configured in context *local*

```
show configuration context local radius group all
```

The following command shows the configuration for a context named PGW.

```
show configuration context pgw
```

## show configuration errors

Displays current configuration errors and warning information for the target configuration file as specified for a service.

### Product

All

### Privilege

Security Administrator, Administrator, Operator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show configuration errors [ section section_name ] [ verbose ] [ | { grep grep_options | more } ]
```

**section** {*section\_name*}

Specifies the services and section for which to display and validate a configuration.

The following services and sections are supported:

- **aaa-config**: Displays configuration errors/warnings for the AAA service(s) configured on the system.
- **active-charging**: Displays configuration errors/warnings for the Enhanced Charging Service(s) and the Personal Stateful Firewall service(s) configured on the system.
- **alcap-service**: Displays configuration errors/warnings for Access Link Control Application Part (ALCAP) on HNB-GW for IuCS-over-ATM support towards CS core network.




---

**important** In Release 20 and later, HNBGW is not supported. This keyword must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

---

- **apn**: Displays configuration errors/warnings for the APN configuration(s) on the system.
- **apn-profile**: Displays configuration errors/warnings for the APN Profile configuration(s) on the system.
- **apn-remap-table**: Displays configuration errors/warnings for the APN Remap Table configuration(s) on the system.
- **asngw-service**: Displays configuration errors/warnings for the Access Service Network Gateway (ASN-GW) Service configured in a specific context for which configuration errors/warnings is to be displayed.
- **asnpc-service**: Displays configuration errors/warnings for the ASN Paging Controller and Location Registry (ASN PC-LR) Service(s) configured on the system.
- **call-control-profile**: Displays configuration errors/warnings for the Call Control Profile configuration(s) on the system.
- **camel-service**: Displays configuration errors/warnings for the Customised Applications for Mobile networks Enhanced Logic (CAMEL) Service configuration(s) on the system.
- **closed-rp-service**: Displays configuration errors/warnings for the closed RP service(s) configured on the system.
- **cs-network**: Displays configuration errors/warnings for the circuit switched (CS) network configuration(s) on the system.
- **diameter**: Displays configuration errors/warnings for the Diameter configuration(s) on the system.
- **dns-client**: Displays configuration errors/warnings for the DNS client configuration(s) on the system.
- **egtp-service**: Displays configuration errors/warnings for the evolved GPRS Tunneling Protocol (eGTP) service configuration(s) on the system.
- **event-notif**: Displays configuration errors/warnings for the event notification (SNMP) interface client.
- **fa-service**: Displays configuration errors/warnings for the Foreign Agent (FA) service(s) configured on the system.
- **fng-service**: Displays configuration errors/warnings for the Femto Network Gateway (FNG) configuration(s) on the system.
- **ggsn-service**: Displays configuration errors/warnings for the Gateway GPRS Support Node (GGSN) service(s) configured on the system.
- **gprs-service**: Displays configuration errors/warnings for the General Packet Radio Service (GPRS) service(s) configured on the system.
- **gs-service**: Displays configuration errors/warnings for the Gs service(s) configured on the system. The Gs interface between the SGSN and the MSC (VLR) uses the BSSAP+ protocol.
- **ha-service**: Displays configuration errors/warnings for the Home Agent (HA) service(s) configured on the system.
- **hnbgw-network-service**: Displays configuration errors/warnings for the Home Evolved Node B Gateway (HNB-GW) network service configuration(s) on the system.




---

**important** In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

- **hnbgw-service**: Displays configuration errors/warnings for the Home Evolved Node B Gateway (HNB-GW) Service configuration(s) on the system.




---

**important** In Release 20 and later, HNBNB is not supported. This keyword must not be used for HNBNB in Release 20 and later. For more information, contact your Cisco account representative.

---

- **hsgw-service**: Displays configuration errors/warnings for the HRPD Serving Gateway (HSGW) service(s) configured on the system.
- **imei-profile**: Displays configuration errors/warnings for the International Mobile Equipment Identity (IMEI) Profile configuration(s) on the system.
- **imsa-config**: Displays configuration errors/warnings for the IMS Authorization (IMSA) configuration(s) on the system.




---

**important** In 16.0 and later releases, error message will be displayed in the output of **show configuration errors** command when the user tries to configure an endpoint which is already configured in other IMSA service.

---

- **imssh-service**: Displays configuration errors/warnings for the IMS Sh (IMSSh) service(s) configured on the system.
- **imsue-service**: Displays configuration errors/warnings for the IMS UE service(s) configured on the system.
- **ipms**: Displays configuration errors/warnings for the Intelligent Packet Monitoring System (IPMS) service(s) configured on the system.
- **ipne**: Displays configuration errors/warnings for the IP Network Enabler (IPNE) facility configured on the system.
- **ipsg-service**: Displays configuration errors/warnings for the IP Security Gateway (IPSG) service(s) configured on the system.
- **iups-service**: Displays configuration errors/warnings for the IuPS service(s) configured on the system.
- **lac-service**: Displays configuration errors/warnings for the Layer 2 Tunneling Protocol (L2TP) Access Concentrator (LAC) service(s) configured on the system.
- **lns-service**: Displays configuration errors/warnings for the L2TP Network Server (LNS) service(s) configured on the system.
- **local-policy**: Displays configuration errors/warnings for the Local Policy configuration(s) on the system.
- **map-service**: Displays configuration errors/warnings for the SS7 Mobile Application Part (MAP) service(s) configured on the system.
- **mme-service**: Specifies the configuration errors for a Mobility Management Entity (MME) service configured in a specific context for which configuration errors/warnings are to be displayed.

- **operator-policy**: Displays configuration errors/warnings for the Operator Policy configuration(s) on the system.
- **pcc-policy-service**: Displays configuration errors/warnings for the Policy and Charging Control (PCC) Policy Service configuration(s) on the system.
- **pcc-quota-service**: Displays configuration errors/warnings for the Policy and Charging Control (PCC) Quote Service configuration(s) on the system.
- **pcc-service**: Displays configuration errors/warnings for the PCC Service configuration(s) on the system.
- **pdg-service**: Displays configuration errors/warnings for the Packet Data Gateway (PDG) Service configuration(s) on the system.
- **pdif-service**: Displays configuration errors/warnings for the Packet Data Interworking Function (PDIF) service(s) configured on the system.
- **pdsn-service**: Displays configuration errors/warnings for the Packet Data Serving Node (PDSN) service(s) configured on the system.
- **pgw-service**: Displays configuration errors/warnings for the PDN-Gateway (P-GW) service configuration(s) on the system.
- **phsgw-service**: Displays configuration errors/warnings for the Payload Header Suppression (PHS) Gateway service(s) configured on the system.
- **policy-grp-config**: Displays configuration errors/warnings for the Policy Group configuration(s) on the system.
- **ps-network**: Displays configuration errors/warnings for the packet switched (PS) network configuration(s) on the system.
- **saegw-service**: Displays configuration errors/warnings for the System Architecture Evolution Gateway (SAE-GW) Service configuration(s) on the system.
- **sccp-network**: Displays configuration errors/warnings for the Signaling Connection Control Part (SCCP) network configuration(s) on the system.
- **sgs-service**: Displays configuration errors/warnings for the SGs Service configuration(s) on the system. The SGs interface connects the databases in the VLR and the MME.
- **sgsn-mode**: Displays configuration errors/warnings for the Serving GPRS Support Node (SGSN) mode configuration(s) on the system.
- **sgsn-service**: Displays configuration errors/warnings for the SGSN service(s) configured on the system.
- **sgtp-service**: Displays configuration errors/warnings for the SGSN GPRS Tunneling Protocol (SGTP) service(s) configured on the system.
- **sgw-service**: Displays configuration errors/warnings for the Serving Gateway (S-GW) service configuration(s) on the system.
- **subscriber-config**: Displays configuration errors/warnings for the subscriber configuration(s) on the system.
- **subscriber-map**: Displays configuration errors/warnings for the Subscriber Map configuration(s) on the system.

### verbose

Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

**{ *grep* *grep\_options* | *more* }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For more information on the usage of **grep** and **more**, refer *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to view the current configuration errors and warning to review recent changes. For additional information, refer to the Administration Guides for products installed on your ASR 5x00 system.

### Example

The following command displays configuration errors and warnings for all services configured in a context/system:

```
show configuration errors verbose | more
```

The following command displays configuration errors and warnings for Active Charging service and Personal Stateful Firewall service configured in a context:

```
show configuration errors section active-charging verbose
```

The following command displays configuration errors and warnings for QoS-configuration in a context:

```
show configuration errors section qos-marking verbose
```

## show congestion-control

Displays information pertaining to congestion control functionality on the system

### Product

All

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show congestion-control { configuration | statistics { manager [ all |
instance task_instance ] } [ | { grep grep_options | more } ]
show congestion-control statistics mme { critical | full | major | minor
} [ | { grep grep_options | more } ]
```

#### configuration

Displays congestion control configuration information including threshold parameters and policy settings for the configured services.

#### statistics

Displays congestion control statistics for manager services.



**manager**

Specifies the name of the service/session manager for which statistics are displayed. The following types of *manager* services are supported:

- **a11mgr**: Specifies that statistics are displayed for PDSN services.
- **asngwmgr**: Specifies that statistics are displayed for ASN-GW services.




---

**important** ASNGW is no longer supported. For more information, contact your Cisco account representative.

---

- **asnpcmgr**: Specifies that statistics are displayed for ASN PC-LR services.
- **bindmux**: Specifies that statistics are displayed for Bindmux Manager used by PCC service.
- **egtpinmgr**: Specifies that statistics are displayed for EGTP ingress demuxmgr.
- **gtpcmgr**: Specifies that statistics are displayed for GGSN services.
- **hamgr**: Specifies that statistics are displayed for HA services.
- **hnbmgr**: Specifies that statistics are displayed for HNB Manager used by HNB-GW service.




---

**important** In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

---

- **imsimgr**: Specifies that statistics are displayed for IMSI managers.
- **ipsecmgr**: Specifies that statistics are displayed for IPSec managers.
- **ipsgmgr**: Specifies that statistics are displayed for IPSG managers.
- **l2tpmgr**: Specifies that statistics are displayed for L2TP managers.
- **service**: Specifies that statistics are displayed for services.
- **sgmbmgr**: Specifies that statistics are displayed for SGMB Demux managers.

**statistics mme { critical | full | major | minor }**

Displays the statistics based on the current state of all instances of the specified task.

- **critical**: Specifies that statistics are displayed for the critical congestion policy for MME services.
- **full**: Specifies that statistics are displayed for all congestion policies for MME services.
- **major**: Specifies that statistics are displayed for the major congestion policy for MME services.
- **minor**: Specifies that statistics are displayed for the minor congestion policy for MME services.

**all**

Displays the statistics based on the current state of all instances of the specified task.

**instance task\_instance**

Displays statistics for a specified software task instance. *task\_instance* can be configured to an integer from 1 to 128.




---

**Important** The **inst** column of the **show task table** command output displays the instance of a particular task.

---

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

### Usage Guidelines

This command displays congestion control configuration information or statistics for a particular service type.

When the **all** keyword is used, the system compares the current state of all instances of the specified task. The state is based on whether or not any congestion control thresholds have been exceeded. If one or more instances are experiencing congestion, the state is displayed as "Applied", and the various thresholds that have been crossed are indicated.

### Example

The following command displays congestion control statistics for a PDSN service using an **allmgr** task with an instance of 2:

```
show congestion-control statistics allmgr instance 2
```

The following command displays congestion control statistics for an ASN-GW service using an **asngwmgr** task with an instance of 2:

```
show congestion-control statistics asngwmgr instance 2
```

The following command displays congestion control statistics for an ASN PC-LR service using an **asnpcmgr** task with an instance of 2:

```
show congestion-control statistics asnpcmgr instance 2
```




---

**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show connectedapps

Displays information about the current Connected Apps (CA) configuration.

---

### Product

SecGW (WSG)

---

### Privilege

Security Administrator, Administrator

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**    `show connectedapps`

---

**Usage Guidelines**    Displays information about the current Connected Apps (CA) configuration between the CA client on the ASR 9000 VSM and IOS-XR.

**Example**

This command displays Connected Apps configuration information:

```
show connected apps
```

## show content-filtering category database

Displays details of the specified category based content filtering database for content filtering application configured in a system/service.

---

**Product**    CF

---

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

---

**Command Modes**    Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**    `show content-filtering category database [ active | all | facility srdbmgr { all | instance instance_number } | url url_string ] [ verbose ] [ | { grep grep_options | more } ]`

**active**

Displays the information about all active databases, for example databases in memory. This is the default setting for category database information.

**all**

Displays the information about all active databases, for example, databases in memory and all saved databases on a system.

**facility**

Displays logged events for a specific facility.

**srdbmgr { all | instance *instance\_number* }**

Displays logged events for all static rating database managers or for all or for a specific instance.

- **all**: Displays the logged events for all Static Rating Database (SRDB) Manager instances.
- **instance *instance\_number***: Displays events logged for a specific SRDB Manager instance specified as an integer from 1 through 8.

**url *url\_string***

Displays the information of the database located at the URL that specifies the name/location of the category database from which to retrieve information as an alphanumeric string of 1 through 512 characters.

**verbose**

This option enables the detailed mode for additional information display for specific database.

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display information of database for category based content filtering application in a service.

**Example**

The following command displays a detailed information for all active databases in memory.

```
show content-filtering category database active all
```

The following command displays the CF database status of all running SRDB managers.

```
show content-filtering category database facility srdbmgr all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show content-filtering category policy-id

Displays Content Filtering category policy definitions.

**Important**

In StarOS 8.1 and later releases this command is replaced by the **show active-charging content-filtering category policy-id** command.

**Product**

CF

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show content-filtering category policy-id { all | id cf_policy_id } [ | {
grep grep_options | more } ]
```

**all**

Displays definitions of all Content Filtering category policies.

**id *cf\_policy\_id***

Displays definitions of an existing Content Filtering category policy ID specified as an integer from 1 through 4294967295.

**{ *grep grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view Content-Filtering Category definitions for a specific/all Policy IDs.

**Example**

The following command displays Content Filtering category definitions for policy ID 3:

```
show content-filtering category policy-id id 3
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show content-filtering category statistics

Displays statistics for the category-based Content Filtering application configured in a system/service.

**Product**

CF

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show content-filtering category statistics [ facility srdmgrp { all |
instance instance_number } ] [ | { grep grep_options | more } ]
```

**facility**

Displays logged events for a specific facility.

**srdmgrp { all | instance *instance\_number* }**

Displays logged events for all Static Rating Database (SRDB) Manager instances or for the specified instance.

- **all**: Displays events logged for all SRDB Manager instances.
- **instance *instance\_number***: Displays events logged for the SRDB Manager instance specified as an integer from 1 through 8.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to view the statistics of Category Based Content Filtering application in a service. This command's output also indicates capability of the system to perform Content Filtering and Dynamic Content Filtering if configured.



#### Important

Content filtering cannot be performed if less than two PSCs are activated. Dynamic Content Filtering cannot be performed if less than three PSCs are activated.

### Example

The following command displays the detailed statistics of configured category based content filtering application:

```
show content-filtering category statistics
```

The following command displays the detailed statistics of configured category based content filtering application based on running SRDB Manager *instance1*.

```
show content-filtering category statistics facility srdmgrp instance
instance1
```



#### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show content-filtering category url

Displays the information about the categories of the database at the specific URL configured for the category-based content filtering application in a system/service.

### Product

CF

### Privilege

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show content-filtering category url url_string [ policy-id cf_policy_id | rulebase rulebase_name ] [ verbose ] [ | { grep grep_options | more } ]
```

**url *url\_string***

Displays the category information of the URL specified as an alphanumeric string of 1 through 512 characters.

**policy-id *cf\_policy\_id***

Displays the category information of a URL configured with an existing content filtering category policy ID specified as n integer from 0 through 65535.

**rulebase *rulebase\_name***

Displays the category information of a URL configured in ACS Configuration Mode for category-based content filtering in specific rulebase.

*rulebase\_name* must be the name of an existing rulebase, and must be an alphanumeric string of 1 through 15 characters.

**verbose**

Enables the detailed mode for additional information display for a specific database.

**{ **grep** *grep\_options* | **more** }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display information of a database URL for category based content filtering application in a service.

**Example**

The following command displays a detailed information for all active databases in memory.

```
show content-filtering category url /cf_server/cf/optcmd.bin verbose
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

# show content-filtering server-group

Displays information for Content Filtering Server Group (CFSG) configured in the service.

---

## Product

CF

---

## Privilege

Security Administrator, Administrator, Operator, Inspector

---

## Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

## Syntax Description

```
show content-filtering server-group [ name cfs_name | statistics ] [ | { grep grep_options | more } ]
```

### **name** *cfs\_name*

Displays information for an existing CFSG specified as an alphanumeric string of 1 through 63 characters.

### **statistics**

Displays statistical information for all configured CFSGs.

### | { **grep** *grep\_options* | **more** }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

## Usage Guidelines

Use this command to display information for Content Filtering Server Group configured in a service.

### Example

The following command displays a detailed information for all charging actions:

```
show content-filtering server-group statistics
```

The following command displays a details of a specific charging action:

```
show content-filtering server-group name test123
```




---

### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---



# show context

Displays information for currently configured contexts.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
show context [ all | name context_name ] [ | { grep grep_options | more } ]
```

**all | name *context\_name***

**all**: Displays information for all currently configured contexts.

**name *context\_name***: Displays information for an existing context specified as an alphanumeric string of 1 through 79 characters.

**{ **grep** *grep\_options* | **more** }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

View configured contexts. This may be useful in verifying configuration or troubleshooting the system.

**Example**

The following command displays information for the configured context named *sampleContext*:

```
show context name sampleContext
```

The following command displays information for all contexts:

```
show context all
```




---

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

# show cpu

Displays information on system CPUs.

---

**Product** All

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show cpu** { **info** [ **card** *card\_num* [ **cpu** *cpu\_num* ] ] [ **crypto-cores** ] [ **graphs** ] [ **verbose** ] | **table** } [ | { **grep** *grep\_options* | **more** } ]

**info** [ **card** *card\_num* [ **cpu** *cpu\_num* ] ] [ **crypto-cores** ] [ **graphs** ] [ **verbose** ]

Displays information for an entire card or a specific CPU.

**card** *card\_num*: Specifies the card for which to display associated information. *card\_num* must be a value in the range 1 through 48 on the ASR 5000 or 1 through 20 on the ASR 5500 and must refer to an installed card.

**cpu** *cpu\_num*: Optionally selects a specific CPU on the card of interest to display specific information. *cpu\_num* must be a value in the range 0 through 3 and must refer to an installed CPU.

The output of **show cpu info card n verbose** also includes usage details for individual cores within each CPU.

**crypto-cores** : Optionally, specifies to display the CPU crypto core utilization information.

**graphs**: In addition to textual CPU information display CPU utilization information in graphs.

**verbose**: Output is to display all information available.

**table**

Display, in tabular format, all cards and CPUs.

| { **grep** *grep\_options* | **more** }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines** View CPU statistics to aid in diagnosing service problems for the case of overload conditions.



---

**Important** This command is not supported on all platforms.

---

### Example

The following command displays the CPU information in tabular format for all CPUs on all installed cards:

```
show cpu table
```

The following command displays CPU information for card 8 in verbose mode:

```
show cpu info card 8 verbose
```

The following command displays information for CPU 0 on card 1:

```
show cpu info card 1 cpu 0
```

The following command displays information for crypto core utilization for CPU 0 on card 2:

```
show cpu info card 2 cpu 0 crypto-cores
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show crash

Displays software crash events records and associated dump files (minicore, NPU or kernel) for all crashes or a specified crash event.

### Product

All

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

**show crash**

**all | list | number *crash\_num***

**all**: Displays the dump files for all crash event records in the crash log.

**list**: Displays a list of recent crash event records. this is the contents of the crashlog2 file.

**number *crash\_num*** displays the dump file for an existing crash number. The crash number can be displayed using the **list** keyword.

**{ *grep grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

View the crash list to determine frequency of crashes or if crashes occur at some specific time of day. To aid in troubleshooting, this command may also be used to view the dump file for a specific crash.

For additional information refer to the *System Logs* section of the *System Administration Guide*.

**Example**

The following displays the list of crash event records on the active management card.

```
show crash list
```

The following command will display the dump file for crash number 11.

```
show crash number 11
```

## show credit-control sessions

Displays credit control sessions information.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show credit-control session [ all | callid | full | mdn | nai | summary ] [ | { grep grep_options | more } ]
```

```
session [ all | callid | full | mdn | nai | summary ]
```

Displays the credit control session status based on the following keywords:

**all:** Displays all available information for Credit Control sessions

**callid:** Displays the Credit Control Session Call ID

**full:** Displays All available information for the associated display or the filter keyword

**mdn:** Displays the Credit Control Message Delivery Notification (MDN) information.

**nai:** Displays the Credit Control NI

**summary:** Displays the summary of Credit Control session information

```
{ { grep grep_options | more } }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

**Usage Guidelines**

Use this command to show active credit control application for service sessions.

**Example**

The following command shows the configured Credit Control application sessions:

```
show credit-control sessions
```

## show credit-control statistics

Displays credit control statistics.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show credit-control statistics cc-service name [ | { grep grep_options | more } ]
```

**cc-service**

Specifies the Credit Control Service.

*name* must be the name of a Credit Control Service, and must be an alphanumeric string of 1 through 63 characters.

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

**Usage Guidelines**

Use this command to show active credit control statistics.

**Example**

The following command shows the configured credit control statistics for a service named *service1*:

```
show credit-control statistics cc-service service1
```

## show crypto blockedlist file

Displays the contents of the blockedlist (access denied) file.

**show crypto group**


---

**Product** All products supporting IPSec blockedlist

---

**Privilege** Security Administrator

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** In releases prior to StarOS 21.26:

```
show crypto blacklist file
```

From StarOS 21.26 and later releases:

```
show crypto blockedlist file
```

---

**Usage Guidelines** Use this command to display the current contents of the blockedlist file.

### Example

In releases prior to StarOS 21.26:

The following command displays the contents of the blacklist file:

```
show crypto blacklist file
```

## show crypto group

Displays information pertaining to configured crypto groups.




---

**Important**

HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

---



---

**Product** ePDG  
FA  
GGSN  
HA  
HeNBGW  
HNBGW  
HSGW  
MME  
P-GW  
PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show crypto group** [ **name** *group\_name* | **summary** ]

**name** *group\_name*

Displays information for an existing crypto group specified as an alphanumeric string of 1 through 127 characters.

**summary**

Displays state and statistical information for configured crypto groups in this context.

---

**Usage Guidelines** Use this command to display information and statistics pertaining to one or all configured crypto groups within the current context.

If the **summary** keyword is not used, detailed information is displayed.

### Example

The following command displays detailed information for a crypto group called *group1*:

```
show crypto group name group1
```

## show crypto ikev1

Displays pre-shared key information for peer security gateways configured within the context.




---

**Important**

HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

---



---

**Product** ePDG

FA

GGSN  
 HA  
 HeNBGW  
 HNBGW  
 HSGW  
 MME  
 P-GW  
 PDSN  
 S-GW  
 SAEGW  
 SCM  
 SecGW  
 SGSN

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show crypto ikev1 { keys | policy [ *preference* ] | security-associations [ summary ] }**

**keys**

Displays the IKE pre-shared key information based on the peer security gateway.

**policy [ *preference* ]**

Displays configuration information for the Internet Exchange Key (IKE) policy priority specified as an integer from 1 through 100. If no preference is specified, information will be displayed for all configured policies.

**security-associations [ summary ]**

Displays information for established IPsec security associations (SAs).

---

**Usage Guidelines** Use this command to:

- Display pre-shared key information. This information can be used to verify configuration and/or for troubleshooting.
- Verify the configuration of IKE policies within the context.
- Display established IPsec SA information. This information can be used for troubleshooting.



**Example**

The following command lists the pre-shared keys received from peer security gateways as part of the Diffie-Hellman exchange:

```
show crypto ikev1 keys
```

The following command displays information for an IKE policy with a preference of *I*:

```
show crypto ikev1 policy 1
```

The following command displays the currently established SAs:

```
show crypto ikev1 security-associations summary
```

## show crypto ikev2-ikesa security-associations

Displays a summary view of Internet Key Exchange v2 (IKEv2) IKE Security Associations (IKE SAs).

**Important**

HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

**Product**

ePDG  
FA  
GGSN  
HA  
HeNBGW  
HNBGW  
HSGW  
MME  
P-GW  
PDSN  
S-GW  
SAEGW  
SCM  
SecGW  
SGSN

**Privilege**

Administrator, Security Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show crypto ikev2-ikesa security-associations peer ipv4/v6_address [ | { grep
grep_options | more } ]
show crypto ikev2-ikesa security-associations summary [ cookies ] [
distribution ] | [ dpd ] [ ipsecmgr instance instance_value ] [ natt [
remote-gw ipv4/v6_address ] [ spi ] [ | { grep grep_options | more } ]
show crypto ikev2-ikesa security-associations tag crypto_map [ | { grep
grep_options | more } ]
```

#### peer ipv4/v6\_address

Specifies the crypto map peer IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

#### summary

Displays SA summary information only.

This information can be one of the following:

- **cookies**: Display IKE cookies for connections.



**Input** The **cookies** keyword has been deprecated for release 17.0 and above.

- **distribution**: Display summary distribution.
- **dpd**: Display DPD (Dead Peer Detection) information for connections.
- **ipsecmgr instance instance\_value**: Display ipsecmgr instance information. *instance\_value* is an integer from 177 through 352.
- **natt [ remote-gw ipv4/v6\_address ]**: Display NAT-T information for connections or a specified remote gateway.
- **spi**: Display IKE Security Parameter Index.

#### tag tag\_name

Specifies a crypto map name as an alphanumeric string of 1 through 127 characters.

#### | { grep grep\_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

### Usage Guidelines

Shows the information of the of the SAs configured for a crypto template. It shows the total configured SA lifetime in seconds and the number of seconds left on the timer.

**Example**

Use this command to display the SA summary:

```
show crypto ikev2-ikesa security-associations summary
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show crypto ikev2-ikesa transform-set

Displays IKEv2/IKESA (Internet Key Exchange v2/IKE Security Association) transform set configuration information.

**Important**

HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

**Product**

ePDG  
FA  
GGSN  
HA  
HeNBGW  
HNBGW  
HSGW  
MME  
P-GW  
PDSN  
S-GW  
SAEGW  
SCM  
SecGW  
SGSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show crypto ikev2-ikesa transform-set transform_set_name [ | { grep grep_options
| more }
```

**show crypto ikev2-ikesa transform-set *transform\_set\_name***

Specifies the name of an existing IKEv2/IKSA transform set for which to display information as an alphanumeric string of 1 through 127 characters that is case sensitive.

**{ *grep grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

**Usage Guidelines**

Use this command to verify the configuration of IKEv2/IKESA transform sets within the context.

If no keyword is specified, information will be displayed for all IKEv2/IKESA transform sets configured within the context.

**Example**

The following command displays information for an IKEv2/IKESA transform set named *test1*:

```
show crypto ikev2-ikesa transform-set test1
```

## show crypto ipsec security-associations

Displays IPSec security associations (SAs) configured within or facilitated by the context and can optionally display statistics for them.

**Important**

HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

**Product**

ePDG  
FA  
GGSN  
HA  
HeNBGW  
HNBGW  
HSGW

MME  
 P-GW  
 PDSN  
 S-GW  
 SAEGW  
 SCM  
 SecGW  
 SGSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show crypto ipsec security-associations [ map-type { ikev2-ipv4-cfg |
ikev2-ipv4-node | ikev2-ipv6-cfg | ikev2-ipv6-node | ipsec-dynamic |
ipsec-ikev1 | ipsec-ikev2-subscriber | ipsec-l2tp | ipsec-manual |
ipsec-mobile-ip } | summary [ distribution | ipsecmgr | map-type ] | [ | {
grep grep_options | more } ] | [ tag tag_name ] | [ | { grep grep_options | more } ]
```

**map-type { ikev2-ipv4-cfg | ikev2-ipv4-node | ikev2-ipv6-cfg | ikev2-ipv6-node | ipsec-dynamic | ipsec-ikev1 | ipsec-ikev2-subscriber | ipsec-l2tp | ipsec-manual | ipsec-mobile-ip }**

Specifies that information for all crypto maps of a specific type configured within the context will be displayed. The following types can be specified:

- **ikev2-ipv4-cfg**: IKEv2 IPv4 IPsec configured (ACL) Tunnel
- **ikev2-ipv4-node**: IKEv2 IPv4 IPsec spawned node Tunnel
- **ikev2-ipv6-cfg**: IKEv2 IPv6 IPsec configured (ACL) Tunnel
- **ikev2-ipv6-node**: IKEv2 IPv6 IPsec spawned node Tunnel
- **ipsec-dynamic**: Dynamic IPsec Tunnel
- **ipsec-ikev1**: IKEv1 IPsec Tunnel
- **ipsec-ikev2-subscriber**: IKEv2 Subscriber Tunnel
- **ipsec-l2tp**: L2TP IPsec Tunnel
- **ipsec-manual**: Manual (Static) IPsec Tunnel
- **ipsec-mobile-ip**: Mobile IP IPsec Tunnel

**summary [ distribution | ipsecmgr | map-type ]**

Displays only security association summary information.

**distribution:** Show IPsec Manager SA distribution information.

**ipsecmgr** *ipsec\_mgr\_id*: Displays summary SA information for the IPsec manager instance ID specified as an integer from 1 through 200.

**map-type** *map\_type*: Displays summary SA information for the specified type of crypto map. The following types can be specified:

- **ikev2-ipv4-cfg**: IKEv2 IPv4 IPsec configured (ACL) Tunnel
- **ikev2-ipv4-node**: IKEv2 IPv4 IPsec spawned node Tunnel
- **ikev2-ipv6-cfg**: IKEv2 IPv6 IPsec configured (ACL) Tunnel
- **ikev2-ipv6-node**: IKEv2 IPv6 IPsec spawned node Tunnel
- **ipsec-dynamic**: Dynamic IPsec Tunnel
- **ipsec-ikev1**: IKEv1 IPsec Tunnel
- **ipsec-ikev2-subscriber**: IKEv2 Subscriber Tunnel
- **ipsec-l2tp**: L2TP IPsec Tunnel
- **ipsec-manual**: Manual (Static) IPsec Tunnel
- **ipsec-mobile-ip**: Mobile IP IPsec Tunnel

**tag** *tag\_name*

Displays the SAs for an existing crypto map specified as an alphanumeric string of 1 through 127 characters that is case sensitive.

**{ grep** *grep\_options* **| more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

### Usage Guidelines

Use this command to display IPsec SA information and statistics. This information can be used for performance monitoring and/or troubleshooting.

The displayed information categorizes control signal and data statistics. Data statistics are further categorized according to the encapsulation method, either GRE or IP-in-IP.

### Example

The following command displays summary SA statistics for all IPsec managers.

```
show crypto ipsec security-associations summary
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

# show crypto ipsec transform-set

Displays IPsec transform set configuration information.



## Important

HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

## Product

ePDG  
FA  
GGSN  
HA  
HeNBGW  
HNBGW  
HSGW  
MME  
P-GW  
PDSN  
S-GW  
SAEGW  
SCM  
SecGW  
SGSN

## Privilege

Security Administrator, Administrator, Operator, Inspector

## Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

## Syntax Description

**show crypto ipsec transform-set** [ *transform\_name* ]

### ***transform\_name***

Displays information for the IPsec transform set specified as an alphanumeric string of 1 through 127 characters that is case sensitive.

## Usage Guidelines

Use this command to verify the configuration of IPsec transform sets within the context.

If no keyword is specified, information will be displayed for all IPSec transform sets configured within the context.




---

**Important** This command is supported in PDIF Release 8.3 only.

---

### Example

The following command displays information for an IPSec transform set named *test1*:

```
show crypto ipsec transform-set test1
```

## show crypto isakmp keys

Displays pre-shared key information (Internet Security Association and Key Management Protocol, ISAKMP) for peer security gateways configured within the context.

---

### Product

PDSN  
GGSN

---

### Privilege

Security Administrator, Administrator, Operator, Inspector

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

```
show crypto isakmp keys
```

---

### Usage Guidelines

Use this command to display pre-shared key information based on the peer security gateway. This information can be used to verify configuration and/or for troubleshooting.

### Example

The following command lists the pre-shared keys received from peer security gateways as part of the Diffie-Hellman exchange:

```
show crypto isakmp keys
```




---

**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

---



## show crypto isakmp policy

Displays Internet Security Association and Key Management Protocol (ISAKMP) policy configuration information.

---

**Product**

PDSN  
GGSN

---

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
show crypto isakmp policy [ preference ]
```

***preference***

Displays configuration information for the ISAKMP policy priority specified as an integer from 1 through 100.

---

**Usage Guidelines**

Use this command to verify the configuration of ISAKMP policies within the context.

If no *preference* is specified, information will be displayed for all configured policies.

**Example**

The following command displays information for an ISAKMP policy with a preference of 1:

```
show crypto isakmp policy 1
```

## show crypto isakmp security-associations

Displays currently established Internet key Exchange (IKE) security associations (SAs) facilitated by the context.

---

**Product**

PDSN  
GGSN

---

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
show crypto isakmp security-associations [ cookies ]
```

**cookies**

Specifies that cookies should be displayed.

**Usage Guidelines**

Use this command to display established IPsec SA information. This information can be used for troubleshooting.

**Example**

The following command displays the currently established SAs:

```
show crypto isakmp security-associations
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show crypto managers

Displays statistics per IPsec Manager.

**Important**

HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

**Product**

ePDG  
FA  
GGSN  
HA  
HeNBGW  
HNBGW  
HSGW  
MME  
P-GW  
PDSN  
S-GW  
SAEGW  
SCM  
SecGW  
SGSN

<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<p><b>show crypto managers</b> [ <b>context</b> <i>context_name</i>   <b>crypto-map</b> <i>map_name</i>   <b>instance</b> <i>instance_num</i>   <b>summary</b> [ <b>distribution</b>   <b>ike-stats</b>   <b>ikev2-stats</b>   <b>ipsec-sa-stats</b>   <b>npu-stats</b> ]     { <b>grep</b> <i>grep_options</i>   <b>more</b> } ]</p> <p><b>context</b> <i>context_id</i></p> <p>Displays IPsec manager statistics for an existing context specified as an alphanumeric string of 1 through 80 characters.</p> <p><b>crypto-map</b> <i>map_name</i></p> <p>Displays IPsec Managers for an existing crypto map specified as an alphanumeric string of 1 through 128 characters.</p> <p><b>instance</b> <i>instance_num</i></p> <p>Displays statistics for the IPsec manager instance specified as an integer from 1 through 366.</p> <p><b>summary</b> [ <b>distribution</b>   <b>ike-stats</b>   <b>ikev2-stats</b> [ <b>demux-stats</b> ]   <b>ipsec-sa-stats</b>   <b>npu-stats</b> ]</p> <p>Shows statistics per service IP address for each manager.</p> <p><b>distribution</b>: Displays a summary list of IPsec manager distribution.</p> <p><b>ike-stats</b>: Displays a summary list of IPsec IKE statistics. for each IPsec manager.</p> <p><b>ikev2-stats</b>: Displays IKEv2 Statistics on each IPsec Manager.</p> <ul style="list-style-type: none"> <li>• <b>demux-stats</b>: Displays session demux statistics on each IPsec Manager.</li> </ul> <p><b>ipsec-sa-stats</b>: Displays a summary list of IPsec Security Association (SA) statistics for each IPsec Manager.</p> <p><b>npu-stats</b>: Displays NPU statistics on each IPsec Manager.</p> <p>{ <b>grep</b> <i>grep_options</i>   <b>more</b> }</p> <p>Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.</p> <p>Refer to <i>Regulating a Command's Output</i> section of the <i>Command Line Interface Overview</i> chapter for details on the usage of <b>grep</b> and <b>more</b>.</p>

**Usage Guidelines** Use this command to view statistics relating to IPsec managers.

### Example

The following command displays summary information for all IPsec managers:

```
show crypto managers summary
```



**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show crypto map

Displays crypto map configuration information.



**Important** HNDBGW is not supported from Release 20 and later, and HeNDBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNDBGW and HeNDBGW in these releases. For more information, contact your Cisco account representative.

### Product

ePDG  
FA  
GGSN  
HA  
HeNDBGW  
HNDBGW  
HSGW  
MME  
P-GW  
PDSN  
S-GW  
SAEGW  
SCM  
SecGW  
SGSN

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show crypto map [ map-type [ ikev2-ipv4-cfg | ikev2-ipv4-node |
ikev2-ipv6-cfg | ikev2-ipv6-node | ipsec-ikev1 | ipsec-ikev2-subscriber |
ipsec-l2tp | ipsec-manual | ipsec-mobile-ip | [ { grep grep_options | more } ]
| [ summary ] | [ tag tag_name ] | [ [ { grep grep_options | more } ] ]
```

**map-type [ ikev2-ipv4-cfg | ikev2-ipv4-node | ikev2-ipv6-cfg | ikev2-ipv6-node | ipsec-ikev1 | ipsec-l2tp | ipsec-manual | ipsec-mobile-ip | [ { grep *grep\_options* | more } ] ]**

Specifies that information for all crypto maps of a specific type configured within the context will be displayed. The following types can be specified:

- **ikev2-ipv4-cfg**: IKEv2 IPv4 IPsec configured (ACL) Tunnel
- **ikev2-ipv4-node**: IKEv2 IPv4 IPsec spawned node Tunnel
- **ikev2-ipv6-cfg**: IKEv2 IPv6 IPsec configured (ACL) Tunnel
- **ikev2-ipv6-node**: IKEv2 IPv6 IPsec spawned node Tunnel
- **ipsec-ikev1**: IKEv1 IPsec Tunnel
- **ipsec-ikev2-subscriber**: IKEv2 Subscriber Tunnel
- **ipsec-l2tp**: L2TP IPsec Tunnel
- **ipsec-manual**: Manual (Static) IPsec Tunnel
- **ipsec-mobile-ip**: Mobile IP IPsec Tunnel

### summary

Displays summary information for all crypto maps configured in the context.

### tag *map\_name*

Specifies the name of an existing crypto map in the current context for which to display configuration information as an alphanumeric string of 1 through 127 characters that is case sensitive.

### [ { grep *grep\_options* | more } ]

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

### Usage Guidelines

Use this command to verify the configuration of crypto maps within the context.

If no keyword is specified, information will be displayed for all maps configured within the context regardless of type.

### Example

The following command displays configuration information for a dynamic crypto map named *test\_map3*:

```
show crypto map tag test_map3
```

# show crypto statistics

Displays Internet Protocol Security (IPSec) statistics.



## Important

HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

## Product

ePDG  
FA  
GGSN  
HA  
HeNBGW  
HNBGW  
HSGW  
MME  
P-GW  
PDSN  
S-GW  
SAEGW  
SCM  
SecGW  
SGSN

## Privilege

Security Administrator, Administrator, Operator, Inspector

## Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

## Syntax Description

```
show crypto statistics [ ikev1 | ikev2 [ service-ip-address ip-address ] [ service-name name ] ] [ [ | { grep grep_options | more ] ]
```

### ikev1

Displays global ikev1 statistics for this context.

```
ikev2 [ service-ip-address ip-address ] [ service-name name ]
```

Displays global ikev2 statistics for this context.

**service-ip-address** *ip-address*: Specifies the Packet Data Interworking Function (PDIF) service IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**service-name** *name*: Specified PDIF service name, a string of size 1 through 63.

[ { **grep** *grep\_options* | **more** ]

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

### Usage Guidelines

Use this command to display statistics for IPsec tunnels facilitated by the context. This information can be used for performance monitoring and/or troubleshooting.

### Example

The following command displays cumulative IPsec statistics for the current context:

```
show crypto statistics
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show crypto template

Displays information about crypto templates.



### Important

HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

### Product

ePDG  
FA  
GGSN  
HA  
HeNBGW  
HNBGW  
HSGW  
MME  
P-GW  
PDSN

S-GW  
 SAEGW  
 SCM  
 SecGW  
 SGSN

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show crypto template** [ **map-type** [ **ikev2-dynamic** | **ipsec-dynamic** ] | **summary**  
 | **tag** *map\_name* ] [ | { **grep** *grep\_options* | **more**

**map-type** [ **ikev2-dynamic** | **ipsec-dynamic**

Specifies a specific map type.

**summary**

Displays summary information for all templates.

**tag** *map\_name*

Specifies a crypto map name as an alphanumeric string of 1 through 127 characters.

| { **grep** *grep\_options* | **more** ]

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

---

**Usage Guidelines** Use this command to display statistics for crypto templates. This information can be used for performance monitoring and/or troubleshooting.

**Example**

The following command displays summary information for all crypto templates:

```
show crypto template summary
```

## show crypto vendor-policy

Displays information about crypto vendor policy.



**Product**

ePDG  
 FA  
 GGSN  
 HA  
 HeNBGW  
 HSGW  
 MME  
 P-GW  
 PDSN  
 S-GW  
 SAEGW  
 SCM  
 SecGW  
 SGSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show crypto vendor-policy [ name vendor_policy_name | summary ] [ | grep
grep_options | more ]
```

**name *vendor\_policy\_name***

Displays information on the specified vendor policy.

*vendor\_policy\_name* must be an alphanumeric string from 1 to 127 characters.

**summary**

Displays summary information for all vendor policies.

**[ { **grep** *grep\_options* | **more** ]**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

**Usage Guidelines**

Use this command to display statistics for crypto templates. This information can be used for performance monitoring and/or troubleshooting.

**Example**

The following command displays summary information for all crypto vendor policies:

```
show crypto vendor-policy summary
```

## show crypto permitlist file

Displays the contents of the permitlist (access granted) file.

---

**Product**

All products supporting IPSec permitlisting




---

**Important**

This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

---



---

**Privilege**

Security Administrator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

In releases prior to StarOS 21.26:

```
show crypto blacklist file
```

From StarOS 21.26 and later releases:

```
show crypto blockedlist file
```

---

**Usage Guidelines**

Use this command to display the current contents of the permitlist file.

**Example**

In releases prior to StarOS 21.26:

The following command displays the contents of the whitelist file:

```
show crypto whitelist file
```

## show cs-network




---

**Important**

In Release 20 and later, HN BGW is not supported. This command must not be used for HN BGW in Release 20 and later. For more information, contact your Cisco account representative.

---

Displays statistics for the Circuit Switched (CS)-network(s) instance configured on a chassis for HNB-GW service sessions.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show cs-network { all | name cs_name } [ status ] [ | { grep grep_options | more } ]
```

**all**

Displays status counters for all CS (circuit switched) networks configured for HNB-GW service sessions on a chassis.

**name *cs\_name***

Displays status counters for a CS network configured for HNB-GW service specified as an alphanumeric string of 1 through 127 characters that is case sensitive

**{ **grep** *grep\_options* | **more** }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

**Usage Guidelines**

Use this command to display the status of any or all CS-network(s) instance configured on a chassis for HNB-GW service sessions.

**Example**

The following command displays the output for CS network instance status named *cs\_1\_hnb*:

```
show cs-network name cs_1_hnb status
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

# show cs-network counters



## Important

In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Displays the session counter information for an HNB-CS Network associated with Home-NodeB Gateway (HNB-GW) services configured and running on a system.

## Product

HNB-GW

## Privilege

Inspector

## Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

## Syntax Description

```
show cs-network counters [ name cs_svc_name [ msc msc_point_code ] ] [ | { grep grep_options | more } ]
```

### **name** *cs\_svc\_name*

Filters the counter display based on an existing HNB-CS Network service name associated with an HNB-GW service running on system. *cs\_svc\_name* is an alphanumeric string of 1 through 63 characters.

### **msc** *msc\_point\_code*

Filters the counter display filtered on the basis of MSC address provided in the SS7 point code that is connected to a particular HNB-CS Network service. *msc\_point\_code* must be the address of an MSC in SS7 point code notation.

### | { **grep** *grep\_options* | **more** }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *Command Line Interface Overview* chapter.

## Usage Guidelines

Use this command to view the session counter information for HNB-CS Network services configured and MSCs connected on a system.

## Example

The following command displays the counters for the HNB-CS Network service named *hnb\_cs\_svc1*:

```
show cs-network counters name hnb_cs_svc1
```



**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show cs-network statistics



**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Displays the Circuit Switched session statistics for Home-NodeB Gateway (HNB-GW) services configured and running on this system.

**Product** HNB-GW

**Privilege** Inspector

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **show cs-network statistics** [ **name** *cs\_svc\_name* [ **msc** *msc\_point\_code*]] [ **ranap-only** | **rtp-only** | **sccp-only** ] [ [ | { **grep** *grep\_options* | **more** } ]

### **name** *cs\_svc\_name*

Filters the session statistics display based on an existing HNB-CS Network service name that is associated with an HNB-GW service running on this system. *cs\_svc\_name* is an alphanumeric string of 1 through 63 characters.

### **msc** *msc\_point\_code*

Filters the counter display filtered on the basis of MSC address provided in the SS7 point code that is connected to a particular HNB-CS Network service. *msc\_point\_code* must be the address of an MSC in SS7 point code notation.

### **ranap-only**

Filters the session statistics to display only Radio Access Network Application Protocol (RANAP) traffic for an HNB-CS Network service which is configured and associated with an HNB-GW service running on this system.

### **rtp-only**

Filters the session statistics to display only Realtime Streaming Protocol (RTP) and Realtime Streaming Control Protocol (RTCP) traffic for the specified HNB-CS Network service which is configured and associated with an HNB-GW service running on this system.

**sccp-only**

Filters the session statistics to display only Signaling Connection Control Part (SCCP) traffic for the specified HNB-CS Network service which is configured and associated with an HNB-GW service running on this system.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *Command Line Interface Overview* chapter of the *Command Line Interface Reference*.

**Usage Guidelines**

Use this command to view the session statistics for overall session or in selected part of user session for HNB-GW services configured and running on this system.

**Example**

The following command displays the session statistics for RTP and RTCP part of session for the HNB-CS Network service named *hnb\_cs1*:

```
show css-network statistics name hnbcs1 rtp-only
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show css delivery-sequence

In StarOS 9.0 and later releases, this command is deprecated.

## show css server

In StarOS 9.0 and later releases, this command is deprecated.

## show css service

In StarOS 9.0 and later releases, this command is deprecated.



## CHAPTER 20

# Exec Mode show Commands (D-G)

The Exec Mode is the initial entry point into the command line interface system. Exec mode **show** commands are useful in troubleshooting and basic system monitoring.

### Command Modes

This section includes the commands **show dhcp** through **show gtpu-service**.

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```



### Important

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

- [show dhcp](#), on page 794
- [show dhcp-service](#), on page 797
- [show dhcpv6](#), on page 798
- [show dhcpv6-client-profile](#), on page 800
- [show dhcpv6-server-profile](#), on page 801
- [show dhcpv6-service](#), on page 802
- [show diameter-hdd-module](#), on page 803
- [show diameter aaa-statistics](#), on page 804
- [show diameter accounting servers aaa-group](#), on page 805
- [show diameter authentication servers aaa-group](#), on page 805
- [show diameter dynamic-dictionary](#), on page 806
- [show diameter endpoint](#), on page 807
- [show diameter endpoints](#), on page 807
- [show diameter message-queue](#), on page 808
- [show diameter peers](#), on page 810
- [show diameter proclet-map-memcache](#), on page 811
- [show diameter proclet-map-table](#), on page 812
- [show diameter route status](#), on page 813
- [show diameter route table](#), on page 814
- [show diameter statistics](#), on page 815
- [show diameter-service](#), on page 816

- [show diameter tps-statistics](#), on page 817
- [show dns-client](#), on page 819
- [show dynamic-policy statistics](#), on page 820
- [show egtpc peers](#), on page 821
- [show egtpc sessions](#), on page 823
- [show egtpc statistics](#), on page 825
- [show egtpc-service](#), on page 828
- [show emps-profile](#), on page 829
- [show epdg-service](#), on page 829
- [show event-record](#), on page 832
- [show external-inline-servers](#), on page 832
- [show fa-service](#), on page 832
- [show fa-spi-list](#), on page 833
- [show fans](#), on page 834
- [show file](#), on page 835
- [show fng-service](#), on page 836
- [show fng-service session](#), on page 838
- [show fng-service statistics](#), on page 839
- [show freeze-ptmsi imsi](#), on page 840
- [show ggsn sessmgr](#), on page 841
- [show ggsn-service](#), on page 841
- [show ggsn-service sgsn-table](#), on page 842
- [show global-title-translation](#), on page 843
- [show gmb statistics](#), on page 844
- [show gmm-sm statistics](#), on page 844
- [show gprsns statistics](#), on page 847
- [show gprsns status](#), on page 848
- [show gprs-service](#), on page 849
- [show gprssf](#), on page 850
- [show gs-service](#), on page 852
- [show gtpc](#), on page 853
- [show gtpc statistics](#), on page 854
- [show gtp](#), on page 856
- [show gtp accounting](#), on page 857
- [show gtp counters](#), on page 858
- [show gtp group](#), on page 859
- [show gtp statistics](#), on page 860
- [show gtp storage-server](#), on page 862
- [show gtpu](#) , on page 863
- [show gtpu-service](#), on page 865

## show dhcp

Displays counter information pertaining to Dynamic Host Configuration Protocol IPv4 (DHCP) functionality based on specific criteria.



**Product**

GGSN  
 ASN-GW  
 P-GW  
 SAEGW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show dhcp [ counters | full | summary ] [ all | apn apn_name | callid id | chaddr mac_address | dhcp-service svc_name | imsi imsi | msid msid | server server_address | statistics [ dhcp-service svc_name | server server_address ] | status [ dhcp-service svc_name | server server_address ] | user-address address | username name ] [ wfl ] [ | { grep grep_options | more } ]
```

**counters**

Displays DHCP counter information.

**full**

Displays all available information pertaining to the criteria specified.

**summary**

Displays a summary of the DHCP statistics.

**all**

Displays counter information for each active PDP context.

**apn *apn\_name***

Displays information based on an existing Access Point Name (APN) specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**callid *id***

Displays information for an existing call identification number specified as a 4-digit hexadecimal number.

**chaddr *mac\_address***

Displays information for a mobile node specified by its MAC address.

**dhcp-service *svc\_name***

Displays information for an existing DHCP service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**imsi *imsi***

Displays information for an International Mobile Subscriber Identity (IMSI) specified as a string of 1 to 15 digits.

**msid *msid***

Displays information for a Mobile Subscriber Identity (MSID) specified as a string of 1 to 15 digits.

**server *server\_address***

Displays information for a DHCP server specified by its IP address in IPv4 dotted-decimal notation.

**statistics [ *dhcp-service svc\_name* | *server server\_address* ]**

Displays DHCP statistics for either a specific or for all DHCP services and servers configured.

**dhcp-service *svc\_name***: Displays statistics for a DHCP service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**server *server\_address***: Displays statistics for a DHCP server specified by its IP address in IPv4 dotted-decimal notation.

**status [ *dhcp-service svc\_name* | *server server\_address* ]**

Displays configuration information for either a specific or for all DHCP services and servers configured.

**dhcp-service *svc\_name***: Displays statistics for a DHCP service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**server *server\_address***: Displays statistics for a DHCP server specified by its IP address in IPv4 dotted-decimal notation.

**user-address *address***

Displays information for a DHCP-assigned user IP address specified in IPv4 dotted-decimal notation.

**username *name***

Displays information for a subscriber specified as an alphanumeric string of 1 through 127 characters (including wildcards "\$" and "\*") that is case sensitive.

**wf1**

Displays all available information for associated filter keyword in wide-format number 1.

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage Guidelines**

Counters pertaining to DHCP functionality can be displayed as cumulative values or for specific APNs, PDP contexts, servers, or DHCP services.

**Example**

The following command displays DHCP counter information for a DHCP service called *DHCP-Gi*:

```
show dhcp dhcp-service DHCP-Gi
```

The following command displays DHCP counter information for a DHCP Call ID *01calla2*:

```
show dhcp call-id DHCP-Gi
```

The following command displays DHCP information for the specified mobile node:

```
show dhcp chaddr 00:05:47:00:37:44
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show dhcp-service

Displays information for either a specific or for all Dynamic Host Configuration Protocol IPv4 (DHCP) services.

**Product**

GGSN  
ASN-GW  
P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show dhcp-service { all | name svc_name } [ | { grep grep_options | more } ]
```

**all**

Displays information for all configured DHCP services.

**name *svc\_name***

Displays information for a DHCP service name specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

### Usage Guidelines

This command is used to verify the configuration of one or all DHCP services for monitoring or troubleshooting purposes. The output is a concise listing of DHCP service parameter settings.

If this command is executed from within the local context with the **all** keyword, information for all DHCP services configured on the system will be displayed.

### Example

The following command displays configuration information for a DHCP service called *dhcp1*:

```
show dhcp-service name dhcp1
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show dhcpv6

Displays counter information pertaining to Dynamic Host Configuration Protocol IPv6 (DHCPv6) functionality based on specific criteria.

### Product

GGSN  
ASN-GW  
P-GW  
SAEGW

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show dhcpv6 [ counters | full | summary ] [ all | callid id | server
server_address | service svc_name | statistics [ dhcp-service svc_name | server
server_address ] | status [ dhcp-service svc_name | server server_address ] [ |
{ grep grep_options | more } ]
```

#### counters

Displays DHCPv6 counter information.

#### full

Displays all available information pertaining to the criteria specified.

**summary**

Displays a summary of the DHCPv6 statistics.

**all**

Displays counter information for each active PDP context.

**callid *id***

Displays information for an existing call identification number specified as an 8-digit hexadecimal number.

**server *server\_address***

Displays information for a DHCPv6 server specified by its IP address in IPv6 colon-separated-hexadecimal notation.

**Important**


---

In StarOS 15.0 and later releases, this option is deprecated

---

**statistics [ *dhcp-service svc\_name* ]**

Displays DHCPv6 statistics for either a specific or for all DHCPv6 services.

**dhcp-service *svc\_name***: Displays statistics for a DHCPv6 service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**server *server\_address***: Displays statistics for a DHCPv6 server specified by its IP address in IPv6 colon-separated-hexadecimal notation.

**Important**


---

In StarOS 15.0 and later releases, this option is deprecated

---

**status [ *dhcp-service svc\_name* ]**

Displays configuration information for either a specific or for all DHCPv6 services and servers configured.

**dhcp-service *svc\_name***: Displays statistics for a DHCPv6 service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**server *server\_address***: Displays statistics for a DHCPv6 server specified by its IP address in IPv6 colon-separated-hexadecimal notation.

**Important**


---

In StarOS 15.0 and later releases, this option is deprecated

---

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

### Usage Guidelines

Counters pertaining to DHCP IPv6 functionality can be displayed as cumulative values or for specific APNs, PDP contexts or DHCPv6 services.

### Example

The following command displays DHCPv6 status information for a DHCPv6 service called *DHCPv6-Gi*:

```
show dhcpv6 status service DHCPv6-Gi
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show dhcpv6-client-profile

Displays configuration information for a specific or all Dynamic Host Configuration Protocol IPv6 (DHCPv6) client profiles.

### Product

GGSN  
ASN-GW  
P-GW  
SAEGW

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show dhcpv6-client-profile [ all | name profile_name ] | { grep grep_options  
| more }
```

#### all

Displays configuration information for all DHCPv6 client profiles.

#### name profile\_name

Displays profile configuration information for an existing DHCPv6 client profile specified as an alphanumeric string of 1 through 63 characters.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

### Usage Guidelines

Use this command to display configuration information for one or all DHCPv6 client profiles.

### Example

The following command displays all DHCPv6 client profiles:

```
show dhcpv6-client-profile all
```

## show dhcpv6-server-profile

Displays configuration information for a specific or all Dynamic Host Configuration Protocol IPv6 (DHCPv6) server profiles.

### Product

GGSN  
ASN-GW  
P-GW  
SAEGW

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show dhcpv6-server-profile [ all | name profile_name ] | { grep grep_options | more }
```

#### all

Displays configuration information for all DHCPv6 server profiles.

#### name *profile\_name*

Displays profile configuration information for an existing DHCPv6 server profile specified as an alphanumeric string of 1 through 63 characters.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

### Usage Guidelines

Use this command to display configuration information for one or all DHCPv6 server profiles.

### Example

The following command displays all DHCPv6 server profiles:

```
show dhcpv6-server-profile all
```

## show dhcpv6-service

Displays service information and configuration counters for a specific or all Dynamic Host Configuration Protocol IPv6 (DHCPv6) services.

### Product

GGSN  
ASN-GW  
P-GW  
SAEGW

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show dhcpv6-service [ all | name svc_name ] | { grep grep_options | more }
```

#### all

Displays configuration information and counters for all DHCPv6 services.

#### name *svc\_name*

Displays configuration information and counters for an existing DHCPv6 service specified as an alphanumeric string of 1 through 63 characters.

#### | { grep *grep\_options* | more }

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

### Usage Guidelines

Use this command to display configuration information and counters for one or all DHCPv6 services.



**Example**

The following command displays all DHCPv6 services:

```
show dhcpv6-service all
```

# show diameter-hdd-module

Displays the HDD module configuration information.

**Important**

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

**Product**

HA  
P-GW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show diameter-hdd-module { file-space-usage | statistics } [ | { grep
grep_options | more } ] ]
```

**file-space-usage**

Displays the limit and usage of hard-disk space for the credit-control-event module.

**statistics**

Displays statistics for the credit-control-event module.

**{ { grep grep\_options | more } }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage Guidelines**

Use this command to view the HDD module configuration information.

**Example**

The following command displays the hard-disk space utilization for the credit-control-event module:

```
show diameter-hdd-module file-space-usage
```

# show diameter aaa-statistics

Displays Diameter Authentication, Authorization and Accounting (AAA) statistics.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
show diameter aaa-statistics [ all | group group_name [ server server_name ]
| misc-data [ instance instance_number ] | server server_name ] [ | { grep
grep_options | more } ]
```

**all**

Displays all available Diameter server statistics.

**group *group\_name* [ server *server\_name* ]**

Displays all Diameter server statistics within an existing AAA group specified as an alphanumeric string of 1 through 64 characters.

*server\_name* must be the name of a Diameter server, expressed as an alphanumeric string of 1 through 64 characters.

**misc-data instance *instance\_number***

Displays Diameter specific miscellaneous statistics among all AAA manager instances. This display also includes the maximum backpressure statistics and the time at which it was seen.

**instance *instance\_number***: Displays the maximum backpressure statistics at a specified AAA manager instance. The instance number must be an integer from 1 through 385 characters.

**server *server\_name***

Displays Diameter server statistics for the Diameter server name specified as an alphanumeric string of 1 through 64 characters.

**{ **grep** *grep\_options* | **more** }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

---

**Usage Guidelines**

Use this command to view Diameter AAA statistics.

**Example**

The following command displays all available Diameter server statistics:

```
show diameter aaa-statistics all
```

## show diameter accounting servers aaa-group

Displays Diameter accounting server information for an Authentication, Authorization and Accounting (AAA) group.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show diameter accounting servers [ aaa-group group_name ] [ | { grep
grep_options | more } ]
```

**aaa-group group\_name**

Specifies the name of an existing AAA group as an alphanumeric string of 0 through 64 characters.

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage Guidelines**

Use this command to view Diameter accounting server information for an AAA group.

**Example**

The following command displays Diameter accounting server information for an AAA group named in *group12*:

```
show diameter accounting servers aaa-group group12
```

## show diameter authentication servers aaa-group

Displays Diameter Authentication server information for a specified AAA group.

---

**Product** All

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show diameter authentication servers [ aaa-group *group\_name* ]**

**aaa-group *group\_name***

Specifies the name of an existing AAA group as an alphanumeric string of 0 through 64 characters.

---

**Usage Guidelines** Use this command to view Diameter authentication server information for an AAA group.

### Example

The following command displays Diameter authentication server information for an AAA group named *group12*:

```
show diameter authentication servers aaa-group group12
```

## show diameter dynamic-dictionary

Displays the contents of Diameter dictionary that is loaded dynamically at run time.

---

**Product** All

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show diameter dynamic-dictionary { { all [ contents ] } | { name *dict\_name* [ contents | { full facility { aaamgr | diamproxy | sessmgr instance *instance\_no* } } ] [ | { grep *grep\_options* | more } ] }**

### all

Displays, in text format, the information for all dynamically loaded dictionaries configured in the Global Configuration mode. Displays up to 10KB buffered text from each dictionary file.

### name *dict\_name*

Displays detailed information for an existing dynamically loaded dictionary specified as an alphanumeric string of 1 through 15 characters. Displays up to 10KB buffered text from the specified dictionary file.

**full facility { aaamgr | diamproxy | sessmgr }**

Displays all available information for the specified instance associated with one of the following facilities:

- aaamgr — Accounting and authentication Manager
- diamproxy — Diameter Proxy
- sessmgr — Session Manager

**instance *instance\_no***

Specifies the instance number from which dynamic dictionary details to be fetched, is an integer value between 0 through 4294967295.

**{ *grep grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage Guidelines**

Use this command to view the contents of dynamically loaded Diameter dictionaries.

For more details on the dynamic configuration of Diameter dictionary, refer to the **diameter dynamic-dictionary** command in the *Global Configuration Mode Commands* chapter.

**Example**

The following command displays the contents of dynamically loaded Diameter dictionary file named *dyn1*:

```
show diameter dynamic-dictionary name dyn1
```

## show diameter endpoint

This command has been deprecated, and is replaced by the [show diameter endpoints, on page 807](#) command.

## show diameter endpoints

This command displays the status of Diameter client endpoint(s).

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show diameter endpoints { all | endpoint endpoint_name } [ | { grep grep_options | more } ]`

**all**

Displays status of all Diameter client endpoints.

**endpoint *endpoint\_name***

Displays status of an existing Diameter client endpoint specified as an alphanumeric string of 1 through 63 characters.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage Guidelines**

Use this command to view the status of Diameter client endpoints.

If you are in the local context, then all contexts are searched for the specified endpoint(s). Specify **all** to see all endpoints; otherwise, just the named endpoint will be displayed. If no argument is provided, a summary of all endpoints is displayed.

Default value: N/A

**Example**

The following command displays status of all Diameter client endpoints.

```
show diameter endpoints all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show diameter message-queue

Displays Diameter message queue statistics.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show diameter message-queue counters { inbound | outbound } [ endpoint
endpoint_name [ peer-host peer_id [ peer-realm realm_id ] ] | session-id session_id
] [ | { grep grep_options | more } ]
```

**counters { inbound | outbound }**

Specifies the message counters:

**inbound**: Specifies Diameter inbound messages

**outbound**: Specifies Diameter outbound messages

**endpoint endpoint\_name**

Specifies the Diameter endpoint as an alphanumeric string of 1 through 63 characters.

**peer-host peer\_id**

Specifies the Diameter peer host as an alphanumeric string of 1 through 63 characters.

**peer-realm realm\_id**

Specifies the Diameter peer realm as an alphanumeric string of 1 through 127 characters.

**session-id session\_id**

Specifies the session ID as an alphanumeric string of 1 through 127 characters.

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage Guidelines**

Use this command to view the count of the messages in the Diameter message queue for specific counter type, session ID, or endpoint, peer host, and peer realm.

**Example**

The following command displays message queue statistics for outbound messages specific to the Diameter endpoint named *asr5k.testnetwork.com*:

```
show diameter message-queue counters outbound endpoint
asr5k.testnetwork.com
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

# show diameter peers

Displays Diameter peer information.

---

## Product

All

---

## Privilege

Security Administrator, Administrator, Operator, Inspector

---

## Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

## Syntax Description

```
show diameter peers [ full | summary ] [ all | [ endpoint endpoint_name ] [ peer-host peer_id ] [ peer-realm realm_id ] ] [ | { grep grep_options | more } ]
```

### **full**

Displays full details of all or specified Diameter peers.

### **summary**

Displays summary details of all or specified Diameter peer(s).

### **all**

Displays details of all Diameter peers.

### **endpoint** *endpoint\_name*

Displays details of the origin Diameter endpoint specified as an alphanumeric string of 1 through 255 characters.

### **peer-host** *peer\_id*

Displays details of the Diameter peer host specified as an alphanumeric string of 1 through to 63 characters.

### **peer-realm** *realm\_id*

Displays details of the Diameter peer realm ID specified as an alphanumeric string of 1 through 127 characters.

### | { **grep** *grep\_options* | **more** }

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

---

## Usage Guidelines

Use this command to view the details of Diameter peers.

If you are in the local context, then all contexts are searched for the specified peer(s).



This is similar to the **show subscribers** CLI command and supports multiple filter options specified at the same time.

If filter options are specified (e.g., **all**, **endpoint**, etc.), the default is for one line of output to be displayed per peer. Use **full** to get detailed information per peer, or **summary** to get summarized information about all matching peers.

If no filter options are specified, a summary output for all peers is displayed. Use the **full** option to get detailed information about every peer.

Default value: N/A

### Example

The following command details of the Diameter endpoint named *endpoint12*:

```
show diameter peers endpoint endpoint12
```



#### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show diameter proclt-map-memcache

Displays DIAMPROXY proclt cached memory information for aaamgr, diactrl or sessmgr.

#### Product

All

#### Privilege

Security Administrator, Administrator, Operator, Inspector

#### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

#### Syntax Description

```
show diameter proclt-map-memcache { aaamgr integer | diactrl | sessmgr integer } [ | { grep grep_options | more } ]
```

#### aaamgr integer

Selects memcache information for the aaamgr (AAA manager) instance specified as an integer from 1 to 1152.

#### diactrl

Selects memcache information for the diactrl (Diameter controller).

#### sessmgr integer

Selects memcache information for the sessmgr (Session manager) instance specified as an integer from 1 to 1152.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

### Usage Guidelines

Use this command to selectively display the memcache information for specified Diameter-related StarOS proclats.

### Example

The following command displays the diactrl memcache:

```
show diameter proclat-map-memcache diactrl
```

## show diameter proclat-map-table

Displays DIAMPROXY proclat mapping table information for aaamgr, diactrl or sessmgr.

### Product

All

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show diameter proclat-map-table { aaamgr integer | diactrl | sessmgr integer } [ | { grep grep_options | more } ]
```

#### **aaamgr *integer***

Selects map table information for the aaamgr (AAA manager) instance specified as an integer from 1 to 1152.

#### **diactrl**

Selects map table information for the diactrl (Diameter controller).

#### **sessmgr *integer***

Selects map table information for the sessmgr (Session manager) instance specified as an integer from 1 to 1152.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

### Usage Guidelines

Use this command to selectively display the table information for specified Diameter-related StarOS proclefs.

### Example

The following command displays the diactrl map table information:

```
show diameter proclef-map-table diactrl
```

## show diameter route status

Displays Diameter route health status information.



### Important

In 17.0 and later releases, this command has been deprecated.

### Product

All

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show diameter route status [ endpoint endpoint_name | full [ endpoint
endpoint_name ] ] [ host host_name [ peer peer_id ] ] [ | { grep grep_options |
more } ]
```

### full

Displays information about which Diameter clients are using which peer/host combinations.

### endpoint endpoint\_name

Displays detailed information for the Diameter client endpoint specified as an alphanumeric string of 1 through 63 characters.

### host host\_name

Displays information for the Diameter host specified as an alphanumeric string of 1 through 63 characters.

### peer peer\_id

Displays information for the Diameter peer host specified as an alphanumeric string of 1 through 63 characters.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

### Usage Guidelines

Use this command to view the Diameter route health status.

If you are in the local context, then the route information used by Diameter endpoints in all contexts will be used in the display.

The route status displays status of peer/host combinations. Refer to the **route-failure** CLI command in Diameter Endpoint Configuration mode. When no options are specified, the display will give one line per peer/host combination, indicating how many Diameter clients are using each combination, and for how many clients the combination is available or failed. Specify **full** to see which Diameter clients are using which peer/host combinations. Specify **host** or **peer** to see just combinations with the named host or peer. Specify **endpoint** to see detailed information about the named Diameter client.

Default value: N/A

### Example

The following command displays route health status details of the Diameter client endpoint named *endpoint12*:

```
show diameter route status endpoint endpoint12
```

## show diameter route table

Displays the Diameter routing table.

### Product

All

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show diameter route table [ wide ] [ endpoint endpoint_name ] [ | { grep grep_options | more } ]
```

#### **wide**

Displays the route table information in wide-format.

#### **endpoint** *endpoint\_name*

Displays the Diameter routing table for the Diameter endpoint specified as an alphanumeric string of 1 through 63 characters.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to view the status of Diameter client endpoints.

If you are in the local context, then the route information used by Diameter endpoints in all chassis contexts will be used in the display.

The route table displays all static and dynamic routes. Refer to the route-entry CLI command in Diameter Endpoint Configuration Mode.

Default value: N/A

### Example

The following command displays status of the Diameter client endpoint named *endpoint12*.

```
show diameter route table endpoint endpoint12
```

## show diameter statistics

Displays Diameter peer statistics.

### Product

All

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show diameter statistics [ [ proxy ] endpoint endpoint_name [ peer-host
peer_id [ peer-realm realm_id ] ] [ | { grep grep_options | more } ] ]
```

#### endpoint *endpoint\_name*

Displays statistics for the Diameter endpoint specified as an alphanumeric string of 1 through 63 characters.

#### peer-host *peer\_id*

Displays statistics for the Diameter host peer specified as an alphanumeric string of 1 through 255 characters.

#### peer-realm *realm\_id*

Displays statistics for the Diameter peer realm specified as an alphanumeric string of 1 through 127 characters.

**proxy**

Displays proxy related statistics.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage Guidelines**

Use this command to view Diameter statistics for the specified endpoint or proxy.

**Example**

The following command displays Diameter peer statistics for the endpoint named *endpoint12*:

```
show diameter statistics endpoint endpoint12
```

## show diameter-service

Displays information about configured Diameter services.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show diameter-service { all | lte-s6a trace-id { all | user-name user_name
} | name service_name | statistics name service_name [ vpn-name vpn_context_name
] } [ | { grep grep_options | more } ]
```

**all**

Displays full information for all configured Diameter services.

**lte-s6a trace-id { all | user-name *user\_name* }**

Displays user trace ID information for an LTE/S6a application.

**all**: Displays full information.

**user-name *user\_name***: Displays information for the user specified an alphanumeric string of 1 through 79 characters.

**name *service\_name***

Displays information for the Diameter service name specified as an alphanumeric string of 1 through 79 characters.

**statistics name *service\_name* [ vpn-name *vpn\_context\_name* ]**

Displays statistics for the Diameter service name specified as an alphanumeric string of 1 through 79 characters.

**vpn-name *vpn\_context\_name***: Specifies the name of VPN context as an alphanumeric string of 1 through 79 characters.

**{ *grep grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage Guidelines**

Use this command to view information on configured Diameter services.

**Example**

The following command displays statistics for the Diameter service named *ggsn12*:

```
show diameter-service name ggsn12
```

## show diameter tps-statistics

Displays the Transactions Per Second (TPS) statistics per Diameter application, endpoint and Diameter proxy facility.

**Product**

ePDG  
P-GW  
SAEGW  
S-GW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show diameter tps-statistics [ diamproxy diamproxy_num | application {  
auth-eap | e2 | gmb | gx | gy | rf | s6a | s6b | sgmb | sta | swm } |  
endpoint endpoint_name | summary | verbose ] + [ | { grep grep_options | more  
} ]
```

**diamproxy *diamproxy\_num***

Displays the TPS Key Performance Indicator (KPI) information for the specified Diameter Proxy facility. The *diamproxy\_num* must be an integer from 1 through 144.

**endpoint *endpoint\_name***

Displays the TPS KPI information only for the endpoint specified as a string of size ranging from 1 through 255 characters.

**Important**

The Diameter Endpoints configured on ASR 5000 and ASR 5500 platforms are not shared between various Diameter applications. For example, Gx and Gy should have separate Diameter endpoints configured.

**application { *auth-eap* | *e2* | *gmb* | *gx* | *gy* | *rf* | *s6a* | *s6b* | *sgmb* | *sta* | *swm* }**

Displays the TPS KPI information only for the specified Diameter application.

**summary**

Displays summary information of TPS statistics.

**verbose**

Specifies to display detailed (all available) information. If not specified, concise information is displayed.

**| { *grep grep\_options* | *more* }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display TPS KPI information (the cumulative and the historical statistics) for all Diameter applications, endpoint and Diameter proxy facility.

In releases prior to 20, well-defined Key Performance Indicators (KPIs) were not available for measuring the session and Voice-over-LTE (VoLTE) signaling transaction rates on the gateway platforms. KPIs did not differentiate between successful or unsuccessful PDN session activations and deactivations. In addition, the KPIs did not provide any information related to the VoLTE service.

An external server used to collect bulkstats data every 2 minutes from the gateway node. The bulkstats data such as PDN session activations and deactivations events counters are used to calculate the Call Events Per Second (CEPS) KPI on the external server. The gateway node does not calculate the CEPS; but it only provides the counters to the external server for additional processing of relevant bulkstats data.

To address these issues, CEPS, Session Events Per Second (SEPS), Gx Transactions Per Second (TPS), Gy-TPS, S6b-TPS, Rf-TPS, SWm-TPS KPIs have been implemented. These KPIs measure the signaling load on the gateway, and also the event rate for VoLTE call setup and tear down. This enables operators to perform network dimensioning/planning for the gateway node.

This show CLI command is capable of providing the following for all signaling interfaces:

- CEPS and SEPS KPI values per second, but calculated averaged over 2 minutes



- 8 historical SEPS and CEPS KPI values
- Gx-TPS, Gy-TPS, S6b-TPS, Rf-TPS, and SWm-TPS KPIs per second, but calculated averaged over 1, 10 seconds, 30 seconds, 1 minute, 5 minutes, 10 minutes and 15 minutes

**Important**

TPS is computed based on average of sent and received Diameter messages.

Average values of all KPIs will be provided by the gateway to the external servers using bulkstats data every 2 minutes if requested. The total KPI TPS value as well as breakdown TPS values by each card (i.e., Diameter proxy) on every Diameter interface will be provided using the show CLI command and bulkstats data.

**Example**

The following command displays the summary information of TPS KPI statistics for Gy application:

```
show diameter tps-statistics application gy summary
```

## show dns-client

Displays cache and/or statistics for a specified Domain Name System (DNS) client.

**Product**

ePDG  
SGSN  
HSGW  
MME  
P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show dns-client { cache client name [ query-name name | query-type { A | AAAA | NAPTR | SRV } ] | statistics client name } [ | { grep grep_options | more } ]
```

**cache client *name* [ query-name *name* | query-type { A | AAAA | NAPTR | SRV } ]**

displays statistics for the cache of an existing DNS client specified as an alphanumeric string of 1 through 255 characters.

**query-name *name***: Filters DNS results based on the domain name specified as an alphanumeric string of 1 through 255 characters. *name* is the domain name used to perform the DNS query. It is different from the

actual domain name which is resolved. For example, to resolve the SIP server for *service.com*, the query name is *\_sip.\_udp.service.com* and the query type is **SRV**.

**query-type:**

- **A**: Filters DNS results based on 32-bit domain IPv4 address records (A records).
- **AAAA**: Filters DNS results based on 128-bit domain IPv6 address records (AAAA resource records).
- **NAPTR**: Filters DNS results based on Naming Authority Pointer records.
- **SRV**: Filters DNS results based on service locator records (SRV records).

**statistics client *name***

Displays statistics for an existing DNS client specified as an alphanumeric string of 1 through 255 characters.

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display DNS cache and/or statistics for a specified DNS client.

**Example**

The following command displays statistics for a DNS client named *domain1.com*:

```
show dns-client statistics client domain1.com
```



**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show dynamic-policy statistics

Displays policy control and charging (PCC) statistics from the interface communicating with the Policy and Charging Rules Function (PCRF) via Gx(x).

**Product**

HSGW  
PDSN  
SAEGW  
S-GW

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

**show dynamic-policy statistics { hsgw-service *name* | pdsn-service *name* | sgw-service *name* }**

**hsgw-service *name***

Displays policy control and charging statistics from the Gxa interface communicating with the PCRF. *name* must be an existing HSGW service name and be from 1 to 63 alphanumeric characters.

**pdsn-service *name***

Displays policy control and charging statistics from the Gx interface communicating with the PCRF. *name* must be an existing PDSN service name and be from 1 to 63 alphanumeric characters.

**sgw-service *name***

Displays policy control and charging statistics from the Gxc interface communicating with the PCRF. *name* must be an existing S-GW service name and be from 1 to 63 alphanumeric characters.

---

**Usage Guidelines**

Use this command to display PCC statistics for the specified service and its Gx interface communicating with the PCRF.

**Example**

The following command displays HSGW statistics for an HSGW service named *hsgw4*:

```
show dynamic-policy statistics hsgw-service hsgw4
```

The following command displays PCC statistics for a PDSN service named *cdma4*:

```
show dynamic-policy statistics pdsn-service cdma4
```

The following command displays S-GW statistics for an S-GW service named *sgw4*:

```
show dynamic-policy statistics sgw-service sgw4
```

## show egtpc peers

Displays information about eGTP-C peers.

---

**Product**

ePDG  
MME  
P-GW  
SAEGW  
S-GW

---

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show egtpc peers [ address ip_address | egtp-service name ] | interface {
epdg-egress | mme | pgw-ingress | sgsn | sgw-egress | sgw-ingress |
path-failure-history } [ address ip_address ] [ wf1 ] } [ | { grep
grep_options | more } ]
```

**address** *ip\_address*

Displays information about a eGTP-C peer specified by its IP address in IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.

**egtp-service** *name* [ **address** *ip\_address* ]

Displays information about eGTP-C peers associated with an existing egtp-service name specified as an alphanumeric string of 1 through 63 characters.

**address** *ip\_address*: Additionally, the results can be filtered based on the IP address associated with an existing eGTP-C peer service specified in IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.

**interface** { **epdg-egress** | **mme** | **pgw-ingress** | **sgsn** | **sgw-egress** | **sgw-ingress** } [ **address** *ip\_address* ] [ **wf1** ]

Displays information about eGTP-C peers associated with the service interface configured on this system.

**epdg-egress**: Displays ePDG's egress EGTP interface.

**mme**: Displays information about eGTP-C MME peers associated with the service interface configured on this system. Additionally, the results can be filtered based on the IP address associated with the MME peer.

**pgw-ingress**: Displays information about eGTP-C P-GW ingress peers associated with the service interface configured on this system. Additionally, the results can be filtered based on the IP address associated with the P-GW ingress peer.

**sgsn**: Displays information about eGTP-C SGSN peers associated with the S4 service interface configured on this system. Additionally, the results can be filtered based on the IP address associated with the SGSN peer.

**sgw-egress**: Displays information about eGTP-C S-GW egress peers associated with the service interface configured on this system. Additionally, the results can be filtered based on the IP address associated with the S-GW egress peer.

**sgw-ingress**: Displays information about eGTP-C S-GW ingress peers associated with the service interface configured on this system. Additionally, the results can be filtered based on the IP address associated with the S-GW ingress peer.

**address** *ip\_address*: Specifies the IP address of the selected peer in IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.

**wf1**: Specifies that the output is to be displayed in wide format number 1.

### path-failure-history

Provides detailed information on the last five path failures that occur per configured P-GW peers. This information can assist operators in debugging path failures in the network.

### { `grep` *grep\_options* | `more` }

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on using the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

#### Usage Guidelines

Use this command to display information about eGTP-C peers associated with the service interface configured on this system. The output contains the following information about the peer:

- Status of the peer
- Echo status
- Restart counter status
- Peer restart counter knowledge
- Service ID
- Peer IP address
- Current sessions
- Maximum sessions



#### Important

The primary command, **show egtpc peers**, when entered without additional keywords, displays information for all peers associated with the service operating on this system.

#### Example

The following command returns an output for an eGTP-C S-GW egress peers associated with the service interface configured on this system with an IP address of *10.2.3.4*:

```
show egtpc peers interface sgw-egress address 10.2.3.4
```

The following command returns an output for an eGTP-C MME peer associated with the service interface configured on this system with an IP address of *10.2.3.4*:

```
show egtpc peers interface mme address 10.2.3.4
```

## show egtpc sessions

Displays eGTP-C session information.

#### Product

ePDG

MME  
P-GW  
SAEGW  
S-GW

---

**Privilege** Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show egtpc sessions** [ **egtp-service** *name* | **interface** { **epdg-egress** | **mme** | **pgw-ingress** | **sgsn** | **sgw-egress** | **sgw-ingress** } ] [ | { **grep** *grep\_options* | **more** } ]

**egtp-service *name***

Displays information about eGTP-C sessions associated with an existing egtp-service specified as an alphanumeric string of 1 through 63 characters.

**interface { epdg-egress | mme | pgw-ingress | sgsn | sgw-egress | sgw-ingress }**

Displays information about eGTP-C sessions associated with the service interface configured on this system.

**epdg-egress**: Displays information about ePDG egress associated with EGTP interface.

**mme**: Displays information about eGTP-C sessions associated with the MME interface configured on this system.

**pgw-ingress**: Displays information about eGTP-C sessions associated with the P-GW ingress interface configured on this system.

**sgsn**: Displays information about eGTP-C sessions associated with the SGSN eGTP-C S4 interface configured on this system.

**sgw-egress**: Displays information about eGTP-C sessions associated with the S-GW egress interface configured on this system.

**sgw-ingress**: Displays information about eGTP-C sessions associated with the S-GW ingress interface configured on this system.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on using the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Use this command to display session information for a specific eGTP service or for sessions associated with an interface type configured on this system.

**Example**

The following command displays eGTP-C session information for sessions associated with all P-GW ingress interfaces configured on this system:

```
show egtpc sessions interface pgw-ingress
```

The following command displays eGTP-C session information for sessions associated with all MME interfaces configured on this system:

```
show egtpc sessions interface mme
```

## show egtpc statistics

Displays evolved GPRS Tunneling Protocol Control (eGTP-C) plane statistics for a specific service name or interface type.

**Product**

ePDG  
MME  
P-GW  
SAEGW  
S-GW

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show egtpc statistics [ demux-only | egtp-service name [ interface-type {
  s2a | s2b | s5s8 } ] ] | epdg-address ip_address | event-statistics |
header-decoder-errors | interface { epdg-egress | mme | pgw-ingress [
interface-type { s2a | s2b | s5s8 } ] | sgsn | sgw-egress | sgw-ingress }
| mme-address ip_address | path-failure-reasons | pgw-address ip_address |
piggybacking-statistics | sessmgr-only | sgsn-address ip_address |
sgw-address ip_address ] [ verbose ] [ | { grep grep_options | more } ]
```

**demux-only**

Displays entry point statistics at demux manager.

**egtp-service *name* [ interface-type { s2a | s2b | s5s8 } ]**

Displays statistics for an existing eGTP service specified as an alphanumeric string of 1 through 63 characters.

**interface-type:** Displays the eGTP-C sub-interface statistics only for the specified eGTP-C service. Possible interfaces are:

- **s2a:** Interface type Sa

- **s2b**: Interface type Sb
- **s5s8**: Interface type S5/S8

**Important**

The keywords **s2a** and **s2b** are only visible if WiFi Integration functionality is enabled. WiFi Integration requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

**epdg-address *ip\_address***

Displays eGTP-C statistics for an existing ePDG IP address expressed in IPv6 colon-separated-hexadecimal notation.

**event-statistics**

Displays total eGTP-C events sent/received.

**header-decoder-errors**

Displays header decoding errors of incoming packets at eGTP-C stack/demux manager.

**interface { epdg-egress | mme | pgw-ingress [ interface-type { s2a | s2b | s5s8 } ] | sgw-egress | sgw-ingress }**

**epdg-egress**: Displays eGTP-C statistics for all ePDG egress interfaces.

**mme**: Displays eGTP-C statistics for all MME interfaces.

**pgw-ingress**: Displays eGTP-C statistics for all eGTP P-GW ingress interfaces.

**interface-type**: Displays the eGTP-C interface statistics of a particular sub-interface of P-GW ingress. Possible interfaces are:

- **s2a**: Interface type Sa
- **s2b**: Interface type Sb
- **s5s8**: Interface type S5/S8

**Important**

The keywords **s2a** and **s2b** are only visible if WiFi Integration functionality is enabled. WiFi Integration requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

**sgsn**: Displays eGTP-C statistics for all eGTP S4 SGSN interfaces.

**sgw-egress**: Displays eGTP-C statistics for all eGTP S-GW egress interfaces.

**sgw-ingress**: Displays eGTP-C statistics for all eGTP S-GW ingress interfaces.

**mme-address *ip\_address***

Displays eGTP-C statistics for an existing MME IP address expressed in IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.



**path-failure-reasons**

Displays breakup of reasons for path failure.

**pgw-address *ip\_address***

Displays eGTP-C statistics for an existing P-GW IP address expressed in IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.

**piggybacking-statistics**

Displays total piggybacked messages sent/received at eGTP-C stack.

**sessmgr-only**

Displays entry point statistics at sessmgr.

**sgsn-address *ip\_address***

Displays eGTP-C statistics for an existing SGSN S4 IP address expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**sgw-address *ip\_address***

Displays eGTP-C statistics for an existing S-GW IP address expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**verbose**

Displays the maximum amount of detail available for this commands output. If this option is not specified, the output is truncated to a more concise level.

All of the cause codes supported for GTPv2 are displayed as part of this option. All the cause code values are shown for each of the messages.

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on using the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display evolved GPRS Tunneling Protocol Control (eGTP-C) plane statistics for a specific service name or interface type.

**Example**

The following command displays eGTP-C statistics for interfaces configured as S-GW ingress interfaces:

```
show egtpc statistics interface sgw-ingress
```

The following command displays eGTP-C session information for sessions associated with all MME interfaces configured on this system:

```
show egtpc sessions interface mme
```

## show egtp-service

Displays configuration information for evolved GPRS Tunneling Protocol (eGTP) services on this system.

---

### Product

ePDG  
MME  
P-GW  
SAEGW  
S-GW

---

### Privilege

Inspector

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

```
show egtp-service { all | name service_name } [ | { grep grep_options | more } ]
```

#### **all**

Displays configuration information for all eGTP services configured on this system.

#### **name** *service\_name*

Displays configuration information for an existing eGTP service specified as an alphanumeric string of 1 through 63 characters.

#### | { **grep** *grep\_options* | **more** }

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference Guide*.

---

### Usage Guidelines

Use this command to view configuration information for eGTP services on this system.

#### **Example**

The following command displays service statistics for the eGTP service named *egtp1*:

```
show egtp-service name egtp1
```

## show emps-profile

Displays a particular or all eMPS profile(s) configured with its associated attributes.

---

### Product

P-GW  
SAEGW  
S-GW

---

### Privilege

Security Administrator, Administrator, Operator, Inspector

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax

```
show emps-profile { all | name emps_profile_name }
```

### all

Displays configuration information for all eMPS profiles configured with its associated attributes.

### name *emps\_profile\_name*

Displays configuration information for an existing eMPS profile specified as an alphanumeric string of 1 through 63 characters.

---

### Usage Guidelines

Use this command for displaying emps-profile-name, configured eARP value, configured DSCP value, and enabled or disabled message-priority.

### Example

The following command displays service statistics for the eMPS profile named *emps1*:

```
show emps-profile name emps1
```

## show epdg-service

Displays information about selected EPDG calls/services.

---

### Product

ePDG

---

### Privilege

Inspector

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show epdg-service { all [ counters [ | { grep grep_options | more } ] ] | name
epdg_service_name [ counters [ | { grep grep_options | more } ] ] | statistics [
apn-name apn_name | dns-stats | name name ] | session { all | apn-name apn_name
| callid call_id | [ counters ] | [ full ] | ip-address { < ip_address | > ip_address
| IP-ADDRESS | greater-than ip_address | less-than ip_address } | peer-address
peer_address | [ summary ] | username user_name [ | { grep grep_options | more } ]
} statistics [ dns-stats ] [ name service_name ] [ peer-address peer_address ] [
| { grep grep_options | more } ] }
```

#### **all**

Displays information for all configured services.

#### **counters**

Displays counters associated with EPDG service.

#### **name** *epdg\_service\_name*

Displays specific service. This must be followed by service name *epdg\_service\_name*, which is a string of size between 1 and 63.

#### **statistics**

Displays information about total of collected information for specific protocol since last restart or clear command.

#### **apn-name** *apn-name*

Displays statistics for specific APN, must be followed by apn name, which is a string of size between 1 and 63.

#### **dns-stats**

Displays information related to DNS PGW selection.

#### **name** *name*

Displays specific service. Must be followed by service name.

#### **session**

Displays information about configured EPDG sessions.

#### **callid** *call\_id*

Specifies a Call Identification Number as an eight-digit hexadecimal number.

#### **full**

Displays all available information for associated display or filter keyword (previous keyword).

**ip-address**

Displays IP address of the subscriber. Must be followed by IPv4 address in dotted-decimal notation.

**< ip\_address | less-than ip\_address**

Specifies Less Than. Must be followed by an IP address specified in IPv4 dotted-decimal or IPV6 colon-separated-hexadecimal notation.

**> ip\_address | greater-than ip\_address**

Specifies Greater Than. Must be followed by an IP address specified in IPv4 dotted-decimal or IPV6 colon-separated-hexadecimal notation.

**peer-address peer\_address**

Specifies the IP address of an IP Peer in IPv4 address dotted-decimal or IPV6 address colon-separated-hexadecimal notation.

**summary**

Displays the summary of available information for associated display or filter keyword (previous keyword).

**username user\_name**

Displays the name of specific user within current context. *user\_name* is an alphanumeric string of 1 through 127 characters.

**statistics**

Displays the total of collected information for specific protocol since last **reload** or **clear** command.

**dns-stats**

Displays information related to DNS PGW selection.

**name service\_name**

Displays specific service. *service\_name* is an alphanumeric string of 1 through 63 characters.

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on using the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display information about selected EPDG calls/services.

**Example**

The following command displays ePDG counter information:

```
show epdg-service all counters | grep 21
```

## show event-record

Displays event record statistics for a P-GW node.

---

**Product** P-GW  
ePDG

---

**Privilege** Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show event-record statistics { epdg | pgw } [ | {grep grep_options | more } ]`

`| { grep grep_options | more }`

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on using the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines** Use this command to display all event record statistics for a P-GW node.

### Example

The following command displays all P-GW event level statistics:

```
show event-record statistics pgw
```

## show external-inline-servers

This command is obsolete.

## show fa-service

Displays information on configured foreign agent (FA) services.

---

**Product** PDSN  
GGSN  
ASN-GW

---

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

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show fa-service { all | name fa_name } [ | { grep grep_options | more } ]
```

**all | name *fa\_name***

**all**: indicates information on all foreign agent services is to be displayed.

**name *fa\_name***: indicates only the information for the named FA service is to be displayed.

**{ **grep** *grep\_options* | **more** }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage Guidelines**

Display foreign agent service configuration information.

**Example**

The following commands display information on the FA service *sampleService* and all services, respectively.

```
show fa-service name sampleService
```

```
show fa-service all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show fa-spi-list

Displays Security Parameter Indices (FA-SPIs) for configured foreign agent (FA) services.

**Product**

PDSN

GGSN

ASN-GW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show fa-spi-liste { all | name fa_name } [ | { grep grep_options | more } ]`

**all | name *fa\_name***

**all**: indicates information on all foreign agent services is to be displayed.

**name *fa\_name***: indicates only the information for the named FA service is to be displayed.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

---

**Usage Guidelines** Display foreign agent SPI information.

### Example

The following command displays SPI information for the FA service *sampleService*.

```
show fa-spi-list name sampleService
```




---

**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show fans

Displays the current control status, speed, and temperature for the upper and lower fans in an ASR 5x00 chassis.

---

**Product** All

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show fans [ verbose ] [ | { grep grep_options | more } ]`

**verbose**

*ASR 5500 only*: Displays additional information regarding the state of the fan trays.



**{ `grep` *grep\_options* | `more` }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

### Usage Guidelines

View the fan information to verify system hardware status as necessary.

### Example

The following command displays information regarding the cooling fans in the ASR 5x00 chassis:

```
show fans
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show file

Displays the contents of the file specified. The contents are paginated as if it were normal ASCII output.

### Product

All

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show file url url [ | { grep grep_options | more } ]
```

#### **url** *url*

Specifies the location of a file to display. *url* may refer to a local or a remote file. *url* must be entered using the following format:

For the ASR 5000:

```
[ file: ] { /flash | /pcmcia1 | /hd } [ /directory ] /file_name
tftp: // { host [ :port# ] } [ /directory ] /file_name
[ http: | ftp: | sftp: ] // [ username [ :password ] @ ] { host } [ :port# ] [ /directory ] /file_name
```



### Important

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

For the ASR 5500:

```
[ file: ]{ /flash | /usb1 | /hd }[ /directory ]/file_name
tftp://{ host[ :port# ] }[ /directory ]/file_name
[ http: | ftp: | sftp: ]//[ username[ :password ]@ ] { host }[ :port# ][
/directory ]/file_name
```



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

*directory* is the directory name.

*filename* is the actual file of interest.

*username* is the user to be authenticated.

*password* is the password to use for authentication.

*host* is the IP address or host name of the server.

*port#* is the logical port number that the communication protocol is to use.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Display the contents of files to view such information as log data, trace information, etc.

### Example

The following will display the contents of the local file */pub/log.txt*.

```
show file //pcmcial/pub/log.txt
```

The following command will display the contents of the file */pub/log.txt* on remote host *remoteABC*.

```
show file ftp://remoteABC/pub/log.txt
```

## show fng-service

Displays information about specified Femto Network Gateway (FNG) service configuration, status, and counters, and includes information about all the sessions currently maintained by the FNG.

### Product

FNG

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
show fng-service { all [ counters ] | name service_name | session |
statistics }
```

**all**

Displays information for all configured FNG services.

**counters**

Displays counters associated with the FNG service.

**name service\_name**

Displays information only for an existing FNG service specified as an alphanumeric string of 1 through 63 characters.

**session**

Displays information about configured FNG sessions.

**Important**

See **show fng-service session** for detailed options.

---

**statistics service\_name**

Total of collected information for specific protocol since the last **restart** or **clear** command.

**Important**

See **show fng-service statistics** for detailed options.

---

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the section *Regulating a Command's Output* in the chapter *Command Line Interface Overview* in the *Command Line Interface Reference*.

---

**Usage Guidelines**

Use this command to view information for selected configured FNG services.

**Example**

The following command displays available information for all active FNG services.

```
show fng-service all
```

**Important**

Command output descriptions are available in the *Statistics and Counters Reference*.

---

# show fng-service session

Displays statistics for specific Femto Network Gateway (FNG) sessions.

**Product** FNG

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

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **show fng-service session** [ **all** | **callid** *call\_id* | **counters** | **full** [ **all** | **callid** *call\_id* | **ip-address** *ip-address* | **peer-address** *ip\_address* | **username** *name* ] | **ip-address** *ip-address* | **peer-address** *ip-address* | **summary** [ **all** | **callid** *call\_id* | **ip-address** *ip-address* | **peer-address** *ip-address* | **username** *name* ] | **username** *name* ]

## **all**

Displays all related information for all active FNG sessions.

## **callid**

Displays PPP information for the call ID specified as a 4-digit hexadecimal number.

## **counters**

Displays counters for the configured FNG sessions.

## **full**

Displays all available information for the associated display or filter keyword.

## **ip-address** *ipv4\_address*

Displays information for the subscriber IP address specified in IPv4 dotted-decimal notation.

## **peer-address** *ipv4\_address*

Displays information for the IP peer specified by its IP address in IPv4 dotted-decimal notation.

## **summary**

Displays summary information for FNG sessions.

## **username** *user\_name*

Displays information for a username within the current context specified as an alphanumeric string of 1 through 127 characters.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the section *Regulating a Command's Output* in the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to view configuration information for an FNG session.

### Example

The following command displays all available FNG sessions.

```
show fng-service session all
```



### Important

Command output descriptions are available in the *Statistics and Counters Reference*.

## show fng-service statistics

Displays statistics for the FNG since the last restart or clear command. The output includes the number of each type of protocol message. For example, the output includes the various types of EAP messages.

### Product

FNG

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show fng-service statistics [ name service_name | peer-address ipv4_address ]
```

#### **name *service\_name***

Displays statistics for an existing service name specified as an alphanumeric string of 1 through 63 characters.

#### **peer-address *ipv4\_address***

Displays statistics for an IP peer specified by its IP address in IPv4 dotted-decimal notation.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the section *Regulating a Command's Output* in the *Command Line Interface Overview* chapter.

**Usage Guidelines** Use this command to display FNG statistics.



**Important** You may use more than one keyword per command line.

### Example

The following command displays information about the FNG service.

```
show fng-service statistics
```



**Important** Command output descriptions are available in the *Statistics and Counters Reference*.

## show freeze-ptmsi imsi

Displays the P-TMSI (packet-temporary mobile subscriber identify) corresponding to the IMSI (international mobile subscriber identity) that has entered a frozen state after the purge timeout timer expires.

**Product** SGSN

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

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `show freeze-ptmsi imsi imsi_num`

### *imsi imsi\_num*

Specifies the IMSI that has been frozen as a sequence of up to 15 digits. The first three digits are the MCC (mobile country code). The next two or three digits are the MNC (mobile network code). The remaining digits are the MSIN (mobile station identification number).

**Usage Guidelines** This command enables the operator to know whether a frozen IMSI has an associated P-TMSI.

### Example

The following command displays the P-TMSI corresponding to a frozen IMSI:

```
show freeze-ptmsi imsi 262090426000194
```

## show ggsn sessmgr

Displays session manager (SessMGR) statistics specific to the gGSN service.

---

**Product** GGSN

---

**Privilege** Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show ggsn sessmgr** { **all** | **instance** *smgr\_inst* }

### **all**

Displays all SessMGR statistics specific to the system's GGSN services.

### **instance** *smgr\_inst*

Displays the statistics for a session manager instance of the GGSN service specified as an integer between 1 and 10000000.

---

**Usage Guidelines** Use this command to display information for GGSN services.

### **Example**

The following command displays GGSN SessMGR statistics for all GGSN services on the system:

```
show ggsn sessmgr all
```

## show ggsn-service

Displays configuration information for Gateway GPRS Support Node (GGSN) services on the system.

---

**Product** GGSN

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show ggsn-service** { **all** | **name** *ggsn\_svc\_name* } [ | { **grep** *grep\_options* | **more** } ]

**all**

Displays information for all GGSN services configured with the given context.

**name *ggsn\_svc\_name***

Displays information for an existing GGSN service name specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For more information on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference*.

**Usage Guidelines**

This command is used to verify the configuration of one or all GGSN services for monitoring or troubleshooting purposes. The output is a concise listing of GGSN service parameter settings.

If this command is executed from within the local context with the **all** keyword, information for all GGSN services configured on the system will be displayed.

**Example**

The following command displays configuration information for a GGSN service called *ggsn1*:

```
show ggsn-service name ggsn1
```

## show ggsn-service sgsn-table

Lists all Serving GPRS Support Nodes (SGSNs) by IP addresses and shows the current number of subscribers to each SGSN.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show ggsn-service sgsn-table
```

**Usage Guidelines**

While there are existing commands to show SGSN subscriber information, this command is the only way to list all SGSNs by IP address and show the current number of subscribers to each SGSN.



**Example**

The following command will bring up a table showing the current active/inactive status, IP address, reboots/restarts and SGSN users.

```
show ggsn-service sgsn-table
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show global-title-translation

Displays configuration information for Global Title Translation (GTT).

**Product**

SGSN

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show global-title-translation { address-map { all | instance instance } |
association { all | instance instance } }
```

**address-map { all | instance }**

Displays configuration information for either the entire GTT address map database or for a specific instance of an address map. *instance* is an integer from 1 to 4096 which uniquely identifies the address map configuration.

**association { all | instance }**

Displays configuration information for either the entire database of GTT association lists for for a specific instance of GTT association configuration. *instance* is an integer from 1 to 16 which uniquely identifies the GTT association configuration.

**Usage Guidelines**

This command displays the configuration for the GTT address maps and associations.

**Example**

The following command displays the address map 2047.

```
show global-title-translation address-map 2047
```

## show gmb statistics

Displays the collected statistics for the Gmb reference point. Gmb handles broadcast multicast service center (BM-SC) related signaling, which includes the user specific and bearer service messages for Multimedia Broadcast/Multicast Service (MBMS) service.

**Product** GGSN

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

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `show gmb statistics [ apn name | bmsc-profile profile_name ] [ | { grep grep_options | more }]`

### **apn *name***

Displays only the Gmb information for the specified Access Point Name (APN) specified as an alphanumeric string of 1 through 62 characters.

### **bmsc-profile *profile\_name***

Displays only the Gmb information for the specified BM-SC profile specified as an alphanumeric string of 1 through 79 characters.

### **| { **grep** *grep\_options* | **more** }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For more information on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference*.

**Usage Guidelines** Use this command to display usage statistics for the Gmb reference point.

### **Example**

The following command displays all Gmb statistics:

```
show gmb statistics
```

## show gmm-sm statistics

Displays statistics for the GPRS Mobility Management and Session Management (GMM/SM) configuration of the system's SGSN service. GMM/SM supports mobility to allow the SGSN to know the location of a

Mobile Station (MS) at any time and to activate, modify and deactivate the PDP sessions required by the MS for user data transfer.

**Product** SGSN

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

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **show gmm-sm statistics** [ **gmm-only** | **gprs-service** *svrc\_name* | **iups-service** *svrc\_name* | **plmn-id** *mcc mcc mnc mnc* [ **access-type** { **gprs** | **umts** } ] | **recovered-values** | **sgsn-service** *svrc\_name* | **sm-only** ] [ **verbose** ] [ | { **grep** *grep\_options* | **more** } ]

Keywords are presented below. Primary keywords are listed in the order of selection as shown in the syntax. Secondary or filtering keywords are presented alphabetically after the description of the primary keywords.

#### **gmm-only**

Displays only GPRS mobility management (GMM) information for other specified keyword parameters for the current context.

#### **gprs-service** *svrc\_name*

Displays the statistics for an existing 2.5G GPRS service name specified as an alphanumeric string of 1 through 63 characters.

The display request can be narrowed by adding either the **nsei** or **routing-area** filter keywords.

#### **iups-service** *svrc\_name*

Displays the statistics for an existing IuPS service specified as an alphanumeric string of 1 through 63 characters.

The display request can be narrowed by adding either the **rnc** or **routing-area** filter keywords.

#### **plmn-id** *mcc mcc mncmnc* [ **access-type** { **gprs** | **umts** } ]

Filters the statistics display per PLMN.

Enter the **access-type** keyword to fine-tune the display of the GMM/SM statistics to an aggregate of the IuPS (select access-type UMTS) and/or the GPRS (select access-type GPRS) services belonging to the PLMN.

#### **recovered-values**

Only displays recovered values for key KPI counters that were backed-up.

#### **sgsn-service** *svrc\_name*

Displays the statistics for an existing 3G SGSN service specified as an alphanumeric string of 1 through 63 characters.

The display request can be narrowed by adding either the **rnc** or **routing-area** filter keywords.

**sm-only**

Displays only session management (SM) information for other specified keyword parameters for the current context.

**access-type *type***

Filters the display of service statistics by 2.5G GPRS services or 3G IuPS services for UMTS:

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

If this keyword is not included, then statistics for both access types are displayed.

**lac *lac\_id***

Specifies the location area code (LAC) as part of the identification of the RNC or RA as an integer from 1 through 65535.

**mcc *mcc\_id***

Specifies the mobile country code (MCC) as part of the identification of the RNC or RA an integer from 100 through 999.

**mnc *mnc\_id***

Specifies the mobile network code (MNC) as part of the identification of the RNC or RA as a 2- or 3-digit integer from 00 through 999.

**nsei *nse\_id***

Displays the GMM/SM session statistics for an existing network service entity (NSEI) specified as an integer from 0 to 65535.

**rac *rac\_id***

Specifies the routing area code (RAC) as part of the identification of the RNC or RA as an integer from 1 through 255.

**rnc *rnc\_id***

Enter this keyword to fine-tune the display of the GMM/SM session statistics just for the radio network controller (RNC) specified as an integer from 0 through 4095.

**routing-area *mcc\_id mnc\_id lac\_id rac\_id***

Enter the **routing-area** keyword to fine-tune the display of the GMM/SM statistics for a specified routing area (RA) identified by the MCC, MNC, LAC and RAC.

**verbose**

Displays all possible statistics for specified command or keyword.

**{ `grep` *grep\_options* | `more` }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For more information on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display usage statistics for the GMM/SM session configurations for SGSN services, including a BSC attaches, activations, and throughput.

### Example

The following command displays GMM/SM statistics for a specific routing area defined for the 2.5G SGSN's GPRS service:

```
show gmm-sm statistics gprs-service gprs1 routing-area mcc 123 mcc 131
lac 24 rac 11
```

The following command displays all possible information for GMM/SM statistics:

```
show gmm-sm statistics verbose
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show gprsns statistics

Displays the statistics for the 2.5G SGSN's GPRS NS layer (link level).

### Product

SGSN

### Privilege

Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show gprsns statistics { msg-stats { consolidated nse nse_id | nse nse_id
} | sns-msg-stats } | { grep grep_options | more }
```

#### msg-stats

Displays the transmit (Tx) and receive (Rx) message statistics (except for SNS messages) in the statistics output.

#### consolidated nse *nse\_id*

*nse\_id*: Enter an integer from 0 to 65535.

**nse *nse\_id***

Display statistics for a NSE specified as an integer from 0 to 65535.

**sns-msg-stats**

Display subnetwork service (SNS) sublayer message statistics.

**{ *grep grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage Guidelines**

This command is used to display Frame Relay statistics configured for the NSE/NSVC with the commands documented in the *Network Service Entity - Peer NSEI Configuration Mode Commands* chapter.

Collected statistics are cleared (deleted) with the **clear gprsns statistics** described in the *Exec Mode Commands (A-C)* chapter.

**Example**

Use the following command to display the collected message statistics for NSEI 1422:

```
show gprsns statistics msg-stats nse 1422
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show gprsns status

Displays the status of the network service virtual circuits (NSVC) for the GPRS NS layer (link level).

**Product**

SGSN

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show gprsns status { nsvc-status-all nse nse_id | nsvc-status-consolidated
  nse nse_id | nsvc-status-per-bvci bvci bvc_id nse nse_id } | { grep grep_options
  | more }
```

**nsvc-status-all nse { all | *nsense\_id* }**

Displays status information for all NSVCs included in the NSE specified as an integer from 0 to 65535.

**nsvc-status-consolidated nse *nse\_id***

**nsvc-status-per-bvci bvci *bvc\_id* nse *nse\_id***

*bvc\_id* is an integer from 0 to 65535.

*nse\_id* is an integer from 0 to 65535.

**[ { *grep grep\_options* | more } ]**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

### Usage Guidelines

This command is used to display the status of the NSVC.

### Example

Use the following command to display status of all NSVC for NSE 1422:

```
show gprsns status nsvc-status-all nse 1422
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show gprs-service

Displays the statistics for GPRS services.

### Product

SGSN

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show gprs-service { all | name gprs_srvc_name } [ nsei { all | id nse_id } |
{ grep grep_options | more } ]
```

#### all

Instructs the SGSN to display information for all GPRS services configured with this context.

#### name *gprs\_srvc\_name*

Instructs the SGSN to display information for the specified GRPS service.

*gprs\_srvc\_name* is a case-sensitive string of 1 to 63 characters, any combination of letters, digits, dots (.) and dashes (-) that identifies a specific GPRS service.

### **nsei { all | id }nse\_id**

Instructs the SGSN to display network service entity information for either a specific NSEI or for all NSEI configured for the specified GRPS service(s).

*nse\_id* is an integer from 0 to 65535.

### **{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For more information on the usage of **grep** and **more**, refer to the Regulating a Command's Output section of the Command Line Interface Reference.

## Usage Guidelines

This command is used to verify the configuration of one or all GPRS services for monitoring or troubleshooting purposes. The output is a concise listing of GPRS service parameter settings.

If this command is executed from within the local context with the **all** keyword, information for all GPRS services configured on the system will be displayed.

## Example

The following command displays configuration information for all GPRS services configured in this context:

```
show gprs-service all
```

Use a command similar to the following to display statistics for NSEI 4257 for the GPRS service named *London2*:

```
show gprs-service name London2 nsei id 4257
```



## Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

# show gprssf

Displays statistics for various 3GPP Customised Applications for Mobile network Enhanced Logic (CAMEL) service GPRS Service Switching Function (gprSSF) entities.

## Product

SGSN

## Privilege

Inspector

## Command Modes

Exec

The following prompt is displayed in the Exec mode:



```
[local]host_name#
```

---

**Syntax Description**

```
show gprssf { counters | statistics } [ camel-service svrc_name | gprs [
2g-sgsn-app | 3g-sgsn-app ] | gsmscf-address { address | all } | sms ] [
| { grep | more } ]
```

**counters**

Displays collected status counter information for CAMEL service entities.

**statistics**

Displays collected statistics for CAMEL service entities.

**camel-service *svrc\_name***

Filters the display of counters and statistics for an existing CAMEL service name in the SGSN configuration specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**gprs [ 2g-sgsn-app | 3g-sgsn-app ]**

Filters the counter/statistic output to display GPRS protocol information specific to either the 2.5G or 3G SGSN.

**gsmscf-address { *address* | all }**

The GSM service control function (gsmSCF) address is the ISDN address of the SCP where the CAMEL service resides. It is possible to display information for one or all of the configured CAMEL services.

*address* is a standard ISDN E.164 address of 1 to 15 digits.

**sms**

Filters the display of counters and statistics for SMS protocol information.

**{ { grep *grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

---

**Usage Guidelines**

Use this command to display CAMEL service status counter information and statistics collected since the last restart or clear command. If filters are not included with the command, then all statistics or counters are displayed for all CAMEL services in all contexts in which CAMEL services have been defined.

Collected statistics are cleared (deleted) with the **clear gprssf statistics** command described in the chapter *Exec Mode Commands (A-C)*.

**Example**

Use the following command to display the status counter totals of the GPRS Dialogue parameters for a 3G SGSN:

```
show gprsssf counter gprs 3g-sgsn-app
```




---

**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show gs-service

Displays configuration information and statistics for Gs services configured on system.

---

### Product

SGSN

---

### Privilege

Security Administrator, Administrator, Operator, Inspector

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

```
show gs-service { all | name svc_name } [ | { grep grep_options | more } ]
```

#### **all**

Displays information for all Gs services configured with in the given context.

#### **name** *svc\_name*

Displays information for an existing Gs service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

#### | { **grep** *grep\_options* | **more** }

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For more information on the usage of **grep** and **more**, refer to the Regulating a Command's Output section of the Command Line Interface Reference.

---

### Usage Guidelines

This command is used to verify the configuration of one or all Gs services for monitoring or troubleshooting purposes.

If this command is executed from within the local context with the all keyword, information for all Gs services configured on the system will be displayed.

### Example

The following command displays configuration information for all Gs services configured on a system:

```
show gs-service all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show gtpc

Displays GPRS Tunnelling Protocol-Control (GTPC) information for GTPv0, GTPv1-C, GTPv1-U with filtering options.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show gtpc [ full | counters | summary ] { all | apn apn_name | imsi imsi_value
[ nsapi nsapi_value ] | callid callid | sgsn-address ip_address | ggsn-service
ggsn_name | user-address ip_address | username username }
```

**[ full | counters | summary ]**

Specifies the level of information to be displayed. The following levels can be used:

- **full**: Indicates detailed information is to be displayed.
- **counters**: Indicates the output is to include the statistical counters.
- **summary**: Indicates only summary information is to be displayed.

```
{ all | apn apn_name | imsi imsi_value [ nsapi nsapi_value ] | callid callid | sgsn-address ip_address |
ggsn-service ggsn_name | user-address ip_address | username username }
```

Specifies the filter criteria used when displaying GTP information. The following filters can be used:

- **all**: Specifies that all available information is to be displayed.
- **apn** *apn\_name*: Specifies that GTP information for an APN specified as an alphanumeric string of 1 through 63 characters that is case sensitive.
- **imsi** *imsi\_value* [ **nsapi** *nsapi\_value* ]: Displays GTP information for an International Mobile Subscriber Identity (IMSI) specified as an integer from 1 through 15 characters. Optionally, the IMSI could be further filtered by specifying a particular PDP context using the Network Service Access Point Identifier (NSAPI) expressed as an integer from 5 through 15.

**Important**

In release 18.2 and later, this command option has been deprecated.

- **callid** *callid*: Displays GTP information for a call identification number specified as a 4-digit hexadecimal number.




---

**Important** In release 18.2 and later, this command option has been deprecated.

---

- **sgsn-address** *ip\_address*: Displays GTP information for an SGSN specified by its IP address in IPv4 dotted-decimal notation.
- **ggsn-service** *ggsn\_name*: Displays GTP information for an existing GGSN service specified an alphanumeric string of 1 through 63 characters that is case sensitive.
- **user-address** *ip\_address*: Displays GTP information for a user PDP context specified as an IP address in IPv4 dotted-decimal notation.




---

**Important** In release 18.2 and later, this command option has been deprecated.

---

- **username** *username*: Displays GTP information for a username specified as an alphanumeric string of 1 through 127 characters (including wildcards '\$' and '\*') that is case sensitive.




---

**Important** In release 18.2 and later, this command option has been deprecated.

---

### Usage Guidelines

This command displays statistics for every GTP message type based on the filter criteria. This information is useful for system monitoring or troubleshooting.

### Example

The following command displays GTPC counters for a GGSN service named *ggsn1*:

```
show gtpc counters ggsn-service ggsn1
```

The following command displays GTPC full information:

```
show gtpc full
```

The following command displays GTPC summary information for a specific call identification number of *05f62f34*:

```
show gtpc summary callid 05f62f34
```



### Important

---

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show gtpc statistics

Displays GTPv0, GTPv1-C, GTPv1-U statistics with filtering options.

<b>Product</b>	GGSN
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<b>show gtpc statistics</b> [ [ <b>custom1</b>   <b>custom2</b> ] [ <b>apn</b> <i>apn_name</i>   <b>ggsn-service</b> <i>ggsn_service_name</i>   <b>mseg-service</b> <i>mseg_service_name</i>   <b>sgsn-address</b> <i>ipv4_address</i> ] [ [ <b>verbose</b> ] <b>format1</b> ] [   { <b>grep</b> <i>grep_options</i>   <b>more</b> } ]

**custom1**

Displays statistics of GTP-C messages for preservation mode and free of charge service.

This keyword is customer specific and license enabled. For more information, contact your Cisco sales representative.

**custom2**

Displays statistics for GTP-C messages related to overcharging protection on loss of radio coverage for a GGSN service.

This keyword is feature specific and license enabled. For more information, contact your Cisco sales representative.

**apn *apn\_name***

Displays GTP-C statistics for an existing APN specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**ggsn-service *ggsn\_service\_name***

Displays GTP-C statistics for an existing GGSN service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**mseg-service *mseg\_service\_name*****Important**

This keyword is not supported in this release.

**sgsn-address *ipv4\_address***

Displays GTP statistics for an SGSN specified by its IP address in IPv4 dotted-decimal notation.

**verbose**

Displays detailed instead of concise statistics.

**format1**

Displays more detailed statistical breakouts.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

The information displayed by this command consists of session statistics such as the number of currently active sessions categorized by PDP context type, and statistics for every GTP message type. The statistics are cumulative.

If the verbose keyword is used, additional information will be displayed such as statistics for every type of error code.

**Example**

The following command displays verbose GTP statistics:

```
show gtpc statistics verbose
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

# show gtp

Displays information on the GPRS Tunneling Protocol Prime (GTPP) for the selected charging gateway function (CGF) or GCDR storage server.

**Product**

GGSN  
P-GW  
SAEGW  
SGSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show gtp { accounting | counters { all | cgf-address | group } | group
{ all | name } | statistics { cgf-address | group } | storage server {
counters | group | local | statistics | status | streaming } } [ | { grep
grep_options | more } ]
```

**Usage Guidelines**

This command displays the GTPP related information for the selected CGF or the G-CDRs storage server. If this command is issued from within the local context, information for all GTPP accounting servers configured on the system is displayed regardless of context.

**Example**

The following command displays the GTPP counters for all the servers:

```
show gtp accounting all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show gtp accounting

Displays information on the GPRS Tunneling Protocol Prime (GTPP) accounting server configuration.

**Product**

GGSN  
P-GW  
SAEGW  
SGSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show gtp accounting servers { group name group_name } [ | { grep grep_options | more } ]
```

**group name *group\_name***

Displays information and CDR statistics for an existing GTPP server group name specified as an alphanumeric string of 1 through 63 characters.

**{ **grep** *grep\_options* | **more** }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For more information on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

This command is used to view the status of GTPP accounting servers configured within a context for monitoring or troubleshooting purposes.

If this command is issued from within the local context, information for all GTPP accounting servers configured on the system is displayed regardless of context.

### Example

The following command displays the status of and information on configured GTPP accounting servers:

```
show gtp accounting servers
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show gtp counters

Displays GTPP counters for configured Charging Gateway Functions (CGFs) within the given context.

### Product

ePDG  
GGSN  
P-GW  
SAEGW  
SGSN

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show gtp counters { all [ gcdrs ] | cgf-address ipv4/ipv6_address [ gcdrs  
| port port_num ] | group name group_name } [ | { grep grep_options | more } ]
```

#### all

Displays counters for all CGFs configured within the context.

**cgf-address** *ipv4/ipv6\_address* [ gcdrs | port *port\_num* ]

Displays counters for a CGF specified by its IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**gcdrs**: Displays G-CDR specific GTPP counters only.

**port** *port\_num*: Specifies the port number of CGF server. The port number must be an integer ranging from 1 to 65535.



This optional keyword is introduced to ease the identification of product specific CDRs. This configuration provides the flexibility to send ePDG, SaMOG and P-GW LBO CDRs to the same CGF server on different ports.

When port is specified along with the IP address, this command displays the GTPP counters for the specified CGF server IP address and port. If port is not provided, then it will show the accumulated counters for all CGF servers with the specified IP address.

**group name** *group\_name*

Displays counters for a GTPP server group name specified as an alphanumeric string of 1 through 63 characters.

**{ { grep** *grep\_options* | **more** }

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For more information on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

### Usage Guidelines

Counters for a single CGF can be viewed using the **cgf-address** keyword. Counters for all CGFs in the context can be viewed by entering the command with the **all** keyword.

If this command is issued from within the local context and no CGF-address is specified, the counters displayed will be cumulative for all CGFs configured on the system regardless of context.

### Example

The following command displays counters for all CGF servers:

```
show gtp counters all
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show gtp group

Displays information pertaining to the configured GTPP storage server group.

### Product

GGSN  
P-GW  
SAEGW  
SGSN

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show gtp group { name gtp_group_name | all } [ | { grep grep_options | more } ]`

**name *gtp\_group\_name***

Displays information and CDR statistics for an existing GTPP server group name specified as an alphanumeric string of 1 through 63 characters.

**all**

Displays statistics for all configured GTPP storage server groups, including default group.

**| { **grep** *grep\_options* | **more** }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For more information on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Use this command to display the CDR statistics on the basis of GTPP server groups. It shows the information for all or specific GTPP server group configured in the context from which this command is issued.

**Example**

The following command displays the status of the GTPP server group backup server configured in a context called *GTPP\_Group1*:

```
show gtp group name GTPP_Group1
```




---

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show gtp statistics

Displays GTPP statistics for configured Charging Gateway Functions (CGFs) within the context.

---

**Product**

ePDG  
GGSN  
P-GW  
SAEGW  
SGSN

---

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

```
show gtp statistics { cgf-address ipv4/ipv6_address [ port port_num ] | group
name group_name } [ | { grep grep_options | more } ]
```

#### **cgf-address** *ipv4/ipv6\_address* [ **port** *port\_num* ]

Displays statistics for a CGF specified by its IP address expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**port** *port\_num*: Specifies the port number of CGF server. The port number must be an integer ranging from 1 to 65535.

This optional keyword is introduced to ease the identification of product specific CDRs. This configuration provides the flexibility to send ePDG, SaMOG and P-GW LBO CDRs to the same CGF server on different ports.

When the port is specified, this command displays statistics of GTPP messages sent/received by CGF server IP address and specified port. If port is not provided then it will show the accumulated statistics for all CGF servers with the specified IP address.

#### **group name** *group\_name*

Displays server statistics information of an existing GTPP server group name specified as an alphanumeric string of 1 through 63 characters.

#### [ { **grep** *grep\_options* | **more** } ]

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For more information on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

---

### Usage Guidelines

Statistics for a single CGF can be viewed by specifying its IP address. Statistics for all CGFs in the context can be viewed by **not** specifying an IP address.

If this command is issued from within the local context, the statistics displayed will be cumulative for all CGFs configured on the system regardless of context.

### Example

The following command displays statistics for a CGF with an IP address of *192.168.1.14*:

```
show gtp statistics cgf-address 192.168.1.14
```




---

### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

# show gtp storage-server

Displays information pertaining to the configured GTPP storage server (GSS).

---

## Product

GGSN  
P-GW  
SAEGW  
SGSN

---

## Privilege

Security Administrator, Administrator, Operator, Inspector

---

## Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

## Syntax Description

```
show gtp storage-server [ counters { all | group name group_name } | group
name group_name | local file { counters { all | group name group_name } |
statistics [ group name group_name ] } | status { group name group_name |
verbose } | streaming file { counters { all | group name group_name } |
statistics [ group name group_name ] } ] [ | { grep grep_options | more } ]
```

### counters

Displays counters for the external GTPP storage server.

### group name *group\_name*

Displays GTPP backup server information for the group name specified as an alphanumeric string of 1 through 63 characters.

### local file

Displays statistics and counters for the local storage-server. This is the hard disk if hard disk support has been enabled with the **gtp storage-server mode** command in the GTPP Group Configuration Mode.

### statistics

Displays statistics for the GTPP storage server.

### status [ **verbose** ]

Displays status of the GTPP storage server. **verbose** enables the detailed view.

### streaming

Displays the status of Charging Data Record (CDR) backup on HDD while streaming mode is enabled.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

### Usage Guidelines

Executing this command with no keywords displays status information for the GTPP backup server configured in the context from which this command is issued.

### Example

The following command displays the GTPP CDR file statistics stored on the local SMC hard disk.

```
show gtp storage-server local file counters all
```

The following command displays the status of the GTPP backup server configured in a context called ggsn1:

```
show gtp storage-server
```

The following command displays statistics for the GTPP backup server configured in a context called ggsn1:

```
show gtp storage-server statistics
```

The following command displays GCDR storage server counters:

```
show gtp storage-server counters
```

The following command displays GCDR storage server status:

```
show gtp storage-server status
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show gtpu

Displays GPRS Tunneling Protocol user plane (GTP-U) statistics and counters on this system.

### Product

ePDG  
P-GW  
SAEGW  
SGSN  
S-GW

### Privilege

Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show gtpu { local-addresses | statistics [ [ gtpu-service gtpu_service_name
] [ gtpumgr-instance gtpumgr_instance | local-address ipv4/ipv6_address |
mseg-service mseg_service_name | peer-address ipv4/ipv6_address ] ] [ | { grep
grep_options | more } ] }
```

#### local-addresses

Displays the number of sessions on all GTPU local addresses in all GTPU services.

#### statistics

Displays all GTP-U statistics on all GTP-U services. Refine the display by including one of the filters listed below.

#### gtpu-service *gtpu\_service\_name*

Displays GTP-U statistics for an existing GTP-U service specified as an alphanumeric string of 1 through 63 characters.

#### gtpumgr-instance *instance\_number*

Displays information for an existing GTP-U manager instance specified as an integer from 1 through 4294967295.

#### local-address *ipv4/ipv6\_address*

Displays subscriber statistics and counters in the current active session per local GTPU IP address specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation in a GTPU service.

#### mseg-service *mseg\_service\_name*



### Important

This keyword is not supported in this release.

#### peer-address *ipv4/ipv6\_address*

Displays GTP-U statistics and counters for an existing peer IP address specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

#### | { grep *grep\_options* | more }

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference Guide*.

### Usage Guidelines

Use this command to view statistics and counters for GTP-U traffic on this system. Refine the statistics display by including a filter with the command.



**Important** The **show gtpu statistics** command should be given from the local context only; issuing the command from any other context will result in an error message.

### Example

The following command displays statistics for the GTP-U service named *gtp1*:

```
show gtpu statistics gtpu-service gtp1
```

The following command displays active sessions on all local-addresses categorised by GTPU service:

```
show gtpu local-addresses
```

The following command displays statistics for local GTPU address *168.123.123.1*:

```
show gtpu statistics local-address 168.123.123.1
```

## show gtpu-service

Displays configuration information for GPRS Tunneling Protocol user plane (GTP-U) services on this system.

### Product

ePDG  
P-GW  
SAEGW  
S-GW

### Privilege

Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show gtpu-service { all | name service_name } [ | { grep grep_options | more } ]
```

#### **all**

Displays configuration information for all GTP-U services configured on this system.

#### **name service\_name**

Displays configuration information for an existing GTP-U service specified an alphanumeric string of 1 through 63 characters.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference Guide*.

---

**Usage Guidelines**

Use this command to view configuration information for GTP-U services on this system.

**Example**

The following command displays service statistics for the GTP-U service named *gtpu1*:

```
show gtpu-service name gtpu1
```





# CHAPTER 21

## Exec Mode show Commands (H-L)

The Exec Mode is the initial entry point into the command line interface system. Exec mode **show** commands are useful in troubleshooting and basic system monitoring.

### Command Modes

This section includes the commands **show ha-service** through **show lte-policy**.

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```



### Important

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

- [show ha-service](#), on page 869
- [show ha-spi-list](#), on page 870
- [show hardware](#), on page 871
- [show hd raid](#), on page 872
- [show hd-storage-policy](#), on page 872
- [show hcnbgw](#), on page 873
- [show hcnbgw-access-service](#), on page 875
- [show hcnbgw-network-service](#), on page 877
- [show hexdump-module](#), on page 879
- [show hcnbgw access-control-db](#), on page 880
- [show hcnbgw counters](#), on page 881
- [show hcnbgw-global](#), on page 882
- [show hcnbgw sessions](#), on page 882
- [show hcnbgw statistics hcnbgw-service](#), on page 885
- [show hcnbgw statistics hcnbid](#), on page 887
- [show hcnbgw-service](#), on page 888
- [show hsgw-service](#), on page 889
- [show hss-peer-service](#), on page 891
- [show imei-profile](#), on page 892
- [show ims-authorization policy-control](#), on page 893
- [show ims-authorization policy-control misc-info](#), on page 894

- [show ims-authorization policy-gate](#), on page 895
- [show ims-authorization servers](#), on page 897
- [show ims-authorization service](#), on page 898
- [show ims-authorization sessions](#), on page 900
- [show instance-logging](#), on page 902
- [show inventory](#), on page 903
- [show ip access-group statistics](#), on page 903
- [show ip access-list](#), on page 904
- [show ip arp](#), on page 905
- [show ip as-path-access-list](#), on page 906
- [show ip bgp](#), on page 906
- [show ip framed-prefixes](#), on page 909
- [show ip igmp group](#), on page 910
- [show ip interface](#), on page 910
- [show ip ipsp](#), on page 912
- [show ip localhosts](#), on page 913
- [show ip ospf](#), on page 913
- [show ip policy-forward](#), on page 915
- [show ip pool](#), on page 916
- [show ip prefix-list](#), on page 918
- [show ip route](#), on page 919
- [show ip route-access-list](#), on page 920
- [show ip static-route](#), on page 921
- [show ip vrf](#), on page 922
- [show ip vrf-list](#), on page 923
- [show ipms status](#), on page 923
- [show ipne peers](#), on page 924
- [show ipsg service](#), on page 925
- [show ipsg sessions](#), on page 926
- [show ipsg statistics](#), on page 927
- [show ipv6 access-group statistics](#), on page 929
- [show ipv6 access-list](#), on page 929
- [show ipv6 interface](#), on page 930
- [show ipv6 neighbors](#), on page 931
- [show ipv6 ospf](#), on page 932
- [show ipv6 pool](#), on page 934
- [show ipv6 prefix-list](#), on page 935
- [show ipv6 route](#), on page 936
- [show ipv6 route-access-list](#), on page 937
- [show iups-service](#), on page 938
- [show l2tp sessions](#), on page 939
- [show l2tp statistics](#), on page 941
- [show l2tp tunnels](#), on page 942
- [show lac-service](#), on page 944
- [show lawful-intercept](#), on page 945
- [show lawful-intercept ssdf statistics](#), on page 945

- [show ldap connection all](#), on page 945
- [show leds](#), on page 946
- [show license](#), on page 947
- [show link-aggregation](#), on page 949
- [show linkmgr](#), on page 951
- [show llc statistics](#), on page 951
- [show llc status](#), on page 952
- [show lma-service](#), on page 954
- [show lns-service](#), on page 956
- [show local-policy](#), on page 957
- [show local-user](#), on page 957
- [show location-service](#), on page 959
- [show logging](#), on page 960
- [show logical-port utilization table](#), on page 961
- [show logs](#), on page 962
- [show lte-policy](#), on page 974

## show ha-service

Displays information on configured Home Agent (HA) services.

---

**Product** HA

---

**Privilege** Security Administrator Operator, Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show ha-service** { **all** | **name** *ha\_name* } [ | { **grep** *grep\_options* | **more** } ]

**all** | **name** *ha\_name*

**all**: Displays information on all Home Agent services.

**name** *ha\_name*: Displays information for an existing HA service specified as an alphanumeric string of 1 through 63 characters.

| { **grep** *grep\_options* | **more** }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines** Display home agent service configuration information.

**Example**

The following commands displays information on the HA service *sampleService* and all services, respectively.

```
show ha-service name sampleService
show ha-service all
```

## show ha-spi-list

Displays all or a specific Home Agent-Security Parameters Index (HA-SPI) remote address list(s).

**Product**

HA

**Privilege**

Security Administrator Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show ha-spi-list { all | name ha_name } [ | { grep grep_options | more } ]
```

**all | name *ha\_name***

**all**: Displays information on all HA-SPI lists.

**name *ha\_name***: Displays information for an existing HA-SPI list specified as an alphanumeric string of 1 through 63 characters.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Display a single or all HA-SPI lists.

**Example**

The following commands displays information on the HA-SPI list named *spi012* and all lists, respectively.

```
show ha-spi-list name spi012
show ha-spi-list all
```

# show hardware

Displays information on the system hardware.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
show hardware { card [ card_num ] | inventory | version [ board | diags | fans ] } [ | { grep grep_options | more } ]
```

**card [ *card\_num* ]**

Provides the hardware information for all ASR 5x00 cards or the card specified by *card\_num*. *card\_num* must be a value in the range 1 through 48 for the ASR 5000 or 1 through 20 for the ASR 5500 and must refer to an installed card.

**inventory**

Displays the ASR 5x00 hardware information for all slots in tabular format.

**version [ board | diags | fans ]**

Displays the CPU information for all ASR 5x00 application cards and fan controller version for the upper and lower fan trays.

**board**: Only include the CPLD and FPGA version information.

**diags**: Only include the CFE diagnostics version information.

**fans**: Show the fan controller versions for the upper and lower fan trays.

**{ **grep** *grep\_options* | **more** }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Show the hardware information and hardware component versions.

**Example**

The following displays the hardware information for a card installed in slot 1.

```
show hardware card 1
```

The following command displays the hardware inventory for the entire chassis.

**show hardware inventory**

The following command results in the display of the CPU version for all application cards displaying only the CPLD and FPGA information.

**show hardware version board**

The following command displays VPC virtual card information:

**show hardware**


---

**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show hd raid

Shows the output of the Redundant Array of Independent Disks (RAID) established on the ASR 5000 SMCs or ASR 5500 FSCs.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator, Administrator, Operator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<b>show hd raid [ verbose ]</b>

**Example**

The following command displays HD RAID configuration information:

**show hd raid verbose**


---

**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show hd-storage-policy

Displays Array Configuration Replicator (ACR) counter and statistical information.

<b>Product</b>	HSGW P-GW SAEGW
----------------	-----------------------

S-GW

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show hd-storage-policy { all | counters [ all ] [ name name ] [ verbose ]
| name name | statistics [ all ] [ name name ] [ verbose ] }
```

**all**

Displays ACR information for all HD storage policies configured on the system.

**counters [ all ] [ name *name* ] [ verbose ]**

**all:** Displays ACR counter information for all HD storage policies configured on the system.

**name *name*:** Displays ACR counter information for an existing HD storage policy specified as an alphanumeric string of 0 through 63 characters.

**statistics [ all ] [ name *name* ] [ verbose ]**

**all:** Displays ACR statistical information for all HD storage policies configured on the system.

**name *name*:** Displays ACR statistical information for an existing HD storage policy specified as an alphanumeric string of 0 through 63 characters.

**verbose**

Displays HD storage statistics based on instance.

**Usage Guidelines**

Use this command to display ACR counter and statistic information.

**Example**

The following command displays ACR statistical information for an HD storage policy named *pgwsgw*:

```
show hd-storage-policy statistics name pgwsgw
```

# show henbgw

**Important**

In Release 20, 21.0 and 21.1, HeNBGW is not supported. This command must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

This command displays Home evolved NodeB Gateway (HeNBGW) service related information.

---

**Product** HeNBGW

---

**Privilege** Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
show hcnbgw { hcnb-association [ all | full | hcnbgw-access-service
hcnbgw_acc_svc_name | peer-address peer_ip_address | peer-id peer_id_value |
summary ] | session [ all | callid call_id | full [ all | callid call_id
| qci qci_value | s1-peer s1_peer_address ] | qci qci_value | s1-peer s1_peer_address
| summary [ all | callid call_id | qci qci_value | s1-peer s1_peer_address ]
] | ue [ all | summary ] [ [ { grep grep_options | more } ] ] }
```

**hcnb-association** [ **all** | **full** | **hcnbgw-access-service** *hcnbgw\_acc\_svc\_name* | **peer-address** *peer\_ip\_address* | **peer-id** *peer\_id\_value* | **summary** ]

**hcnb-association** : Displays information about HENB associations.

**all**: Displays information for all HeNB associations.

**full**: Displays all available information for associated display or filter keyword (previous keyword).

**hcnbgw-access-service**: Displays information about HeNB associations with the specified HeNBGW access service.

*hcnbgw\_acc\_svc\_name* is an alphanumeric string of 1 through 63 characters.

**peer-address**: Displays information about HeNB associations with the specified peer.

*peer\_ip\_address* is an IPv4 address in dotted-decimal notation or an IPv6 address in colon-separated-hexadecimal notation.

**peer-id**: Displays information about HeNB associations for the specified peer.

*peer\_id\_value* is an integer from 0 to 4294967295.

**summary**: Displays a summary of available information for the associated keyword (previous keyword).

#### **session**

Displays HeNBGW sessions.

#### **all**

Displays information for all HeNB sessions.

#### **call-id***call\_id*

**call-id**: Specifies a Call Identification Number. *call\_id* is an eight-digit hexadecimal number.

#### **full**

Displays information on session state for matching sessions.



**qci *qci\_value***

**call-id:** Displays information for the HeNB associated with a specific QCI value. *qci\_value* is an integer between 1 and 9.

**s1-peer *s1\_peer\_address***

**s1-peer:** a specific S1 peer identified by the IP address of a peer eNodeB.

*s1\_peer\_address* is an IPv4 address in dotted-decimal notation or an IPv6 address in colon-separated-hexadecimal notation.

**summary**

This command displays summary information covering matching sessions.

**ue**

Displays UE information.

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to displays HeNBGW service related information.

**Example**

The following command displays information for all HeNB associations :

```
show henbgw henb-association all
```

# show henbgw-access-service

**Important**

In Release 20, 21.0 and 21.1, HeNBGW is not supported. This command must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

This command displays HeNBGW Access service related information.

**Product**

HeNBGW

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show hcnbgw-access-service { all | hcnb-association [ all | csg-id
csg_id_value| full | hcnbgw-access-service hcnbgw_acc_svc_name | peer-address
peer_ip_address | peer-id peer_id_value | summary | tai mcc mcc_val mnc mnc_val
tac ] | name name | statistics [ hcnbgw-access-service hcnbgw_acc_svc_name
| miscellaneous [ verbose ] | peer-id peer_id_valuesslap [ cause | [ verbose
] ] | sctp [ buffer [ sessmgr sessmgr_value] ] [ verbose ] ] [ | { grep
grep_options | more } ] }
```

```
hcnb-association [ all | csg-id csg_id_value| full | hcnbgw-access-service hcnbgw_acc_svc_name |
peer-address peer_ip_address | peer-id peer_id_value | summary | tai mcc mcc_val/mnc mnc_val/tac ] |
name name
```

**hcnb-association** : Displays information about HeNB associations.

**all**: Displays information about all HeNBGW Access services.

**csg-id**: Displays information about HeNB associations for the specified CSG ID.

*csg\_id\_value* is an integer between 0 and 4294967295.

**full**: Displays all available information for associated display or filter keyword (previous keyword).

**hcnbgw-access-service**: Displays information about HeNB associations with the specified HeNBGW Access service.

*hcnbgw\_acc\_svc\_name* is an alphanumeric string of 1 through 63 characters.

**peer-address**: Displays information about HeNB associations with the specified peer.

*peer\_ip\_address* is an IPv4 address in dotted-decimal notation or an IPv6 address in colon-separated-hexadecimal notation.

**peer-id**: Displays information about HeNB associations for the specified peer.

*peer\_id\_value* is an integer from 0 to 4294967295.

**summary**: Displays a summary of available information for associated display or filter keyword (previous keyword).

**tai**: Displays information about HeNB associations for the specified TAI.

**mcc**: Specifies a Mobile Country Code (MCC) as a three-digit number between 100 to 999.

*mcc\_val*is MCC value. MCC values of 000-099 are Reserved codes.

**mnc**: Specifies the Mobile National Code (MNC).

*mnc\_val*is MCC a two- or three-digit number between 00 to 999.

**tac**: Displays information about HeNB associations for the specified Type Allocation Code (TAC).

**miscellaneous** : Displays all available information for associated display or filter keyword (previous keyword).

```
namename statistics [ hcnbgw-access-service hcnbgw_acc_svc_name | miscellaneous [ verbose ] | peer-id
peer_id_valuesslap [ cause | [ verbose ] ] | sctp [ buffer [ sessmgr sessmgr_value
```

**name**: Displays information for specific HeNBGW Access service name.

*name*: is an alphanumeric string of 1 through 63 characters.

**statistics:** Displays HeNBGW Access service statistics

**miscellaneous :** Displays Miscellaneous statistics.

**s1ap:** Displays S1AP statistics.

**cause:** Displays S1AP cause statistics.

**setp:** Displays SCTP statistics.

**buffer:** Displays SCTP TX/RX buffer statistics.

**sessmgr:** Displays SCTP TX/RX buffer statistics on a specific sessmgr.

**verbose:** Specifies the verbosity.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display HeNBGW Access service related information.

### Example

The following command displays S1AP statistics:

```
show henbgw-access-service statistics s1ap
```

## show henbgw-network-service



### Important

In Release 20, 21.0 and 21.1, HeNBGW is not supported. This command must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

This command displays configuration for HeNBGW Network service.

### Product

HeNBGW

### Privilege

Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show henbgw-network-service { all | mme-association [ all | full |
henbgw-network-service henbgw_net_svc_name | peer-address peer_ip_address |
peer-id peer_id_value | summary ] | name name | statistics [
henbgw-network-service henbgw_net_svc_name | peer-id peer_id_value | slap [
```

```
cause | [ verbose ] ] | sctp [ buffer [ henbgwmgr henbgwmgr_value ] ] [
verbose ] ] [ | { grep grep_options | more } ] }
```

**henb-association** [ all | csg-id *csg\_id\_value* | full | henbgw-access-service *henbgw\_acc\_svc\_name* | peer-address *peer\_ip\_address* | peer-id *peer\_id\_value* | summary ] | name *name*

**mme-association** : Displays information about MME associations.

**all**: Displays all HeNBGW Network services.

**full**: Displays all available information for associated display or filter keyword (previous keyword).

**henbgw-network-service**: Displays information about HeNB associations with the specified HeNBGW Network service.

*henbgw\_net\_svc\_name* is an alphanumeric string of 1 through 63 characters.

**peer-address**: Displays information about HeNB associations with the specified peer.

*peer\_ip\_address* is an IPv4 address in dotted-decimal notation or an IPv6 address in colon-separated-hexadecimal notation.

**peer-id**: Displays information about HeNB associations for the specified peer.

*peer\_id\_value* is an integer from 0 to 4294967295.

**summary**: Displays a summary of available information for the associated display or filter keyword (previous keyword).

**name name statistics** [ henbgw-network-service *henbgw\_net\_svc\_name* | peer-id *peer\_id\_value* s1ap [ cause | [ verbose ] ] ] | sctp [ buffer [ henbgwmgr *sessmgr\_value*

**name**: Displays information for specific HeNBGW Network service name.

*name*: is an alphanumeric string of 1 through 63 characters.

**statistics**: Displays statistics for specified object.

**s1ap**: Displays S1AP statistics.

**cause**: Displays S1AP cause statistics.

**sctp**: Displays Sctp statistics.

**buffer** Displays Sctp TX/RX buffer statistics.

**henbgwmgr**: Displays Sctp TX/RX buffer statistics on a specific henbgwmgr.

**verbose**: Specifies the verbosity.

| { grep *grep\_options* | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

## Usage Guidelines

Use this command to display HeNBGW Network service related information.

**Example**

The following command displays S1AP Cause statistics :

```
show henbgw-network-service statistics slap cause
```

## show hexdump-module

This command displays hexdump module related information.

**Product**

ePDG  
SaMOG

**Privilege**

Administrator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show hexdump-module { file-space-usage | statistics } [ | { grep grep_options | more } ]
```

**file-space-usage**

Displays information about the file space usage of hexdump records.

**statistics**

Displays information on various statistics related to hexdump records.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display hexdump module related information.

**Example**

The following command displays information about the file space usage of hexdump records:

```
show hexdump-module file-space-usage
```

# show hnbgw access-control-db



## Important

In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Displays the white list of IMSI records in the Access Control database residing on Home NodeB Gateway (HNB-GW) service instances that control HNB and UE access to HNB-GW sessions.

## Product

HNBGW

## Privilege

Inspector

## Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

## Syntax Description

**show hnbgw access-control-db { hnbgw-service *hnbgw\_svc\_name* | imsi *imsi\_value* }**

### **hnbgw-service *hnbgw\_svc\_name***

Displays Access Control database records for an existing HNB-GW service specified as an alphanumeric string of 1 through 63 characters.



## Note

This keyword is not supported in StarOS 14.0 and higher releases.

### **imsi *imsi\_value***

Specifies the International Mobile Subscriber Identification (IMSI) number which is found on the Access Control database for the HNB-GW service.

*imsi\_value* is an integer consisting of the 3-digit MCC (Mobile Country Code), the 2- or 3-digit MNC (Mobile Network Code) followed by the MSIN (Mobile Subscriber Identification Number). The total IMSI value must not exceed 15 digits.

## Usage Guidelines

This command displays the white list IMSI records in an Access Control database residing on a system support all Home-NodeB Gateway (HNB-GW) service instances. The white list controls HNB and UE access to HNB-GW sessions. Access Control database records can be filtered by IMSI value.

## Example

The following command displays the information for registered IMSIs and their status in the HNB-GW database:

```
show hnbgw access-control-db imsi
```



**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show hnbgw counters



**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Displays the session counter information for Home-NodeB Gateway (HNB-GW) services connected on this system.

**Product** HNBGW

**Privilege** Inspector

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **show hnbgw counters** [ **hnbgw-service** *hnbgw\_svc\_name* | **hnbid** *hnb\_identifier* ] [ | { **grep** *grep\_options* | **more** } ]

### **hnbgw-service** *hnbgw\_svc\_name*

Filters the counter display based on an existing HNB-GW service name specified as an alphanumeric string of 1 through 63 characters.

### **hnbid** *hnb\_identifier*

Filters the counter display based on a Home-NodeB identifier specified as an alphanumeric string of 1 through 255 characters.

### { **grep** *grep\_options* | **more** }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *Command Line Interface Overview* chapter.

**Usage Guidelines** Use this command to view the session counter information for HNB-GW services configured and HNBs connected on this system.

### **Example**

The following command displays the counters for the HNB-GW service named *hnbgw1*:

```
show hnbgw counter hnbgw-service hnbgw1
```




---

**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show hnbgw-global




---

**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

---

Displays the global configuration parameters for configured HNBGW service(s) on this system.

---

**Product** HNBGW

---

**Privilege** Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show hnbgw-global`

---

**Usage Guidelines** Use this command to view the global configuration parameters set for all HNBGW service(s) on this system.

### Example

The following command displays the global configuration parameters applicable for all HNBGW services configured on this system:

```
show hnbgw-global
```




---

**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show hnbgw sessions




---

**Important** In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

---



Displays the active/dormant session information about registered HNB(s) on Home-NodeB Gateway (HNB-GW) service instances configured and running on this system based on different filter criteria.

**Product** HNBGW

**Privilege** Inspector

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **show hnbgw sessions** [**full** | **summary**] [**all**] [**address** *hnb\_ip\_address* | **cell-id** *cell\_id* | **hnb-access-mode** {**closed**| **hybrid** | **open** } | **hnb-local-id** *hnb\_id* | **hnbgw-service** *hnbgw\_svc\_name* [ **hnb-access-mode** { **closed** | **hybrid** | **open** }]| **hnbid** *hnb\_glbl\_id* | **mcc** *mcc* | **mnc** *mnc* [**lac** *lac* | **rac** *rac* | **rnc** *rnc*]] [ | {**grep** *grep\_options* | **more** }]

#### **full**

Displays the full information for a specific registered HNB session(s) on an HNB-GW service instance running on the system. The display can be filtered based on given filtering criteria.

#### **summary**

Displays summarized information for a specific registered HNB session(s) on an HNB-GW service instance running on the system. The display can be filtered based on given filtering criteria.

#### **all**

Displays summarized information for all registered HNB sessions on an HNB-GW service instance running on the system. The display can be filtered based on given filtering criteria.

#### **address** *hnb\_ip\_address*

Filters the display of full or summarized session statistics to show only HNB session(s) based on the registered HNB IP address expressed in IPv4 dotted-decimal notation.

#### **cell-id** *cell\_id*

Filters the display of full or summarized session statistics to show only HNB session(s) based on the registered Femto cell ID where the user/subscriber is geographically located. and must be an integer from 0 through 268435455. *cell\_id* is an integer from 0 through 268435455.

#### **hnb-access-mode** {**closed** | **open** | **hybrid** }

Filters the display of full or summarized session statistics to show only HNB session(s) based on the HNB access mode in an HNB-GW service instance.

- **closed** filters the session statistics for closed HNBs connected with HNB-GW service instance in Closed Access mode.
- **hybrid** filters the session statistics for hybrid HNBs connected with HNB-GW service instance in Hybrid Access mode.

- **open** filters the session statistics for open HNBs connected with HNB-GW service instance in Open Access mode.

### **hnb-local-id** *hnb\_id*

Filters the display of full or summarized session statistics to show only HNB session(s) based on the registered local ID of HNB specified as an integer from 1 through 25.

### **hnbgw-service** *hnbgw\_svc\_name*

Filters the display of session statistics to show only registered HNB session(s) based on an existing HNB-GW service name specified as an alphanumeric string of 1 through 63 characters.

This can be further filtered by using access-mode criteria: Closed, Hybrid, or Open.

### **hnbid** *hnb\_glbl\_id*

Displays summarized or full information of HNB session(s) based on the registered global ID of HNB specified as an integer between 1 through 255.

### **mcc** *mcc*

Displays summary information of HNB session(s) based on the registered Mobile Country Code (MCC) identification number of the UE specified as an integer between 101 through 999.

### **mnc** *mnc*

Displays summarized or full information of HNB session(s) based on the registered Mobile Network Code (MCC) identification number of the UE specified as a 2- or 3-digit integer between 00 through 999.

### **lac** *lac*

Displays summarized or full information for HNB session(s) based on the registered Location Area Code (LAC) identification number of the UE specified as an integer between 1 through 65535.

### **rac** *rac*

Displays summarized or full information for HNB session(s) based on the registered Radio Access Code (RAC) identification number of the UE specified as an integer between 1 through 255.

### **rnc** *rnc*

Displays summarized or full information for HNB session(s) based on the registered Radio Network Code (RAC) identification number of the HNB specified as an integer between 1 through 65535.

### **| { grep grep\_options | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *Command Line Interface Overview* chapter.

## Usage Guidelines

Use this command to view the session statistics of all or specific registered HNB session(s) or in selected part of user session for HNB-GW services configured and running on this system.

**Example**

The following command displays summarized session statistics for all registered HNBs on the HNB-GW service named *hnbgw1*:

```
show hnbgw sessions summary hnbgw-service hnbgw1
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show hnbgw statistics hnbgw-service

**Important**

In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Displays the session statistics for Home-NodeB Gateway (HNB-GW) services configured and running on this system.

**Product**

HNB-GW

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show hnbgw statistics [ gtpu-only ] [ hnb-access-mode { closed | hybrid
| open } ] [ hnbgw-service hnbgw_svc_name [ gtpu-only | hnb-access-mode {
closed | hybrid | open } | hnbap-only | ipne-only | paging-only |
ranap-only | rtp-only | rua-only | sabp-only | sctp-only ] ] [ hnbid
hnb_identifier ] [ hnbap-only | ipne-only | paging-only | ranap-only | rua-only
| sccp-only | sctp-only ] ] [ verbose] [ | { grep grep_options | more } ]
```

**gtpu-only**

Displays Forwarded GTPU Pkt statistics for selected HNB/HNBGW Service.

**hnb-access-mode { closed | hybrid | open }**

Displays the session statistics of an existing HNB-GW service based on access mode filters. Other supported filters are:

- **closed**: shows the statistics of only those UEs which are connected through Closed HNBs to the HNB-GW services on a chassis. This command applies to all Closed HNB sessions on a chassis. If any other criteria specified it will filter the statistics based on given criteria.

- **hybrid**: shows the statistics of only those UEs which are connected through Hybrid HNBs to the HNB-GW services on a chassis. This command applies to all Closed HNB sessions on a chassis. If any other criteria specified it will filter the statistics based on given criteria.
- **open**: shows the statistics of only those UEs which are connected through Open HNBs to the HNB-GW services on a chassis. This command applies to all Closed HNB sessions on a chassis. If any other criteria specified it will filter the statistics based on given criteria.

**hnbgw-service *hnbgw\_svc\_name***

Filters the display of session statistics for an existing HNB-GW service name specified as an alphanumeric string of 1 through 63 characters.

**hnbap-only**

Filters the display of session statistics to show only Home NodeB Application Part (HNBAP) traffic for the selected HNB-GW service which is configured and running on this system.

**ipne-only**

Filters the display of session statistics to show only IPNE for selected HNBGW Service which is configured and running on this system.

**paging-only**

Filters the display of Paging statistics for selected HNBGW Service.

**ranap-only**

Filters the display of session statistics to show only Radio Access Network Application Protocol (RANAP) traffic for the selected HNB-GW service which is configured and running on this system.

**rua-only**

Filters the display of session statistics to show only RANAP User Adaptation (RUA) traffic for the selected HNB-GW service which is configured and running on this system.

**sccp-only**

Filters the display of session statistics to show only Signaling Connection Control Part (SCCP) traffic for the selected HNB-GW service which is configured and running on this system.

**sctp-only**

Filters the display of session statistics to show only Stream Control Transmission Protocol (SCTP) traffic for selected HNB-GW service which is configured and running on this system.

**verbose**

Displays detailed statistics for all sessions on HNB-GW services or for a selected filtered and named HNB-GW service which is configured and running on this system.

**{ `grep` *grep\_options* | `more` }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to view the session statistics for overall session or in selected part of user session for HNB-GW services configured and running on this system.

### Example

The following command displays session statistics for the HNBAP part of session details for the HNB-GW service named *hnbgw1*:

```
show hnbgw statistics hnbgw-service hnbgw1 hnbap-only
```

The following command displays session statistics for the RANAP part of session with maximum details for the HNB-GW service named *hnbgw1*:

```
show hnbgw statistics hnbgw-service hnbgw1 ranap-only verbose
```

## show hnbgw statistics hnbid



### Important

In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Displays the session statistics for Home-NodeB (HNB) connected to an HNB-GW service on this system.

### Product

HNBGW

### Privilege

Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show hnbgw statistics hnbid hnb_identifier [ hnbap-only | ranap-only | rua-only ] [ verbose ] [ | { grep grep_options | more } ]
```

#### **hnbid** *hnb\_identifier*

Filters the display of session statistics based on an existing Home-NodeB identifier specified as an alphanumeric string of 1 through 255 characters.

**hnbap-only**

Filters the display of session statistics display to show only Home NodeB Application Part (HNBAP) traffic for the selected HNB which is connected to this system through HNB-GW service.

**ranap-only**

Filters the display of session statistics display to show only Radio Access Network Application Protocol (RANAP) traffic for the selected HNB which is connected to this system through HNB-GW service.

**rua-only**

Filters the display of session statistics display to show only RANAP User Adaptation (RUA) traffic for the selected HNB which is connected to this system through HNB-GW service.

**verbose**

Displays detailed statistics for all HNB sessions or for the selected filter and HNB which is connected to this system through HNB-GW service.

**{ `grep` *grep\_options* | `more` }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view the session statistics for overall session or in selected part of user session for selected HNB which is connected to this system through HNB-GW service.

**Example**

The following command displays session statistics for the HNBAP part of session details for the HNB identified as *hnb112234* on this system:

```
show hnbgw statistics hnbid hnb112234 hnbap-only
```

The following command displays detailed session statistics for the RANAP part of session details for the HNB identified as *hnb112234* on this system:

```
show hnbgw statistics hnbid hnb112234 ranap-only verbose
```

# show hnbgw-service

**Important**

In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Displays the configuration details for configured HNBGW service(s) on this system.

---

**Product** HNBGW

---

**Privilege** Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show hnbgw-service { all | hnbgw-service *hnbgw\_svc\_name* }**

#### **all**

Displays configuration and other default parameters for all HNB-GW service configured on this system.

#### **hnbgw-service *hnbgw\_svc\_name***

Displays configuration and default parameters for an existing HNB-GW service name specified as an alphanumeric string of 1 through 63 characters.

---

**Usage Guidelines** Use this command to view the configuration and service parameters set for all or any specific HNB-GW service(s) on this system.

#### **Example**

The following command displays configuration parameters for all HNB-GW services configured on this system:

```
show hnbgw-service all
```




---

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show hsgw-service

Displays information for HRPD Serving Gateway (HSGW) services on this system.

---

**Product** HSGW

---

**Privilege** Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show hsgw-service { all | name *service\_name* | statistics { all | name *service\_name* } } [ dns-stats | pcf-status [ address *IPv4\_address* | filter { all |**

```
icmp-monitored | no-calls | summary | up } ] ] [ | { grep grep_options |
more } ]
```

**all**

Displays configuration information for all HSGW services configured on this system.

**name *service\_name***

Displays configuration information for an existing HSGW service specified as an alphanumeric string of 1 through 63 characters.

**statistics**

Displays node-level statistics for the HSGW.

**dns-stats**

Displays information related to DNS P-GW selection for load balancing using DNS SRV lookup.

**pcf-status**

Displays information about the status of Packet Control Functions (PCFs) being monitored.

**address *IPv4\_address***

Displays status information for the specified PCF.

*IPv4\_address* must be specified using IPv4 dotted-decimal notation.

**filter { all | icmp-monitored | no-calls | summary | up }**

Filters the PCF status information. Must be followed by the filter to be applied.

**all**: Shows all the PCFs.

**icmp-monitored**: Shows only PCFs which are ICMP monitored.

**no-calls**: Shows only PCFs which has no active sessions.

**summary**: Shows only a summary of the status of the PCFs.

**up**: Shows only PCFs which are alive.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view configuration information for HSGW services on this system.



**Example**

The following command displays service statistics for the HSGW service named *hsgw1*:

```
show hsgw-service name hsgw1
```

## show hss-peer-service

Displays service, session, and statistics information for Home Subscriber Server (HSS) peer services configured on this system.

**Product**

MME

**Privilege**

Inspector

**Syntax Description**

```
show hss-peer-service { service { all | name name } | session { all |
callid id | full | mdn mdn | nai nai | summary } | statistics { all | service
name | summary } } [ | { grep grep_options | more } ]
```

**service { all | name *name* }**

Displays HSS peer service statistics for HSS peer services configured on this system.

**all**: Displays HSS peer service statistics for all configured HSS peer services on this system.

**name *name***: Displays HSS peer service statistics for an existing HSS peer service specified as an alphanumeric string of 1 through 63 characters.

**session { all | callid *id* | full | mdn *mdn* | nai *nai* | summary }**

Displays HSS peer service statistics for sessions on this system.

**all**: Displays HSS peer service statistics for all sessions on this system.

This keyword is also used to further filter the **full** and **summary** options.

**callid *id***: Displays summarized or detailed statistics of HSS peer service sessions running and filtered on the basis of the call identifier specified as an 8-digit hexadecimal number.

This keyword is also used to further filter the **full** and **summary** options.

**mdn *mdn***: Displays summarized or detailed statistics of MME sessions running and filtered on the basis of an existing Mobile Directory Number (MDN) expressed as an alphanumeric string of 1 through 100 characters.

This keyword is also used to further filter the **full** and **summary** options.

**nai *nai***: Displays summarized or detailed statistics of MME-HSS sessions running and filtered on the basis of an existing Network Access Identifier (NAI) expressed as an alphanumeric string of 1 through 128 characters.

This keyword is also used to further filter the **full** and **summary** options.

**summary**: Displays a summarized output of session information. This keyword can be further filtered by adding the following options:

- **full**

- **callid** *id*
- **mdn** *mdn*
- **nai** *nai*

### **statistics { all | service *name* | summary }**

Displays statistics for HSS peer services configured on this system.

**all**: Displays statistics for all HSS peer services configured on this system.

**service *name***: Displays statistics for an existing HSS peer service expressed as an alphanumeric string of 1 through 63 characters.

**summary**: Displays summarized statistics for all HSS peer services configured on this system.

### **| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *CLI Overview* chapter of the *Command Line Interface Reference*.

#### Usage Guidelines

Use this command to display service, session, and statistics information for HSS peer services configured on this system.

#### Example

The following command displays HSS peer service information and statistics for a session with a call ID of *08f11fa4*:

```
show hss-peer-service sessions full callid 08f11fa4
```

## show imei-profile

Displays information for configured International Mobile Equipment Identity (IMEI) profiles.

#### Product

SGSN

#### Privilege

Inspector

#### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

#### Syntax Description

```
show imei-profile { all | full { all | name imei_name } | name imei_name } [
  | { grep grep_options | more } ]
```

#### **all**

Lists all IMEI profiles configured on the system.

**full { all | name *apn\_name* }**

**full:** Instructs the system to display all information in the IMEI profile(s).

**all:** Displays a full set of information for all IMEI profiles configured on the system.

**name *imei\_name*:** Displays a full set of information for a specific IMEI profile.

*apn\_name:* Must be an existing IMEI profile expressed as an alphanumeric string of 1 through 64 characters.

**name *imei\_name***

Displays information for a specific IMEI profile expressed as an alphanumeric string of 1 through 64 characters.

**{ *grep grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display information for IMEI profiles configured on the system. APN profiles are configured through the global configuration mode and in the IMEI profile configuration mode. For more information regarding IMEI profile commands, refer to the *IMEI Profile Configuration Mode Commands* chapter.

### Example

The following command displays all available information for an IMEI profile named *imeiprofl*:

```
show imei-profile full name imeiprofl
```

## show ims-authorization policy-control

Displays information and statistics specific to the policy control in IP Multimedia Subsystem (IMS) authorization service.

### Product

SCM  
GGSN  
IMS  
P-GW  
SAEGW

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show ims-authorization policy-control statistics [ service ims_auth_svc_name
| server { ip-address ip_address [ port port_value ] | name server_name } ] [
| { grep grep_options | more } ]
```

**statistics**

Displays the total collected statistics of all policy control parameters of IMS authorization service sessions since the last system **restart** or **clear** command.

**service *ims\_auth\_svc\_name***

Displays the total collected statistics of all IMS authorization sessions processed by a specific IMS authorization service since the last system restart or clear command. *ims\_auth\_svc\_name* must be an existing IMS authorization service name, expressed as an alphanumeric string of 1 through 64 characters.

**server { ip-address *ip\_address* [ port *port\_value* ] | name *server\_name* }**

Displays the server-level message statistics and the server IP address.

Specify the PCRF server name (1 through 64 alphanumeric characters), or server IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**{ { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display information and statistics about policy control configuration in existing IMS authorization services.

**Example**

The following command displays the existing IMS authorization service name *ims\_auth\_gx1* on the system:

```
show ims-authorization policy-control statistics service ims_auth_gx1
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show ims-authorization policy-control misc-info

Displays the maximum backpressure information.

**Product**

GGSN

P-GW

<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<pre><b>show ims-authorization policy-control misc-info max-backpressure [ all   facility sessmgr instance instance_number ] [   { grep grep_options   more } ]</b></pre> <p><b>all</b> Displays the max-backpressure count among all active session manager instances.</p> <p><b>facility sessmgr instanceinstance_number</b> Displays logged events for specific facility. That is, it will display the maximum backpressure count on that specific session manager instance. <i>instance_number</i> must be an existing IMS authorization service name, expressed as an alphanumeric string of 0 to 10000000 characters.</p> <p><b>{ grep grep_options   more }</b> Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of <b>grep</b> and <b>more</b>, refer to the <i>Regulating a Command's Output</i> section of the <i>Command Line Interface Overview</i> chapter.</p>
<b>Usage Guidelines</b>	Use this command to display the maximum backpressure at a particular session manager instance or at all instances, and the time stamp at which maximum backpressure was seen.

**Example**

The following command displays the maximum backpressure information for *session1* facility on the system:

```
show ims-authorization policy-control misc-info max-backpressure facility
sessmgr instance session1
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show ims-authorization policy-gate

Displays information of installed Policy Gates for specific subscriber in an IP Multimedia Subsystem (IMS) authorization (IMSA) service.

**Product**

SCM  
 GGSN  
 IMS  
 P-GW  
 SAEGW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show ims-authorization policy-gate { { status [ summary | full ] [ { imsi
  imsi_value [ nsapi nsapi_value ] } | callid call_id | { ims-auth-service
  ims_auth_svc } [ rulename rule_name ] } | { counters [ all | { imsi imsi_value
  [ nsapi nsapi_value ] } | { rulename rule_name } | { callid call_id } ] } [ | {
  grep grep_options | more } ] ]
```

**status [ summary | full ]**

Displays the status of the installed policy gates and their flow definitions along with the run-time status in an IMS authorization service based on the specified criteria.

**summary**: Limits the display to a summary on the status of the installed policy gates and their flow definitions along with their run-time status in an IMS authorization service based on the specified criteria.

**full**: Displays the full information on status of the installed policy gates and their flow definitions along with their run-time status in an IMS authorization service based on the specified criteria.

**counters all**

Displays the counters/statistics of the installed policy gates and their flow definitions along with their run-time status in an IMS authorization service based on the specified criteria.

**all** displays all counters of the installed gates and their flow definitions along with their run-time status in an IMS authorization service based on the specified criteria.

**imsi imsi\_value [ nsapi nsapi\_value ]**

Displays all of the counters/status of the installed policy gates and their flow definitions along with the run-time status in an IMS authorization service based on the International Mobile Subscriber Identity (IMSI).

**nsapi nsapi\_value** specifies the Network Service Access Point Identifier (NSAPI) and limits the display to a single PDP context of the subscriber.

**callid call\_id**

Displays all of the counters/status of the installed policy gates and their flow definitions along with their run-time status in an IMS authorization service based on the call identifier.

**ims-auth-service *ims\_auth\_svc***

Displays the status of the installed policy gates and their flow definitions along with their run-time status in the named IMS authorization service.

**rulename *rule\_name***

Displays all of the counters/status of the installed policy gates and their flow definitions along with their run-time status in an IMS authorization service based on the named dynamic charging rule.

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Please refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference* for details on the usage of **grep** and **more**.

**Usage Guidelines**

Use this command to display information/statistics/counters about all of the installed policy gates and their flow definitions along with the run-time status with specified criteria and filters in existing IMS authorization services.

**Example**

The following command displays the full status of the installed policy gates in an existing IMS authorization service on the system:

```
show ims-authorization policy-gate status full
```

The following command displays the all counters of the installed policy gates in an existing IMS authorization service on the system:

```
show ims-authorization policy-gate counters all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show ims-authorization servers

Displays information and statistics specific to the authorization servers used for IP Multimedia Subsystem (IMS) authorization (IMSA) service.

**Product**

SCM  
GGSN  
IMS  
P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show ims-authorization servers [ ims-auth-service ims_auth_svc_name [ | {  
grep grep_options | more } ] ]
```

```
server [ ims-auth-service ims_auth_svc_name ]
```

Displays the information and statistics for all authorization servers configured within an IMS authorization service in a system.

**ims-auth-service *ims\_auth\_svc\_name***: Displays the configured authorization servers for IMS authorization within the named IMS authorization service.

```
| { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Please refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference* for details on the usage of **grep** and **more**.

**Usage Guidelines**

Use this command to display information and statistics about IMS authorization servers configured on a system or IMS authorization service.

**Example**

The following command displays the information and statistics of the authorization servers in the IMS authorization service named in *ims\_auth\_gx1*:

```
show ims-authorization servers ims-auth-service ims_auth_gx1
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show ims-authorization service

Displays information, configuration, and statistics of all/specific IP Multimedia Subsystem (IMS) authorization (IMSA) service.

**Product**

GGSN

P-GW

SAEGW

SCM

**Privilege**

Security Administrator, Administrator



**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show ims-authorization service { { all [ verbose ] | name ims_auth_svc_name
  [ p-cscf { all | ip_address ipv4/ipv6_address | summary ] } | { statistics
  [ all | name ims_auth_svc_name ] [ verbose ] } [ | { grep grep_options | more
  } ]
```

**all [ verbose ]**

Displays information and configuration for all configured IMS authorization services with a single line of information for each IMS authorization service.

**verbose:** Displays all information and configuration data for all IMS authorization services configured on system.

**name *ims\_auth\_svc\_name* [ p-cscf { all | ip\_address *ipv4/ipv6\_address***

Displays the information, statistics, and configuration data for the named IMS authorization service. If the optional keyword is configured, this command displays the statistics information of all P-CSCF servers or specific server.

**summary**

Displays summarized information and configuration data for all IMS authorization services configured in a system.

**statistics [ all | name *ims\_auth\_svc\_name* ] [ verbose ]**

Displays the IMS Authorization service statistics including following information:

- Initial authorization procedures
- Re-authorization procedures initiated by us
- Re-authorization procedures initiated by servers
- Various failure statistics

If no criteria are specified, only summarized statistics for all IMS Authorization services are displayed

- **all:** displays individual statistics for every IMS authorization service configured on system.
- **name *ims\_auth\_svc\_name*:** Displays the statistics for the IMS authorization service named in *ims\_auth\_svc\_name*
- **verbose:** displays detailed statistics for a configured IMS authorization service.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Please refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference* for details on the usage of **grep** and **more**.

### Usage Guidelines

Use this command to display the status, counters and configuration. for an IMS Authorization service. The status includes the state of a server table switchover. The Statistics option displays information about various processes.

### Example

The following command displays the information and configuration data of the IMS authorization service named in *ims\_auth\_gx1*:

```
show ims-authorization service name ims_auth_gx1
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show ims-authorization sessions

Displays information, configuration, and statistics of sessions active in an IP Multimedia Subsystem (IMS) authorization (IMSA) service.

### Product

SCM  
GGSN  
IMS  
P-GW  
SAEGW

### Privilege

Security Administrator, Administrator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show ims-authorization sessions [ all | apn apn_name | callid call_id |
facility sessmgr instance instance_no | full | ggsn-only | ims-auth-service
ims_auth_svc_name | imsi imsi_value [ nsapi nsapi_value ] | ip-address ip_address
| local-sessions | remote-sessions | summary ] [ | { grep grep_options |
more } ] ]
```

### all

Displays information and configuration for all sessions running in IMS authorization services with a single line of information for each IMS authorization session.

**apn *apn\_name***

Displays all of the counters/status for the running services in an IMS authorization service based on the specified Access Point Name (APN).

**callid *call\_id***

Displays all of the counters/status for the running services in IMS authorization service based on the named call identifier.

**facility sessmgr instance *instance\_no***

Displays the IMS authorization sessions at the session manager instance level.

**full**

Displays complete information and configuration data for all sessions in IMS authorization services configured in a system.

**ggsn-only**

Displays GGSN-specific information in addition to detailed information about the session.

**ims-auth-service *ims\_auth\_svc\_name***

Displays the information, statistics, and configuration data for sessions in the named IMS authorization service.

**imsi *imsi\_value* [ *nsapi nsapi\_value* ]**

Displays all of the counters/status of the running services in an IMS authorization service based on the specified International Mobile Subscriber Identity (IMSI) and Network Service Access Point Identifier (NSAPI). The display is limited to a single PDP context of the subscriber.

**ip-address *ip\_address***

Displays all of the counters/status for the running services in IMS authorization service based on the specified host IP address.

**local-sessions**

Displays the IMS authorization sessions that are associated with local-policy.

**remote-sessions**

Displays the IMS authorization sessions that are associated with PCRF.

**summary**

Displays summarized information and configuration data for all IMS authorization services configured in a system.

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Please refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference* for details on the usage of **grep** and **more**.

### Usage Guidelines

Use this command to display the sessions running under IMS Authorization service on a system with different filter criteria.

### Example

The following command displays the information and statistical data for a session in an IMS authorization service:

```
show ims-authorization sessions full
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show instance-logging

Displays the instance numbers for all currently enabled, facility-specific log instances.

### Product

All

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show instance-logging facility facility_name [ | { grep grep_options | more } ]
```

#### **facility** *facility\_name*

Specifies the facility for which instance-level logging has been enabled. *facility\_name* can be aaamgr, hamgr or sessmgr.

#### [ { **grep** *grep\_options* | **more** }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

### Usage Guidelines

Displays the instance numbers for all currently enabled, facility-specific log instances. These instances have been previously enabled via the Exec mode **logging filter enable facility** command.

**Example**

The following command displays instance-specific logging enabled for the sessmgr facility:

```
show instance-logging facility sessmgr
```

## show inventory

Displays Unique Device Identifier (UDI) information for all hardware in the system for which a UDI is available.

---

**Product** All

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show inventory [ | { grep grep_options | more } ]`

`{ grep grep_options | more }`

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Displays UDI information (card/item description, Cisco PID, serial number) for all hardware installed in this system.

**Example**

The following command displays UDI information for all cards in the system:

```
show inventory
```

## show ip access-group statistics

Displays statistics for each rule in an access control group.

---

**Product** HA

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show ip access-group statistics [ | { grep grep_options | more } ]`

`| { grep grep_options | more }`

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines** Use this command to display the configured access control groups in the current context.

#### Example

The following command displays the contents of an access control group named *ACG\_4*:

```
show ip access-list ACG_4
```

## show ip access-list

Displays the information for all Access Control Lists (ACLs) or the named ACL. With no keyword supplied, a list of all access lists and their entries is displayed.

---

**Product** HA

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show ip access-list list_name [ | { grep grep_options | more } ]`

*list\_name*

Specifies the name of an existing ACL configured in the current context as an alphanumeric string of 1 through 47 characters.

`| { grep grep_options | more }`

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines** Use this command to display the configured ACLs in the current context.

**Example**

The following command displays the contents of an ACL named *ACL\_4*:

```
show ip access-list ACL_4
```

# show ip arp

Displays the ARP table or the ARP information associated with the specified IP address.

**Important**

When it restarts, the VPN Manager removes all interfaces from the kernel; the kernel then removes all ARP entries. When this happens, the NPU still holds all of the ARP entries so that there is no traffic disruption. From a user point of view, **show ip arp** is broken since this command gathers information from the kernel and not the NPU.

**Product**

HA

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show ip arp [ ip_address | vrf vrf_name ] [ | { grep grep_options | more } ]
```

***ip\_address***

Specifies an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

***| vrf vrf\_name***

Displays information for an existing VPN Routing and Forwarding (VRF) name expressed as an alphanumeric string of 1 through 63 characters.

***{ grep grep\_options | more }***

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display the configured ACLs in the current context.

**Example**

The following command displays the contents of an ACL named *ACL\_4*:

```
show ip access-list ACL_4
```

## show ip as-path-access-list

Displays the contents of a Border Gateway Protocol (BGP) router Autonomous System (AS) path access list in the current context.

---

**Product** HA

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show ip as-path-access-list list_name [ | { grep grep_options | more } ]`

***list\_name***

Specifies the name of an existing AS path access list configured in the current context as an alphanumeric string of 1 through 79 characters.

***{ grep grep\_options | more }***

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines** Use this command to display the configured entries for the specified BGP router AS path access list in the current context.

**Example**

The following command displays the contents of an AS path access list named *ASlist1*:

```
show ip as-path-access-list ASlist1
```

## show ip bgp

Displays Border Gateway Protocol (BGP) information for the current context.

---

**Product** HA

---

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



**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show ip bgp [ ip_address/mask | debugging | filter-list list_name | neighbors
[ ip_address ] | route-map map_name | vpn4 [ all [ ip_address/mask | neighbors
| summary ] | route-distinguisher { ipv4_address | asn_value } rd_value | vrf
vrf_name [ ip_address/mask | neighbors | summary ] | vpn6 [ all [ ipv4_address |
neighbors | summary ] | route-distinguisher { ipv4_address | asn_value } rd_value
| vrf vrf-name [ ip_address/mask | neighbors | summary ] ] [ | { grep grep_options
| more } ]
```

***ip\_address/mask***

Specifies the IP address and netmask bits for the network for which information should be displayed. The IP address and mask is the number of subnet bits, representing a subnet mask in CIDR notation. These must be entered in the IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal CIDR notation.

**debugging**

Displays debug flags that are enabled.

**filter-list *list\_name***

Displays routes that match the specified filter list.

**neighbors [*ip\_address*]**

Displays information for all neighbors or a neighbor specified as an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**route-map *map\_name***

Displays routes that match the specified route-map.

**summary**

Displays summary BGP information.

```
| vpn4 [ all [ ip_address/mask | neighbors | summary ] | route-distinguisher { ipv4_address | asn_value }
rd_value | vrf vrf_name [ ip_address/mask | neighbors | summary ]
```

Displays all VPNv4 routing data.

- **all**: Displays all VPNv4 routing information. If this is specified, the information displayed is gathered from all the VRF's known to BGP and displayed. It could contain the list of neighbors, the list of networks, or a particular network.
- **neighbors**: Displays neighbor information for the all the VRFs including the default VRF or for the VRF with a matching RD value.
- **summary**: Displays summary information of neighbors for all the VRFs including the default VRF or for the VRF with a matching RD value.

- **route-distinguisher** { *ipv4\_address* | *asn\_value* } *rd\_value*: Displays information about the route distinguisher. Where
  - *ipv4\_address*: Specifies an IP address in IPv4 dotted-decimal notation.
  - *asn\_value*: Specifies an autonomous system number as an integer from 0 through 65535.
  - *rd\_value*: Specifies a route distinguisher value as an integer from 0 through 4294967295.
- **vrf** *vrf\_name* [ *ipv4\_address/mask* | **neighbors** | **summary** ]: Displays information about the VRF. Where
  - *vrf\_name*: Specifies the name of the VRF as an alphanumeric string of 1 through 63 characters.
  - *ip\_address/mask*: Specifies an IP address in IPv4 dotted-decimal CIDR notation.
  - **neighbors**: Displays neighbor information for the all the VRFs including the default VRF or for the VRF with a matching RD value.
  - **summary**: Displays summary information of neighbors for all the VRFs including the default VRF or for the VRF with a matching RD value.

**| vpnv6 [ all [ *ipv4\_address* | **neighbors** | **summary** ] | route-distinguisher { *ipv4\_address* | *asn\_value* } *rd\_value* | vrf *vrf\_name* [ *ip\_address/mask* | **neighbors** | **summary** ] ]**

Displays all VPNv6 routing data.

- **all**: Displays all VPNv6 routing information. If this is specified, the information displayed is gathered from all the VRF's known to BGP and displayed. It could contain the list of neighbors, the list of networks, or a particular network.
- **neighbors**: Displays neighbor information for the all the VRFs including the default VRF or for the VRF with a matching RD value.
- **summary**: Displays summary information of neighbors for all the VRFs including the default VRF or for the VRF with a matching RD value.
- **route-distinguisher** { *ipv4\_address* | *asn\_value* } *rd\_value*: Displays information about the route distinguisher. Where
  - *ipv4\_address*: Specifies an IP address in IPv4 dotted-decimal notation.
  - *asn\_value*: Specifies an autonomous system number as an integer from 0 through 65535.
  - *rd\_value*: Specifies a route distinguisher value as an integer from 0 through 4294967295.
- **vrf** *vrf\_name* [ *ipv4\_address/mask* | **neighbors** | **summary** ]: Displays information about the VRF. Where
  - *vrf\_name*: Specifies the name of the VRF as an alphanumeric string of 1 through 63 characters.
  - *ip\_address/mask*: Specifies an IP address in IPv4 dotted-decimal CIDR notation.
  - **neighbors**: Displays neighbor information for the all the VRFs including the default VRF or for the VRF with a matching RD value.
  - **summary**: Displays summary information of neighbors for all the VRFs including the default VRF or for the VRF with a matching RD value.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command display to BGP information for the current context.

### Example

The following command displays information for all BGP neighbors:

```
show ip bgp neighbors
```

## show ip framed-prefixes

Displays the framed-prefixes along with session-id, vrf-name and pool-name. The command will also display the total number of framed-prefixes matching the filtering criteria.

**Product** All

**Privilege** Inspector

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **show ip framed-prefixes [ sess-id *session\_identifier* | vrf *vrf\_identifier* ]**

### **sess-id *session\_identifier***

Displays framed-prefixes added by a specific session.

*session\_identifier* must be an integer from 1 to 1152.

### **vrf *vrf\_identifier***

Displays VRF specific routing information.

*vrf\_identifier* must be an alphanumeric string of 1 through 63 characters.

### Usage Guidelines

Use this command to display the framed-prefixes. This command also enables filtering of framed-prefixes based on vrf-name and/or session-id to the display. The display will show framed-prefixes along with session-id, vrf-name, and pool-name. The command will also display the total number of framed-prefixes matching the filtering criteria.

### Example

The following command displays ip framed-prefixes by a specific session.

```
show ip framed-prefixes sess-id session_idenfier
```

# show ip igmp group

Displays Internet Group Management Protocol (IGMP) information for all groups in a context or a specific IP address.

---

**Product** All

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show ip igmp group [ ip_address | all ] [ | { grep grep_options | more } ]`

## *ip\_address*

Displays IGMP information for the IP address specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

## **all**

Displays information for all IGMP groups associated with this context.

## | { **grep** *grep\_options* | **more** }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines** Use this command to display IGMP group information.

## **Example**

To display general IGMP information for all groups in this context, enter the following command;

```
show ip igmp all
```

# show ip interface

Displays statistical and configuration information for the IPv4-based interfaces, including a Virtual Routing and Forwarding (VRF) table for a specific context.

---

**Product** All

---

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

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show ip interface [ vrf vrf-name ] [ name intfc_name [ tunnel [ gre-keepalive ] ] [ summary ] [ vrf vrf-name ] [ | { grep grep_options | more } ]
```

**name** *intfc\_name*

Displays information for an existing interface specified as an alphanumeric string of 1 through 79 characters. If no interface name is specified, the information for all IP interfaces is displayed.

**summary**

Displays summarized information about requested IP interfaces.

**tunnel** [ **gre-keepalive** ]

Filters the IP interface information for GRE/IP-in-IP tunnel type interfaces.

**gre-keepalive**: Displays the keepalive information for a generic routing encapsulation (GRE) tunnel configured with this IP interface.

**vrf** *vrf\_name*

Displays Virtual Routing and Forwarding (VRF) routing information for an existing VRF specified as an alphanumeric string of 1 through 63 characters.

**{ grep** *grep\_options* | **more** }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display the summarized of detailed configuration and statistical information for a configured IP interface. This information can be used to verify and/or troubleshoot communication difficulties between to a remote host/node.

**Example**

The following command displays the interface information, including statistics, for the IP interface *Interface\_1*.

```
show ip interface Interface_1 statistics
```

The following command displays the GRE keepalive information for an IP interface named in *IP\_gre1*.

```
show ip interface IP_gre1 tunnel gre-keepalive
```




---

**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show ip ips

Displays the names of IP pools that are enabled for the IP pool sharing protocol (IPSP) and lists the disposition of addresses in the pools.

---

### Product

PDSN  
HA  
ASN-GW

---

### Privilege

Security Administrator, Administrator, Operator, Inspector

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

```
show ip ips [ summary ] [ | { grep grep_options | more } ]
```

#### summary

Displays only the disposition of the addresses in the participating IP pools. Does not show the names of the participating IP pools.

#### { grep *grep\_options* | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

### Usage Guidelines

Use this command to list the names of IP pools that are participating in the IPSP and list the disposition of IP addresses in those pools.




---

**Important** For information on configuring and using IPSP refer to the *System Administration Guide*.

---

### Example

To list information on all IPSP participating pools and address disposition, enter the following command:

```
show ip ips
```



**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show ip localhosts

Displays host name to IP address mapping for current context. Must be followed by a specific IP host name.

### Product

PDSN  
HA  
GGSN

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show ip localhosts hostname [ | { grep grep_options | more ]
```

#### *hostname*

Specifies a configured hostname as an alphanumeric string of 1 through 127 characters.

#### { **grep** *grep\_options* | **more** }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display mappings of a host name to IP addresses.

#### Example

To display IP address mapping for host name *local\_2345*, enter the following command;

```
show ip localhosts local_2345
```

## show ip ospf

Displays Open Shortest Path First (OSPF) routing information.

### Product

PDSN  
HA

GGSN

---

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
show ip ospf [ border-routers | database [ verbose ] [ ls-id ip_addr ] [
adv-router ip_addr ] [ ls-type { router | network | summary | asbr-summary
| external | nssa | integer } ] | debugging | interface | neighbor [ details
] | route | virtual-links ] [ | { grep grep_options | more } ]
```

**border-routers**

Displays all known area border routers (ABRs) and autonomous system border routers (ASBRs) for OSPF.

**database [ verbose ] [ ls-id ip\_addr ] [ adv-router ip\_addr ] [ ls-type { router | network | summary | asbr-summary | external | nssa | integer } ]**

Displays a summary of the database information for OSPF.

**verbose:** Displays detailed OSPF database information.

**ls-id ip\_addr:** Displays OSPF database information for the link state advertisements (LSAs) with the specified link state identifier (LSID). *ip\_addr* is entered using IPv4 dotted-decimal notation.

**adv-router ip\_addr:** Displays OSPF database information for the advertising router with the specified LSID. *ip\_addr* is entered using IPv4 dotted-decimal notation.

**ls-type { router | network | summary | asbr-summary | external | nssa | LSA\_Numerical\_Type } ]:** Displays OSPF database information for the specified LSA type.

**debugging**

Lists which debugging parameters are enabled.

**interface**

Displays interface information for OSPF.

**neighbor [ details ]**

Displays summarized information about all known OSPF neighbors.

**details:** Displays detailed information about all known OSPF neighbors.

**route [ summary ]**

Displays the OSPF routing table.

**summary:** Displays the number of intra-area, inter-area, external-1 and external-2 routes.



**virtual-links**

Displays the OSPF virtual links.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display OSPF information.

**Example**

To display general OSPF information, enter the following command;

```
show ip ospf
```

# show ip policy-forward

Displays information for IP packet redirecting policy for Home Agent (HA).

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show ip policy-forward [ | { grep grep_options | more } ]
```

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to see all the settings for IP packet redirection configuration from existing HA to new HA during upgrade.

**Important**

This is a customer specific command.

**Example**

The following command displays forward policy configuration for an HA:

```
show ip policy-forward
```

# show ip pool

Displays statistics specific to IP pools.

**Product**

PDSN  
GGSN  
HA  
ASN-GW  
A-BG

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show ip pool [ address { pool-name pool_name | group-name group_name } { used
| free | hold | release } [ limit limit ] | group-name group_name | groups
| hold-timer { imsi imsi | msid msid | username username [ imsi imsi | msid
msid ] } | many-to-one | nat-realm | one-to-one | overlap | pool-name
pool_name | private | public | resource | static | summary | verbose | wide
] [ | { grep grep_options | more }
```

**address** { pool-name *pool\_name* | group-name *group\_name* } { used | free | hold | release } [ limit *limit* ]

Displays IP pool addresses for the specified IP pool or pool group that are currently in the specified state.

**pool-name** *pool\_name*: Displays IP addresses from an existing IP pool name specified as an alphanumeric string of 1 through 31 characters.

**group-name** *group\_name*: Displays IP addresses from an existing IP pool group name specified as an alphanumeric string of 1 through 31 characters.

**used**: Displays the IP addresses that are in a used state.

**free**: Displays the IP addresses that are in a free state.

**hold**: Displays the IP addresses that are in a hold state.

**release**: Displays the IP addresses that are in a release state.

**limit** *limit*: Specifies the maximum number of address to display as an integer from 1 through 524287.

**group-name** *group\_name*

Displays information about an existing IP pool group name specified as an alphanumeric string of 1 through 31 characters.

**groups**

Lists information about all IP pool groups.

**hold-timer** {*imsi imsi* | *msid msid* | *username username* [*imsi imsi* | *msid msid*]}

Displays hold timer address information for the specified IMSI, MSID, or username.

**imsi** *imsi*: Displays hold-timer information for a valid IMSI (International Mobile Subscriber Identity), specified as a 15-character field that identifies the subscriber's home country and carrier.

**msid** *msid*: Displays hold-timer information for the MSID specified as a number from 7 through 16 digits.

**username** *username*: Displays hold-timer information for an existing username specified as an alphanumeric string of 1 through 127 characters.

**Important**

---

Active users cannot be displayed. If an active ID or username is entered, the following error message appears: Failure: No address matching the specified information was found! Please confirm that the options used match the network architecture/deployment, such as IMSI/MSID only, Username only, or IMSI/MSID plus Username. Please note that this command does not apply for addresses in the used state.

---

**many-to-one**

Lists information on Many-to-One NAT Realm IP address pools.

**nat-realm**

Lists information on NAT Realm IP address pools.

**one-to-one**

Lists information One-to-One NAT Realm IP address pools.

**overlap**

Lists information on overlapping IP pools.

**pool-name** *pool\_name*

Displays information about an existing IP pool.

**private**

Displays information about IP pools marked Private.

**public**

Displays information about IP pools marked Public.

**resource**

Displays information about resource IP pools.

**static**

Displays information about static IP pools.

**summary**

Displays a summary of all IP pool information.

**verbose**

Displays detailed information about all IP pools.

**wide**

Displays detailed information formatted to more than 80 columns.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display statistics pertaining to IP Pools in the current context.

**Example**

The following command displays IP address information for an IP Pool named *pool1*:

```
show ip pool address pool-name pool
```

To display a summary list for all IP pools in the current context, enter the following command:

```
show ip pool summary
```

The following command displays IP pool information for all IP pools configured in the current context:

```
show ip pool verbose
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show ip prefix-list

Displays IP prefix lists used to filter routes. With no keyword supplied, a list of all prefix lists and their entries is displayed.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<p><b>show ip prefix-list [ detail   name   summary ] list_name [   { grep grep_options   more } ]</b></p> <p><b>detail</b> Displays detailed information for the named prefix list.</p> <p><b>name</b> Displays information for the named prefix list.</p> <p><b>summary</b> Displays summary information for the named prefix list.</p> <p><b>list_name</b> Specifies the name of an existing prefix list as an alphanumeric string of 1 through 79 characters.</p> <p><b>{ grep grep_options   more }</b> Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of <b>grep</b> and <b>more</b>, refer to the <i>Regulating a Command's Output</i> section of the <i>Command Line Interface Overview</i> chapter.</p>
<b>Usage Guidelines</b>	Use this command to display information about IP prefix lists.

**Example**

To display detailed information about a prefix list named `route_101`, enter the following command:

```
show ip prefix-list detail route_101
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show ip route

Displays information related to currently configured static or VRF routes for the current context.

---

**Product** All

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show ip route** [ *ip\_address/mask* | **vrf** *vrf\_name* ] [ | { **grep** *grep\_options* | **more** ]

#### ***ip\_address/mask***

Specifies an IP address/mask (CIDR) for a static route in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

#### **| vrf *vrf\_name***

Displays information for an existing Virtual Routing and Forwarding (VRF) name expressed as an alphanumeric string of 1 through 63 characters.

#### **{ **grep** *grep\_options* | **more** }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines** Use this command to display information related to currently configured static or VRF routes for the current context.

#### **Example**

To display detailed information about a route for a static IP address, enter the following command:

```
show ip route 10.1.0.0/24
```




---

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show ip route-access-list

Displays information related to currently configured route-access-list used to filter routes.

---

**Product** All

---

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

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show ip route-access list [ name ] [ | { grep grep_options | more } ]
```

**name**

Specifies the name of an existing route access list as an alphanumeric string of 1 through 79 characters.

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display information about IP route access lists.

**Example**

To display detailed information about an access list named `access_route_3`, enter the following command:

```
show ip route-access-list access_route_3
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show ip static-route

Displays information related to currently configured static routes.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show ip static route [ ip_address/mask ] [ | { grep grep_options | more } ]
```

**ip\_address/mask**

Specifies an IP address/mask (CIDR) for a static route in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display information about IP static routes.

### Example

To display detailed information about route *192.155.33.2/24*, enter the following command:

```
show ip static route 192.155.33.2/24
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show ip vrf

Displays configuration information for VPN Routing and Forwarding instances.

### Product

All

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

In 21.20.19 and earlier releases:

```
show ip vrf [ vrf_name [ mpls-map-dscp-exp ] ] | { grep grep_options | more
}
```

In 21.20.19 21.24 and later releases:

```
show ip vrf [ name vrf_name [ mpls-map-dscp-exp ] ] | { grep grep_options
| more }
```

#### **vrf\_name**

Specifies an existing VRF name as an alphanumeric string of 1 through 63 characters.

#### **mpls-map-dscp-exp**

Displays the MPLS mapping for the VRF.

### Usage Guidelines

Use this command to display information about VRF names.



**Example**

To display information for a VRF named *corporate\_range2* with MPLS mapping:

```
show ip vrf name corporate_range2 mpls-map-dscp-exp
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show ip vrf-list

Displays configuration information for VRF lists currently on the system.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show ip vrf-list [ list_name ]
```

***list\_name***

Specifies the name of an existing VRF list as an alphanumerical string of 1 through 63 characters.

**Usage Guidelines**

Use this command to display information about all VRF lists or a specified VRF list.

**Example**

The following command displays information about all VRF lists in the system:

```
show ip vrf-list
```

## show ipms status

Displays the status of Intelligent Packet Monitoring System (IPMS) client service with information related to system and call events. It also displays the status of configured IPMS servers.

**Product**

IPMS

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

**show ipms status** [ **summary** | **all** | **server address** *ip\_address* ]

**summary**

Displays the summary of all configured IPMS client and IPMS servers.

**all**

Displays information for all configured IPMS client and IPMS servers.

**server address** *ip\_address*

Displays status for the IPMS server specified as an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

---

**Usage Guidelines**

This command is used to show/verify the status or configuration of one or all IPMS server along with system and call event information.

**Example**

The following command displays status of an IPMS server with IP address *10.2.3.4*:

```
show ipms status server address 10.2.3.4
```

## show ipne peers

Generates a list of the IP Network Enabler (IPNE) peers.

---

**Product**

MME.

---

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

**show ipne peers** { **all** | **service** *ipne\_service\_name* | **summary** } [ | { **grep** *grep\_options* | **more** } ]

**all**

Generates a list of all peers bound to the IPNE services, including the local and peer addresses. Also displays the TCP connections for every Session Manager.

**service** *ipne\_service\_name*

Generates a list of the peers associated with the specified IPNE service.

**Summary**

Generates a summary of all available IPNE peer statistics.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to monitor and troubleshoot MME connections to the IPNE client and peer.

**Example**

List all IPNE peers with a command similar to the following:

```
show ipne peers all
```

# show ipsg service

Displays IP Service Gateway (IPSG) service information.

**Product**

eWAG  
IPSG

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show ipsg service { all | name ipsg_service_name } [ counters ] [ | { grep grep_options | more } ]
```

**all**

Displays information for all IPSG service(s) configured on the system.

**name *ipsg\_service\_name***

Displays information for the specified IPSG service. *ipsg\_service\_name* must be an alphanumeric string of 1 through 63 characters.

**counters**

**counters** requires the output is to display counters associated with the IPSG service(s).

**{ `grep` *grep\_options* | `more` }**

Specifies to pipe (send) the output of this command to the specified command. You must specify a command to which the output of this command should be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

### Usage Guidelines

Use this command to view information for all IPSG services or a specific IPSG service.

### Example

The following command displays information for all IPSG services configured on the system:

```
show ipsg service all
```

## show ipsg sessions

Displays IP Service Gateway (IPSG) session information.

---

### Product

eWAG  
IPSG

---

### Privilege

Security Administrator, Administrator, Operator, Inspector

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

```
show ipsg sessions [ counters | full | summary ] [ all | callid call_id | ip-address ipv4_address | msid msid_number | peer-address ipv4_address | username user_name ] [ | { grep grep_options | more } ]
```

#### counters

Displays session counters for matching sessions.

#### full

Displays all available information for matching sessions.

#### summary

Displays a summary of available information for matching sessions.

#### all

Displays session information including call ID, NAI, and home address for all current IPSG sessions.

This is the default behavior for the **show ipsg sessions** command.

**callid *call\_id***

Displays session information for a current IPSG session based on the specified call ID.

*call\_id* must be an 8-digit hexadecimal number.

**ip-address *ipv4\_address***

Displays session information for a specific IPSG session based on the subscriber IP address.

*ipv4\_address* must be specified in IPv4 dotted-decimal notation.

**msid *msid\_number***

Displays session information for a current IPSG session based on the specified MSID.

*msid\_number* must be an 8-digit hexadecimal number.

**peer-address *ipv4\_address***

Displays session information for a current IPSG session based on the IP address of the device sending the RADIUS accounting messages.

*ipv4\_address* must be specified in IPv4 dotted-decimal notation.

**username *user\_name***

Displays session information for an IPSG session based on subscriber's user name.

*user\_name* must be an alphanumeric string of 1 through 127 characters.

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Use this command to view IPSG session information.

**Example**

The following command displays all the existing IPSG service sessions on the system:

```
show ipsg session all
```

**Important**

---

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show ipsg statistics

Displays IP Services Gateway (IPSG) service statistics.

## show ipsg statistics

<b>Product</b>	eWAG IPSG
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<p><b>show ipsg statistics</b> [ <b>name</b> <i>ipsg_service_name</i>   <b>peer-address</b> <i>ipv4_address</i> ] [   { <b>grep</b> <i>grep_options</i>   <b>more</b> } ]</p> <p><b>name</b> <i>ipsg_service_name</i></p> <p>Displays cumulative statistics of all IPSG sessions processed by the specified service since the last system restart or clear command.</p> <p><i>ipsg_service_name</i> must be the name of an IPSG service, and must be an alphanumeric string of 1 through 63 characters.</p> <p><b>peer-address</b> <i>ipv4_address</i></p> <p>Displays cumulative statistics of all IPSG sessions associated with the specified IP address of the device sending the RADIUS accounting messages. The statistics displayed are from the last system restart or clear command.</p> <p><i>ipv4_address</i> must be specified in IPv4 dotted-decimal notation.</p> <p>{ <b>grep</b> <i>grep_options</i>   <b>more</b> }</p> <p>Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.</p> <p>For details on the usage of <b>grep</b> and <b>more</b>, refer to the <i>Regulating a Command's Output</i> section of the <i>Command Line Interface Overview</i> chapter.</p>
<b>Usage Guidelines</b>	Use this command to view IPSG service statistics.

**Example**

The following command displays cumulative IPSG session statistics on the system:

```
show ipsg statistics
```

The following command displays the cumulative IPSG session statistics for an IPSG service named *ipsg1*:

```
show ipsg statistics name ipsg1
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show ipv6 access-group statistics

Displays statistics for each rule in all IPv6 access groups or a specified IPv6 access control group.

**Product** HA

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

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `show ipv6 access-group statistics [ | { grep grep_options | more } ]`

`| { grep grep_options | more }`

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines** Use this command to display the configured IPv6 access control groups in the current context.

### Example

The following command displays the contents of an IPv6 access control group named `ACGv6_4`:

```
show ipv6 access-group ACGv6_4
```

## show ipv6 access-list

Displays the information for all IPv6 Access Control Lists (ACLs) or the named ACL. With no keyword supplied, a list of all access lists and their entries is displayed.

**Product** HA

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

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `show ipv6 access-list list_name [ | { grep grep_options | more } ]`

***list\_name***

Specifies the name of an existing ACL configured in the current context as an alphanumeric string of 1 through 47 characters.

**| { *grep grep\_options* | *more* }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display the configured IPv6 ACLs in the current context.

**Example**

The following command displays the contents of an IPv6 ACL named *ACLv6\_4*:

```
show ipv6 access-list ACLv6_4
```

## show ipv6 interface

Displays statistical and configuration information for the IPv6-based interfaces, including a Virtual Routing and Forwarding (VRF) table for a specific context.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show ipv6 interface [ name intfc_name ] [ statistics ] [ summary ] [ vrf
vrf-name ] [ | { grep grep_options | more } ]
```

**name *intfc\_name***

Displays information for an existing interface specified as an alphanumeric string of 1 through 79 characters. If no interface name is specified, the information for all IPv6 interfaces is displayed.

**statistics**

Displays the session statistics of all ingress and egress packets processed through this IPv6 interface.

**summary**

Displays summarized information about requested IPv6 interfaces.



**vrf vrf\_name**

Displays Virtual Routing and Forwarding (VRF) routing information for an existing VRF specified as an alphanumeric string of 1 through 63 characters.

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display the summarized of detailed configuration and statistical information for a configured IPv6 interface. This information can be used to verify and/or troubleshoot communication difficulties between to a remote host/node.

**Example**

The following command displays the interface information, including statistics, for the IPv6 interface *IPv6Interface\_2*.

```
show ipv6 interface IPv6Interface_2 statistics
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show ipv6 neighbors

Displays the neighbor table for all IPv6 addresses or a specified IPv6 address in the current context.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show ipv6 neighbors [ ipv6_address ] [ vrf vrf-name ] [ | { grep grep_options | more } ]
```

**ipv6\_address**

Displays information for an existing IPv6 address specified in IPv6 colon-separated-hexadecimal notation. If no IPv6 address is specified, the information for all IPv6 addresses is displayed.

**vrf vrf\_name**

Displays Virtual Routing and Forwarding (VRF) routing information for an existing VRF specified as an alphanumeric string of 1 through 63 characters.

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display neighbor information for IPv6 address(es) in the current context. This information can be used to verify and/or troubleshoot communication difficulties between to a remote host/node.

**Example**

The following command displays the neighbor information for the IPv6 address *ffe:ffff:101::230:6eff:fe04:d9aa*.

```
show ipv6 neighbor ffe:ffff:101::230:6eff:fe04:d9aa
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show ipv6 ospf

Displays information regarding the configuration of the OSPFv3 Protocol on this system.

**Product**

PDSN  
HA  
GGSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show ipv6 ospf [ database | debugging | interface | neighbor | route |
virtual-links ] [ verbose [ verbose ] [ | { grep grep_options | more } ]
show ipv6 ospf database [ adv-routeripv4-address ] [ ls-type { external |
inter-prefix | inter-router | intra-prefix | link | network | router }
show ipv6 ospf debugging
show ipv6 ospf interface
show ipv6 ospf neighbor [ details]
```

```
show ipv6 ospf route [ summary ]  
show ipv6 ospf virtual-links
```

### show ipv6 ospf database

Displays the OSPFv3 database including the following components.

- **adv-router** *ipv4-address*: Displays OSPF database information from the advertising router specified as an IP address in IPv4 dotted-decimal notation.
- **ls-type**: Displays the specified Link-State Advertisement (LSA) type, which can be one of the following:
  - **external**: Display External LSA information
  - **inter-prefix**: Displays Inter Area Prefix LSA information
  - **inter-router**: Displays Inter Area Router LSA information
  - **intra-prefix**: Displays Intra Area Prefix LSA information
  - **link**: Displays Link LSA information
  - **network**: Displays Network LSA information
  - **router**: Displays Router LSA information

### show ipv6 ospf debugging

Displays OSPFv3 Debugging Flags.

### show ipv6 ospf interface

Displays OSPFv3 Interfaces.

### show ipv6 ospf neighbor [ details ]

Displays OSPFv3 neighbors with the option for full details.

### show ipv6 ospf route [ summary ]

Displays OSPFv3 route information with the option for summarized information.

### show ipv6 ospf virtual-links

Displays OSPFv3 virtual links.

### verbose

Displays detailed information.

### { **grep** *grep\_options* | **more** }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines** Use this command to see all OSPFv3 information.

### Example

The following command displays IPv6 OSPF information:

```
show ipv6 ospf
```

## show ipv6 pool

Displays information related IPv6 Pool configuration/state.

### Product

PDSN  
GGSN  
ASN-GW

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show ipv6 pool [ group-name group-name ] [ pool-name pool-name ] [ summary ] [ verbose ] [ | { grep grep_options | more } ]
```

#### **group-name** *group-name*

Displays IP address pool information for an existing group-name specified as an alphanumeric string of 1 through 31 characters.

#### **pool-name** *pool-name*

Displays IPv6 address pool information for an existing pool name specified as an alphanumeric string of 1 through 31 characters.

#### **summary**

Displays summary information about all IP address pools; this is the default.

#### **verbose**

Displays detailed information about all IP address pools.

**{ `grep` *grep\_options* | `more` }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to see all the ipv6 pool information.

### Example

The following command displays IPv6 pool information:

```
show ipv6 pool
```

## show ipv6 prefix-list

Displays information related to an IPv6 prefix list.

### Product

PDSN  
GGSN  
ASN-GW

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show ipv6 prefix-list [ detailprefix-list-name ] [ nameprefix-list-name [ ip-address/mask [ longer ] [ match-first ] ] [ seq seq_value ] ] [ summary prefix-list-name ] [ | { grep grep_options | more } ]
```

#### **detail***prefix-list-name*

Displays detailed IP address information for an existing prefix-list specified as an alphanumeric string of 1 through 79 characters.

#### **name***prefix-list-name*

Displays IP address information for an existing prefix-list specified as an alphanumeric string of 1 through 79 characters.

#### **ip-address/mask**

Specifies an IPv6 Network Address/Mask Bits combination in CIDR notation.

**longer**

Displays IP address prefix-list details in longer format.

**match-first**

Displays first matched IP address prefix-list details.

**seq seq\_value**

Specifies the sequence number as an integer from 1 through 4294967295.

*seq\_value* is the integer value between 1 through 4294967295.

**summary prefix-list-name**

Displays prefix-list summary for an existing prefix-list specified as an alphanumeric string of 1 through 79 characters.

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to see all the ipv6 prefix-list information.

**Example**

The following command displays IPv6 prefix list information:

```
show ipv6 prefix-list
```

## show ipv6 route

Displays information related to specific route for current context.

**Product**

PDSN  
GGSN  
ASN-GW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show ipv6 route [ ip-address/mask ] [ vrf vrf-name ] [ | { grep grep_options | more } ]`

**ip-address/mask**

Specifies an IP address entered using IPv6 colon-separated-hexadecimal and CIDR notation.

**vrf vrf-name**

Displays Virtual Routing and Forwarding (VRF) routing information for an existing VRF specified as an alphanumeric string of 1 through 63 characters.

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines** Use this command to see all the ipv6 route information.

**Example**

The following command displays IPv6 route information:

```
show ipv6 route 2001:0db8:85a3:0000:0000:8a2e:0370:7334/5
```

## show ipv6 route-access-list

Displays the route access list.

---

**Product** PDSN

GGSN

ASN-GW

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show ipv6 route-access-list [ route-access-list ] [ | { grep grep_options | more } ]`

**route-access-list**

*route-access-list* is an alphanumeric string of 1 through 79 characters.

**{ `grep` *grep\_options* | `more` }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines** Use this command to see all the IPv6 route access list information.

### Example

The following command displays IPv6 route access list information:

```
show ipv6 route-access-list
```

## show iups-service

Displays information for Iu-PS services in the current context. The Iu-PS interface links the radio network controller (RNC) with the packet switched core network.

**Product** SGSN

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

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **show iups-service** { **all** | **name** *svrc\_name* } [ **gtpu-table** | **rnc** { **all** | **id** *rnc\_id* } ] [ | { **grep** *grep\_options* | **more** } ]

### all

Shows information for all configured IuPS services.

### name *svrc\_name*

Specifies an existing IuPS service as an alphanumeric string of 1 through 63 characters.

### gtpu-table

Displays the configured GTPU database.

### rnc all

Displays information for all configured RNCs.



**rnc rnc\_id**

Specifies the identification number of an existing RNC configuration instance as an integer from 0 through 4095.

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Iu-PS services control the interface between the SGSN and the RNCs in the UMTS radio access network (UTRAN). Iu-PS services include the control plane and the data plane between these nodes.

Use this command to display information for a specific Iu-PS service or for all Iu-PS services configured within the context. A filtering keyword can limit the display to only information for a specific RNC or for a GTPU table in the Iu-PS service configuration.

**Example**

The next command displays information for all Iu-PS services configured in the current context:

```
show iups-service all
```

This command displays information for a specific RNC for a specific Iu-PS services:

```
show iups-service name iups-svc-1 rnc 123name
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show l2tp sessions

Displays information for Layer 2 Tunneling Protocol (L2TP) tunnels.

**Product**

LNS  
PDSN  
GGSN  
HA

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show l2tp sessions [ full | summary | counters ] [ all | callid id |
username name | msid ms_id | lac-service service_name | lns-service service_name
| pdsncllosedrp-service service_name | peer-address [ operator ] peer_address
]
```

**full**

Displays all available information for the specified sessions.

**summary**

Displays a summary of available information for the specified sessions.

**counters**

Displays counters for the specified L2TP sessions.

**all**

Displays all current sessions.

**callid *id***

Displays session information for the call ID. specified an 8-byte hexadecimal number. The output of the command **show l2tp tunnels** contains a field labeled Callid Hint which lists the call ID information to use with this command.

**username *name***

Displays session information for an existing subscriber specified as an alphanumeric string of 1 through 127 characters. Wildcard characters \$ and \* are allowed.

**msid *ms\_id***

Displays session information for the MSID specified as 7 to 16 digits for an IMSI, MIN, or RMI. Wildcard characters \$ and \* are allowed.

**lac-service *service\_name***

Displays all L2TP sessions in the specified LAC service.

**lns-service *service\_name***

Displays all L2TP sessions in the specified LNS service.

**pdsnclosedrp-service *service\_name***

Displays all L2TP sessions in the specified Closed R-P service.

**peer-address [ *operator* ] *peer\_address***

Displays all L2TP sessions to the destination (peer LNS) specified as an IP address in IPv4 dotted-decimal notation.

In conjunction with **sessions** keyword, indicates a range of peers is to be displayed.

**peer-address** [ *operator* ] *peer\_address* is specified using IPv4 dotted-decimal notation.

*operator* implies how to logically specify a range of *peer-address* and it must be one of the following:

- <: IP address less than the specified *peer\_address*
- >: IP address less than the specified *peer\_address*
- **greater-than**: IP address less than the specified *peer\_address*
- **less-than**: IP address less than the specified *peer\_address*

### Usage Guidelines

Use this command to show information for sessions in the current context.



#### Important

If this command is executed from within the local context, cumulative session information is displayed for all contexts.

#### Example

The following command displays cumulative statistics for all sessions processed within the current context:

```
show l2tp sessions
```

The following command displays all information pertaining to the L2TP session of a subscriber named *isp1vpnuser1*:

```
show l2tp session full username isp1vpnuser1
```



#### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show l2tp statistics

Displays statistics for all Layer 2 Tunneling Protocol (L2TP) tunnels and sessions.

### Product

PDSN

GGSN

HA

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show l2tp statistics [ lac-service service_name | lns-service service_name |
pdsnclosedrp-service service_name | peer-address peer_ip_address ]
```

**lac-service service\_name**

Displays L2TP statistics for all tunnels and sessions in an existing L2TP Access Concentrator (LAC) service specified as an alphanumeric string of 1 through 63 characters.

**lns-service service\_name**

Displays L2TP statistics for all tunnels and sessions in an existing L2TP Network Server (LNS) service specified as an alphanumeric string of 1 through 63 characters.

**pdsnclosedrp-service service\_name**

Displays L2TP statistics for all tunnels and sessions in an existing Closed R-P service specified as an alphanumeric string of 1 through 63 characters.

**peer-address peer\_address**

Displays L2TP statistics for all tunnels and sessions to the destination (peer LNS) at the IP address specified in IPv4 dotted-decimal notation.

**Usage Guidelines**

Use this command to display statistics for L2TP services.

**Example**

The following command displays statistics for a specific LAC service named *vpn1*:

```
show l2tp statistics lac-service vpn1
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

# show l2tp tunnels

Displays information for Layer 2 Tunneling Protocol (L2TP) tunnels.

**Product**

PDSN  
GGSN  
HA

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show l2tp tunnels [ full | summary | counters ] [ all | callid id |  
username name | msid ms_id | lac-service service_name | lns-service service_name  
| pdsnclosedrp-service service_name | peer-address [ operator ] peer_address  
]
```

**full**

Displays all available information for the specified tunnels.

**summary**

Displays a summary of available information for the specified tunnels.

**counters**

Displays counters for the specified L2TP tunnels.

**all**

Displays all current tunnels.

**callid *id***

Displays tunnel information for the call id specified as an 8-digit hexadecimal number. The output of the command **show l2tp tunnels** contains a field labeled Callid Hint which lists the call id information to use with this command.

**username *name***

Displays tunnel information for an existing subscriber specified as an alphanumeric string of 1 through 127 characters. Wildcard characters \$ and \* are allowed.

**msid *ms\_id***

Displays tunnel information for the MSID specified as 7 to 16 digits for an IMSI, MIN, or RMI. Wildcard characters \$ and \* are allowed.

**lac-service *service\_name***

Displays all L2TP tunnels in the specified LAC service.

**lns-service *service\_name***

Displays all L2TP tunnels in the specified LNS service.

**pdsnclosedrp-service *service\_name***

Displays all L2TP tunnels in the specified Closed R-P service.

**peer-address [ *operator* ] *peer\_address***

Displays all L2TP tunnels to the destination (peer LNS) at the IP address specified in IPv4 dotted-decimal notation.

In conjunction with **tunnels** keyword, indicates a range of peers is to be displayed.

**peer-address** [ *operator* ]: Specifies a peer address using IPv4 dotted-decimal notation.

*operator* implies how to logically specify a range of peer-address and it must be one of the following:

- <: IP address less than the specified *peer\_address*
- >: IP address less than the specified *peer\_address*
- **greater-than**: IP address less than the specified *peer\_address*
- **less-than**: IP address less than the specified *peer\_address*

### Usage Guidelines

Use this command to show information for tunnels in the current context.

### Example

The following command displays all of the tunnels currently being facilitated by LAC services within the current context:

```
show l2tp tunnels all
```

The following command displays information pertaining to the L2TP tunnel(s) established for a LAC-service named vpn1:

```
show l2tp tunnels full lac-service vpn1
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show lac-service

Displays the information for all L2TP Access Concentrator (LAC) services or for a particular LAC service.

### Product

PDSN  
HA  
GGSN

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show lac-service { all | name service_name } [ | { grep grep_options | more } ]
```

### all

Display information for all LAC services.

**name *service\_name***

Display information only for an existing LAC service specified as an alphanumeric string of 1 through 63 characters.

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to list information for LAC services configured on this system.

**Example**

The following commands display information for all LAC services and the LAC service named *lac1*, respectively.

```
show lac-service all
show lac-service name lac1
```

## show lawful-intercept

Refer to the *Lawful Intercept Configuration Guide* for a full description of this command.

## show lawful-intercept ssdf statistics

Refer to the *Lawful Intercept Configuration Guide* for a description of these statistics.

## show ldap connection all

Displays all details about the Lightweight Directory Access Protocol (LDAP) subsystem.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show ldap connection all [ | { grep grep_options | more } ]
```

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines** Display all details about the LDAP subsystem.

### Example

The following command displays full information about the LDAP subsystem.

```
show ldap connection all
```

## show leds

Displays the current status of the light emitting diodes (LEDs) for a specific card or all cards.

---

**Product** All

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show leds { all | *card\_num* } [ | { grep *grep\_options* | more } ]**

**all | *card\_num***

**all:** Displays the LED status for all cards.

***card\_num*:** Displays the LED status for the card specified by its slot number.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines** Display the status of the LEDs as a part of an automated periodic script which checks the LEDs of the chassis.




---

**Important** This command is not supported on all platforms.

---



**Example**

The following commands display the LED status for all cards and only card 8, respectively.

```
show leds all
```

```
show leds 8
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show license

Displays information about licensing as configured on this system.

**Product**

All

**Privilege**

Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show license { all | enforcement { policy | status [ allowed | blocked ]
[ feature | service ] } | eval-period | history | information [ key
key_name ] [ full ] | key | privilege-bits | smart-tags [ feature | service
] | statistics [ verbose ] | status | summary | tech-support | udi |
usage } [ | { grep grep_options | more } ]
```

**all**

Shows a superset of information that includes show status, show usage, show UDI, as well as the Smart Licensing agent version.

This keyword applies to Smart Licensing only.

**enforcement { policy | status [ allowed | blocked ] [ feature | service ] }**

Shows the enforcement policy applied to or current enforcement status of Smart Licenses. Status information can be filtered based on the licenses which are currently allowed or blocked, or by license type.

**allowed:** displays the current status, and if out of compliance (OOC) the list of services which are blocked.

**blocked:** displays the list of services and features which are blocked.

**feature:** displays the current status, and if out of compliance (OOC) the list of services which are blocked.

**service:** displays the current status and if out of compliance (OOC) the list of services and features which are blocked.

This keyword applies to Smart Licensing only.

**eval-period**

Shows information about the evaluation period. Licenses are granted a 90 day evaluation period until they are registered.

This keyword applies to Smart Licensing only.

**history**

Displays the history of installed license and how much time each license was in each state. This keyword applies to legacy licensing only.

**information [ key *key\_name* ] [ full ]**

Displays the license information to verify the proper keys have been installed. This command is also helpful in troubleshooting user system access due to the maximum number of sessions being reached.

**key *key\_name***: Displays the information for an existing license key specified as an alphanumeric string of 1 of 1 through 500 characters.

**full**: Displays the full features and quantities without any hardware limits in place.

**key**

Displays the installed keys in encrypted format.

**privilege-bits**

Displays all the CLI privilege bits that are turned on. This keyword applies for legacy licensing only.

**smart-tags [ feature | service ]**

Shows the features and services that are currently supported and the corresponding Smart Entitlement Tags.

**feature**: filters the output to show only features.

**service**: filters the output to show only services.

This keyword applies to Smart Licensing only.

**statistics [ verbose ]**

Shows Smart Licensing details for each individual feature. Use the optional **verbose** keyword to display additional information.

**status**

Shows information about the current state of Smart Licensing on the system, such as registration and license authorization status.

**summary**

Shows information about the current state of Smart Licensing on the system, such as registration, license authorization, and license usage status.

**tech-support**

Shows information useful for debugging issues with Smart Licensing.

**udi**

Shows details for all Unique Device Identifiers (UDI). This keyword applies to Smart Licensing only.

**usage**

Shows the usage information for all entitlements that are currently in use. This keyword applies to Smart Licensing only.

**{ `grep` *grep\_options* | `more` }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

This command displays licensing information, both the legacy licensing model as well as the Smart Licensing model introduced in Release 21.3. The `history`, `information`, `key`, and `privilege-bits` keywords apply only to the legacy license key model. All other keywords display information related to Smart Licensing introduced in Release 21.3.

Refer to the *Smart Licensing* chapter of the *System Administration Guide* for more details about Smart Licensing.

**Example**

The following displays all information about Smart Licensing as configured on the system.

```
show license all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

# show link-aggregation

Displays information about any Link Aggregation Group (LAG) configured in this system. A LAG works by exchanging control packets via Link Aggregation Control Protocol (LACP) over configured physical ports with peers to reach agreement on an aggregation of links. The LAG sends and receives the control packets directly on physical ports.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

```
show link-aggregation { info | lACP info | statistics } group group_number
[ | { grep grep_options | more } ]
show link-aggregation table [all] [ | { grep grep_options | more } ]
show link-aggregation utilization table [ | { grep grep_options | more } ]
```

#### **{ info | lACP info | statistics }**

Displays the following categories of LAG information:

- **info** – LAG configuration and operating state
- **lACP info** – LACP Rx and Tx counters
- **statistics** – LAG Rx and Tx counters and data throughput statistics

#### **group group\_number**

Specifies the LAG number as an integer from 1 through 1023.

#### **table [all] group\_number**

Displays information about the current LAG port configuration in tabular form. The **all** option includes ATM PVCs for ATM ports (ASR 5000 only).

#### **utilization table**

Displays LAG utilization data in tabular form.

#### **| { grep grep\_options | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

### Usage Guidelines

Use this command to displays information about any Link Aggregation Group (LAG) configured in this system.

#### **Example**

The following command displays configuration information for LAG number 100:

```
show link-aggregation info group 100
```




---

#### **Important**

Output descriptions for **show** commands are available in the *Statistics and Counters Reference*.

---

# show linkmgr

Displays statistics for the link manager (linkmgr).

---

**Product** SGSN

---

**Privilege** Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show linkmgr { all | instance instance } [ parser | | ]`

## all

Display statistics for all link managers.

## instance *instance*

Display statistics for a single instance of a link manager specified as an integer from 1 to 4.

## { *grep* *grep\_options* | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

## Usage Guidelines

This command displays statistical information for the SGSN's link manager which handles the layer between the session manager and the SS7 functionality downwards from layer 3.

## Example

Use the following command to display the statistics for link manager 4:

```
show linkmgr 4
```




---

### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

# show llc statistics

Displays traffic statistics for the GPRS logical link-control (LLC) layer.

---

**Product** SGSN

---

**Privilege** Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show llc statistics** [ **gprs-service** *srcv\_name* ] [ **verbose** ] [ | { **grep** *grep\_options* | **more** } ]

**gprs-service *srcv\_name***

Displays the statistics for an existing GPRS service specified as an alphanumeric string of 1 through 63 characters.

**verbose**

Displays all possible statistics for specified command or keyword.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For more information on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference*.

---

**Usage Guidelines** This command can display either a summarized or full (verbose) view of statistics collected for the traffic that has gone through the LLC layer for either all GPRS services or for a specified GPRS service.

**Example**

The following command displays the frame Tx/Rx LLC statistics for GPRS service *gprs1*:

```
show llc statistics gprs-service gprs1
```

## show llc status

Displays status information for the GPRS logical link-control (LLC) layer.

---

**Product** SGSN

---

**Privilege** Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show llc status gprs-service srvc_name sessmgr instance instance { dlci ms-id
  ms_id sapi sapid | lsap sapid sapid | ms ms_id | usap sapid sapid [ | { grep
  grep_options | more } ]
```

**gprs-service *srvc\_name***

Displays the LLC layer status for an existing GPRS service specified as an alphanumeric string of 1 through 63 characters.

**sessmgr instance *instance***

Displays the LLC status for a session manager instance specified as an integer. The range varies depending upon the release:

- for releases prior to 14.0, the range is from 1 to 4294967295.
- for releases 14.0 and later, the range is from 1 to 384.

**dlci ms-id *ms\_id* [ sapi *sapid* ]**

Displays the LLC status for a specific data link connection identifier (DLCI) between the LLC and the mobile station (MS). *ms\_id* must be an integer from 0 to 65536 that identifies the DLCI interface connecting to a specific MS.

**sapi:** Filters the display of the LLC status information to focus on a specific service access point interface (SAPI) within the specified DLCI specified as an integer from 1 to 11

**lsap *sapid***

Refines the display of the LLC status to focus on a specific lower service access point interface (LSAP) specified as an integer from 0 to 65536.

**ms-id *ms\_id***

Displays the LLC status for a connected MS specified as an integer from 0 to 65536.

**usap *sapid***

Refines the display of the LLC statistics to focus on a specific upper service access point interface (USAP) specified as an integer from 0 to 65536.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For more information on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Reference*.

**Usage Guidelines**

This command can display either a summarized or full (verbose) view of statistics collected for the traffic that has gone through the LLC layer for either all GPRS services or for a specified GPRS service.

**Example**

The following command displays the frame Tx/Rx LLC statistics for GPRS service *gprs1*:

```
show llc statistics gprs-service gprs1
```

## show lma-service

Displays statistic and counter information for Local Mobility Anchor (LMA) services on this system.

<b>Product</b>	P-GW SAEGW
<b>Privilege</b>	Inspector
<b>Command Modes</b>	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show lma-service all
show lma-service name service_name
show lma-service session [ all | callid id | counters | full | ipv6-address
  { < address | > address | address | greater-than address [ less-than address ]
  | less-than address [ greater-than address ] } | summary | username name ]
show lma-service statistics [ lma-service name ] } [ | { grep grep_options
  | more } ]
```

**all**

Displays information about all configured LMA services on this system.

**name service\_name**

Displays configuration information for an existing LMA service specified as an alphanumeric string of 1 through 63 characters.

```
session [ all | callid id | counters | full | ipv6-address { < address | > address | address | greater-than address
  [ less-than address ] | less-than address [ greater-than address ] } | summary | username name ]
```

Displays session information filtered by the following parameters:

**all:** Displays all active LMA sessions using LMA services on the system.

**callid id:** Displays available session information for the call identification number specified as an eight-byte hexadecimal number.

**counters:** Displays session counters for active LMA sessions using LMA services on the system. This keyword can also be filtered by the following:

- all



- **callid**
- **ipv6-address**
- **username**

Refer to the keyword descriptions in this command for information regarding these filters.

**full**: Displays additional session information for active LMA sessions using LMA services on the system. This keyword includes the information in the output of the **all** keyword plus additional information. This keyword can also be filtered by the following:

- **all**
- **callid**
- **ipv6-address**
- **username**

Refer to the keyword descriptions in this command for information regarding these filters.

**ipv6-address**:

- **< address** and **less-than address**: Displays summarized information for a group of IPv6 addresses that are less than the specified IPv6 address using one of these keywords. A range can be specified by including an address with the **greater-than** option. *address* must be specified in IPv6 colon-separated-hexadecimal notation.
- **> address** and **greater-than address**: Displays summarized information for a group of IPv6 addresses that are greater than the specified IPv6 address using one of these keywords. A range can be specified by including an address with the **less-than** option. *address* must be specified in IPv6 colon-separated-hexadecimal notation.
- **address**: Displays summarized information for a specific IPv6 address using an LMA service on this system. *address* must be specified in IPv6 colon-separated-hexadecimal notation.

**summary**: Displays the number of LMA sessions currently active for LMA services configured on the system.

**username name**: Displays available session information for an existing user specified as an alphanumeric string of 1 through 127 characters.

**statistics [ lma-service name ]**

**lma-service name**: Displays LMA service statistics for an existing LMA service specified as an alphanumeric string of 1 through 63 characters.

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to view configuration information for LMA services on this system.

**Example**

The following command displays service statistics for the LMA service named *lma1*:

```
show lma-service name lma1
```

## show lns-service

Displays the information for all L2TP Network Server (LNS) services or for a particular LNS service.

**Product**

PDSN  
HA  
GGSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show lns-service { all | name service_name } [ | { grep grep_options | more } ]
```

**all**

Display information for all LNS services.

**name service\_name**

Displays information only for an existing LNS service specified as an alphanumeric string of 1 through 63 characters.

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to list information for LNS services configured on this system.

**Example**

The following commands display information for all LNS services and the LNS service named *lns1*, respectively.

```
show lns-service all
```

```
show lns-service name lns1
```

## show local-policy

Displays information pertaining to local QoS policy services.

---

### Product

P-GW  
SAEGW

---

### Privilege

Security Administrator

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

```
show local-policy statistics { all | service service_name | summary } | { grep grep_options | more }
```

```
statistics { all | service service_name | summary }
```

Display statistics pertaining to local QoS services.

**all**: Displays information for all local QoS services.

**service** *service\_name*: Displays statistics only for an existing local QoS service specified as an alphanumeric string of 1 through 64 characters.

**summary**: Displays summarized statistics all local QoS services.

```
{ grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

### Usage Guidelines

Use this command to display statistics for local QoS policies on this system.

### Example

The following command displays statistics for the local QoS policy named *sample1*.

```
show local-policy statistics service sample1
```

## show local-user

Displays information pertaining to local-user accounts.

**Important**

In a release 20.0 or higher Trusted build, this command is not available.

**Product**

All

**Privilege**

Security Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show local-user [ [ username name ] [ inactive filter ] [ verbose | wide ]
| statistics [ verbose ] ]
```

**username *name***

Displays information for an existing local-user administrative account specified as an alphanumeric string of 3 through 16 characters that is case sensitive. If a username is not specified, information is displayed for all local users.

**inactive *filter***

Specifies a filter for displaying inactive local-user accounts:

- *< days*: Displays accounts that have been inactive less than the specified number of days.
- *> days*: Displays accounts that have been inactive more than the specified number of days.
- **greater-than** *days*: Displays accounts that have been inactive more than the specified number of days.
- **less-than** *days*: Displays accounts that have been inactive less than the specified number of days.

*days* can be configured to an integer from 1 through 365.

**[ verbose | wide ]**

Specifies how the information is to be displayed as one of the following options:

- **verbose**: The data is displayed in list format. Additional information is provided beyond what is displayed when the **wide** option is used.
- **wide**: The data is displayed in tabular format. This is the default setting.

**statistics [ verbose ]**

Displays local-user statistics.

Using the **verbose** keyword displays additional statistics.

**Usage Guidelines**

Use this command to display information and statistics on local-user administrative accounts.

**Example**

The following command displays detailed information on local-user administrative accounts that have been inactive for more than 10 days:

```
show local-user inactive greater-than 10 verbose
```

The following command displays detailed information for a local-user account named *Test*:

```
show local-user username Test verbose
```

The following command displays detailed local-user account statistics:

```
show local-user statistics verbose
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show location-service

Displays information and statistics for all location services or for a specific location service.

**Product**

MME  
SGSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show location-service { service { all | name service_name } | statistics {
  all | service service_name } [ | { grep grep_options | more } ]
```

**service { all | name service\_name }**

Display configuration information pertaining to location services.

**all**: Displays information for all location services.

**name service\_name**: Displays information only for an existing location service specified as an alphanumeric string of 1 through 63 characters.

**statistics { all | service service\_name }**

Display statistics pertaining to location services.

**all**: Displays statistics for all location services.

**name service\_name**: Displays statistics only for an existing location service specified as an alphanumeric string of 1 through 64 characters.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to list configuration information and statistics for location services configured on this system.

### Example

The following commands display information for all location services and the location service named *location\_service1*, respectively.

```
show location-service service all
```

```
show location-service service name location_service1
```

The following command displays statistics for the location service named *location\_service1*.

```
show location-service statistics service location_service1
```

## show logging

Displays the defined logging filters for the current context.

### Product

All

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show logging [ active | verbose ] [ | { grep grep_options | more } ]
```

#### **active | verbose**

**active:** Displays only active CLI logging filter information in concise format.

**verbose:** Displays as much information as possible.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines** View log filters to troubleshoot disk utilization issues.

**Example**

```
show logging
show logging active
show logging verbose
show logging active verbose
```

## show logical-port utilization table

Displays logical port (VLAN and NPU) utilization for a specified interface port.

**Product** All

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

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `show logical port utilization table slot/port [vlan { 5-minute | hourly }] [ | { grep grep_options | more } ]`

**slot/port**

Specifies the port for which logical-port statistics will be displayed. The slot and port must refer to an installed card and port.

**vlan { 5-minute | hourly }**

Displays only active VLAN information for the specified collection interval.

- **5-minute**: Displays 5-minute utilization intervals for the past 24 hours.
- **hourly**: Displays hourly utilization intervals for the past 24 hours.

**| { grep grep\_options | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines** View logical port (VLAN) statistics for 5-minute intervals on port 17/1.

**Example**

```
show logical-port utilization table 17/1 vlan 5-minute
```

# show logs

Displays active and inactive logs filtered by the options specified.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show logs [ active ] [ inactive ] [ callid call_id ] [ encrypted-li ] [
event-verbosity evt_verbosity ] [ facility facility ] [ level severity_level
] [ pdu-data pdu_format ] [ pdu-verbosity pdu_verbosity ] [ proclat facility
] [ since from_date_time [ until to_date_time ] ] [ | { grep grep_options | more
} ]
```

**active**

Displays data from active logs.

**inactive**

Displays data from inactive logs.

**callid *call\_id***

Displays log information only for a call ID specified as a 4-digit hexadecimal number.

**encrypted-li**

This keyword is only visible to an administrator with li-privilege. It displays the boot config output for the encrypted LI configuration when **require segregated li-configuration** has been enabled.

**Note**

For additional information, see the *Lawful Intercept Configuration Guide*.

**event-verbosity *evt\_verbosity***

Specifies the level of verbosity to use in displaying of event data as one of:

- **min** - displays minimal information about the event. Information includes event name, facility, event ID, severity level, date, and time.



- **concise** - displays detailed information about the event, but does not provide the event source within the system.
- **full** - displays detailed information about event, including source information, identifying where within the system the event was generated.

### **facility** *facility*

Specifies the facility to modify the filtering of logged information for as one of:

- **a10**: A10 interface facility
- **a11**: A11 interface facility
- **a11mgr**: A11 Manager facility
- **aaa-client**: Authentication, Authorization and Accounting (AAA) client facility
- **aaamgr**: AAA manager logging facility
- **aaaproxy**: AAA Proxy facility
- **aal2**: ATM Adaptation Layer 2 (AAL2) protocol logging facility
- **acl-log**: Access Control List (ACL) logging facility
- **acsctrl**: Active Charging Service (ACS) Controller facility
- **acsmgr**: ACS Manager facility
- **afctrl**: Fabric Controller facility [ASR 5500 only]
- **afmgr**: Fabric Manager logging facility [ASR 5500 only]
- **alarmctrl**: Alarm Controller facility
- **alcap**: Access Link Control Application Part (ALCAP) protocol logging facility
- **alcapmgr**: ALCAP manager logging facility
- **all**: All facilities
- **asnngwmgr**: Access Service Network (ASN) Gateway Manager facility
- **asnpemgr**: ASN Paging Controller Manager facility
- **bfd**: Bidirectional Forwarding Detection (BFD) protocol logging facility
- **bgp**: Border Gateway Protocol (BGP) facility
- **bindmux**: IPCF BindMux-Demux Manager logging facility
- **bngmgr**: Broadband Network Gateway (BNG) Demux Manager logging facility
- **bssap+**: Base Station Sub-system Application Part+ protocol facility for the login interface between the SGSN and the MSC/VLR (2.5G and 3G)
- **bssgp**: Base Station Sub-system GPRS Protocol logging facility handles exchange information between the SGSN and the BSS (2.5G only)
- **bulkstat**: Statistics logging facility

- **callhome**: Call Home application logging facility
- **cap**: CAMEL Application Part (CAP) logging facility for protocol used in prepaid applications (2.5G and 3G)
- **cbsmgr**: Cell Broadcasting Service (CBS) logging facility [HNBGW]




---

**important** In Release 20 and later, HNBGW is not supported. This keyword must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

---

- **cdf**: Charging Data Function (CDF) logging facility
- **cgw**: Converged Access Gateway (CGW) logging facility
- **cli**: Command Line Interface (CLI) logging facility
- **cmp**: Certificate Management Protocol (IPSec) logging facility
- **confdmgr**: ConfD Manager proctlet (NETCONF) logging facility
- **connectedapps**: SecGW ASR 9000 oneP communication proctlet
- **connproxy**: Controller Proxy logging facility
- **credit-control**: Credit Control (CC) facility
- **esp**: Card/Slot/Port controller facility
- **css**: Content Service Selection (CSS) facility
- **css-sig**: CSS RADIUS Signaling facility
- **cx-diameter**: Cx Diameter Messages facility [CSCF <--> HSS]
- **data-mgr**: Data Manager Framework logging facility
- **dcardctrl**: IPSec Daughter Card Controller logging facility
- **dcardmgr**: IPSec Daughter Card Manager logging facility
- **demuxmgr**: Demux Manager API facility
- **dgmbmgr**: Diameter Gmb Application Manager logging facility
- **dhcp**: Dynamic Host Configuration Protocol (DHCP) logging facility
- **dhcpv6**: DHCPv6
- **dhost**: Distributed Host logging facility
- **diabase**: Diabase messages facility
- **diactrl**: Diameter Controller proctlet logging facility
- **diameter**: Diameter endpoint logging facility
- **diameter-acct**: Diameter Accounting

- **diameter-auth**: Diameter Authentication
- **diameter-dns**: Diameter DNS subsystem
- **diameter-ecs**: ACS Diameter signaling facility
- **diameter-engine**: Diameter version2 engine logging facility
- **diameter-hdd**: Diameter Horizontal Directional Drilling (HDD) Interface facility
- **diameter-svc**: Diameter Service
- **diamproxy**: DiamProxy logging facility
- **dpath**: IPSec Data Path facility
- **drvctrl**: Driver Controller facility
- **dpath**: IPSec Data Path logging facility
- **drvctrl**: Driver Controller logging facility
- **doulosuemgr**: Doulos (IMS-IPSec-Tool) user equipment manager
- **eap-diameter**: Extensible Authentication Protocol (EAP) IP Sec urity facility
- **eap-ipsec**: Extensible Authentication Protocol (EAP) IPSec facility
- **eap-sta-s6a-s13-s6b-diameter**: EAP/STA/S6A/S13/S6B Diameter messages facility
- **ecs-css**: ACSMGR <-> Session Manager Signalling Interface facility
- **egtpc**: eGTP-C logging facility
- **egtpmgr**: enhanced GPRS Tunneling Protocol (eGTP) manager logging facility
- **egtpu**: eGTP-U logging facility
- **embms**: evolved Multimedia Broadcast Multicast Services Gateway facility
- **embms**: eMBMS Gateway Demux facility
- **epdg**: evolved Packet Data (ePDG) gateway logging facility
- **event-notif**: Event Notification Interface logging facility
- **evlog**: Event log facility
- **famgr**: Foreign Agent manager logging facility
- **firewall**: Firewall logging facility
- **fng**: Femto Network Gateway (FNG) logging facility
- **gbmgr**: SGSN Gb Interface Manager facility
- **gmm**:
  - For 2.5G: Logs the GPRS Mobility Management (GMM) layer (above LLC layer)
  - For 3G: Logs the access application layer (above the RANAP layer)

- **gprs-app**: GPRS Application logging facility
- **gprs-ns**: GPRS Network Service Protocol (layer between SGSN and the BSS) logging facility
- **gq-rx-tx-diameter**: Gq/Rx/Tx Diameter messages facility
- **gss-gcdr**: GTP Storage Server GCDR facility
- **gtpc**: GTP-C protocol logging facility
- **gtpcmgr**: GTP-C protocol manager logging facility
- **gtpp**: GTP-prime protocol logging facility
- **gtpu**: GTP-U protocol logging facility
- **gtpumgr**: GTP-U Demux manager
- **gx-ty-diameter**: Gx/Ty Diameter messages facility
- **gy-diameter**: Gy Diameter messages facility
- **h248prt**: H.248 port manager facility
- **hamgr**: Home Agent manager logging facility
- **hat**: High Availability Task (HAT) process facility
- **hdctrl**: HD Controller logging facility
- **henbapp**: Home Evolved NodeB (HENB) App facility




---

**important** In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

- **henbgw**: HENB-GW facility




---

**important** In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

- **henbgw-pws**: HENB-GW Public Warning System logging facility




---

**important** In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

- **henbgw-sctp-acs**: HENB-GW access Stream Control Transmission Protocol (SCTP) facility




---

**hpbat** In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

- **henbgw-sctp-nw**: HENBGW network SCTP facility




---

**hpbat** In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

- **henbgwdemux**: HENB-GW Demux facility




---

**hpbat** In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

- **henbgwmgr**: HENB-GW Manager facility




---

**hpbat** In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

- **hnb-gw**: HNB-GW (3G Femto GW) logging facility




---

**hpbat** In Release 20 and later, HNBGW is not supported. This keyword must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

---

- **hnbmgr**: HNB-GW Demux Manager logging facility




---

**hpbat** In Release 20 and later, HNBGW is not supported. This keyword must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

---

- **hss-peer-service**: Home Subscriber Server (HSS) Peer Service facility
- **igmp**: Internet Group Management Protocol (IGMP)
- **ikev2**: Internet Key Exchange version 2 (IKEv2)
- **ims-authorization**: IP Multimedia Subsystem (IMS) Authorization Service facility

- **ims-sh**: HSS Diameter Sh Interface Service facility
- **imsimgr**: SGSN IMSI Manager facility
- **imsue**: IMS User Equipment (IMSUE) facility
- **ip-arp**: IP Address Resolution Protocol facility
- **ip-interface**: IP interface facility
- **ip-route**: IP route facility
- **ipms**: Intelligent Packet Monitoring System (IPMS) logging facility
- **ipne**: IP Network Enabler (IPNE) facility
- **ipsec**: IP Security logging facility
- **ipsecdemux**: IPSec demux logging facility
- **ipsg**: IP Service Gateway interface logging facility
- **ipsgmgr**: IP Services Gateway facility
- **ipsp**: IP Pool Sharing Protocol logging facility
- **kvstore**: Key/Value Store (KVSTORE) Store facility
- **l2tp-control**: Layer 2 Tunneling Protocol (L2TP) control logging facility
- **l2tp-data**: L2TP data logging facility
- **l2tpdemux**: L2TP Demux Manager logging facility
- **l2tpmgr**: L2TP Manager logging facility
- **lagmgr**: Link Aggregation Group (LAG) manager logging facility
- **lcs**: Location Services (LCS) logging facility
- **ldap**: Lightweight Directory Access Protocol (LDAP) messages logging facility
- **li**: Refer to the *Lawful Intercept Configuration Guide* for a description of this command.
- **linkmgr**: SGSN/BSS SS7 Link Manager logging facility (2.5G only)
- **llc**: Logical Link Control (LLC) Protocol logging facility; for SGSN: logs the LLC layer between the GMM and the BSSGP layers for logical links between the MS and the SGSN
- **local-policy**: Local Policy Service facility
- **location-service**: Location Services facility
- **m3ua**: M3UA Protocol logging facility
- **magmgr**: Mobile Access Gateway manager logging facility
- **map**: Mobile Application Part (MAP) protocol logging facility
- **megadiammgr**: MegaDiameter Manager (SLF Service) logging facility
- **mme-app**: Mobility Management Entity (MME) Application logging facility

- **mme-misc**: MME miscellaneous logging facility
- **mmedemux**: MME Demux Manager logging facility
- **mmemgr**: MME Manager facility
- **mmgr**: Master Manager logging facility
- **mobile-ip**: Mobile IP processes
- **mobile-ip-data**: Mobile IP data facility
- **mobile-ipv6**: Mobile IPv6 logging facility
- **mpls**: Multiprotocol Label Switching (MPLS) protocol logging facility
- **mrme**: Multi Radio Mobility Entity (MRME) logging facility
- **mseg-app**: Mobile Services Edge Gateway (MSEG) application logging facility (This option is not supported in this release.)
- **mseg-gtpc**: MSEG GTP-C application logging facility (This option is not supported in this release.)
- **mseg-gtpu**: MSEG GTP-U application logging facility (This option is not supported in this release.)
- **msegmgr**: MSEG Demux Manager logging facility (This option is not supported in this release.)
- **mtp2**: Message Transfer Part 2 (MTP2) Service logging facility
- **mtp3**: Message Transfer Part 3 (MTP3) Protocol logging facility
- **multicast-proxy**: Multicast Proxy logging facility
- **nas**: Non-Access Stratum (NAS) protocol logging facility [MME 4G]
- **netwstrg**: Network Storage facility
- **npuctrl**: Network Processor Unit Control facility
- **npudrv**: Network Processor Unit Driver facility [ASR 5500 only]
- **npumgr**: Network Processor Unit Manager facility
- **npumgr-acl**: NPUMGR ACL logging facility
- **npumgr-drv**: NPUMGR DRV logging facility
- **npumgr-flow**: NPUMGR FLOW logging facility
- **npumgr-fwd**: NPUMGR FWD logging facility
- **npumgr-init**: NPUMGR INIT logging facility
- **npumgr-lc**: NPUMGR LC logging facility
- **npumgr-port**: NPUMGR PORT logging facility
- **npumgr-recovery**: NPUMGR RECOVERY logging facility
- **npumgr-rri**: NPUMGR RRI (Reverse Route Injection) logging facility
- **npumgr-vpn**: NPUMGR VPN logging facility
- **npusim**: NPUSIM logging facility [ASR 5500 only]

- **ntfy-intf**: Notification Interface logging facility [Release 12.0 and earlier versions only]
- **ocsp**: Online Certificate Status Protocol logging facility.
- **orbs**: Object Request Broker System logging facility
- **ospf**: OSPF protocol logging facility
- **ospfv3**: OSPFv3 protocol logging facility
- **p2p**: Peer-to-Peer Detection logging facility
- **pagingmgr**: PAGINGMGR logging facility
- **pccmgr**: Intelligent Policy Control Function (IPCF) Policy Charging and Control (PCC) Manager library
- **pdg**: Packet Data Gateway (PDG) logging facility
- **pdgmgr**: PDG Demux Manager logging facility
- **pdif**: Packet Data Interworking Function (PDIF) logging facility
- **pgw**: Packet Data Network Gateway (PGW) logging facility
- **pmm-app**: Packet Mobility Management (PMM) application logging facility
- **ppp**: Point-To-Point Protocol (PPP) link and packet facilities
- **pppoe**: PPP over Ethernet logging facility
- **proclat-map-frwk**: Proclat mapping framework logging facility
- **push**: VPNMGR CDR push logging facility
- **radius-acct**: RADIUS accounting logging facility
- **radius-auth**: RADIUS authentication logging facility
- **radius-coa**: RADIUS change of authorization and radius disconnect
- **ranap**: Radio Access Network Application Part (RANAP) Protocol facility logging info flow between SGSN and RNS (3G)
- **rct**: Recovery Control Task logging facility
- **rdt**: Redirect Task logging facility
- **resmgr**: Resource Manager logging facility
- **rf-diameter**: Diameter Rf interface messages facility
- **rip**: Routing Information Protocol (RIP) logging facility [RIP is not supported at this time.]
- **rlf**: Rate Limiting Function (RLF) logging facility
- **rohc**: Robust Header Compression (RoHC) facility
- **rsvp**: Reservation Protocol logging facility
- **rua**: RANAP User Adaptation (RUA) [3G Femto GW - RUA messages] logging facility
- **s102**: S102 protocol logging facility



- **s102mgr**: S102Mgr logging facility
- **s1ap**: S1 Application Protocol (S1AP) Protocol logging facility
- **sabp**: Service Area Broadcast Protocol (SABP) logging facility
- **saegw**: System Architecture Evolution (SAE) Gateway facility
- **sbc**: SBc protocol logging facility
- **sccp**: Signalling Connection Control Part (SCCP) Protocol logging (connection-oriented messages between RANAP and TCAP layers).
- **sct**: Shared Configuration Task logging facility
- **sctp**: Stream Control Transmission Protocol (SCTP) Protocol logging facility
- **sef\_ecs**: Severely Errored Frames (SEF) APIs printing facility
- **sess-gr**: SM GR facility
- **sessctrl**: Session Controller logging facility
- **sessmgr**: Session Manager logging facility
- **sesstrc**: session trace logging facility
- **sft**: Switch Fabric Task logging facility
- **sgs**: SGs interface protocol logging facility
- **sgsn-app**: SGSN-APP logging various SGSN "glue" interfaces (for example, between PMM, MAP, GPRS-FSM, SMS).
- **sgsn-failures**: SGSN call failures (attach/activate rejects) logging facility (2.5G)
- **sgsn-gtpc**: SGSN GTP-C Protocol logging control messages between the SGSN and the GGSN
- **sgsn-gtpu**: SGSN GTP-U Protocol logging user data messages between the SGSN and GGSN
- **sgsn-mbms-bearer**: SGSN Multimedia Broadcast/Multicast Service (MBMS) Bearer app (SMGR) logging facility
- **sgsn-misc**: Used by stack manager to log binding and removing between layers
- **sgsn-system**: SGSN System Components logging facility (used infrequently)
- **sgsn-test**: SGSN Tests logging facility; used infrequently
- **sgtpcmgr**: SGSN GTP-C Manager logging information exchange through SGTPC and the GGSN
- **sgw**: Serving Gateway facility
- **sh-diameter**: Sh Diameter messages facility
- **sitmain**: System Initialization Task main logging facility
- **sls**: Service Level Specification (SLS) protocol logging facility
- **sm-app**: SM Protocol logging facility
- **sms**: Short Message Service (SMS) logging messages between the MS and the SMSC

- **sndcp**: Sub Network Dependent Convergence Protocol (SNDCP) logging facility
- **snmp**: SNMP logging facility
- **sprmgr**: IPCF Subscriber Policy Register (SPR) manager logging facility
- **srdp**: Static Rating Database
- **srp**: Service Redundancy Protocol (SRP) logging facility
- **sscfmi**: Service-Specific Coordination Function for Signaling at the Network Node Interface (SSCF-NNI) logging facility
- **sscop**: Service-Specific Connection-Oriented Protocol (SSCOP) logging facility
- **ssh-ipsec**: Secure Shell (SSH) IP Security logging facility
- **ssl**: Secure Socket Layer (SSL) message logging facility
- **stat**: Statistics logging facility




---

**hptat** The keyword **bulkstat** was added in StarOS release 21.1 to provide consistency with other CLI commands. Both keywords are supported for statistics logging facility.

---

- **supserv**: Supplementary Services logging facility [H.323]
- **system**: System logging facility
- **tacacsplus**: TACACS+ Protocol logging facility
- **tcap**: TCAP Protocol logging facility
- **testctrl**: Test Controller logging facility
- **testmgr**: Test Manager logging facility
- **threshold**: threshold logging facility
- **ttg**: Tunnel Termination Gateway (TTG) logging facility
- **tucl**: TCP/UDP Convergence Layer (TUCL) logging facility
- **udr**: User Data Record (UDR) facility (used with the Charging Service)
- **user-data**: User data logging facility
- **user-l3tunnel**: User Layer 3 tunnel logging facility
- **usertcp-stack**: User TCP Stack
- **vim**: Voice Instant Messaging (VIM) logging facility
- **vinfo**: VINFO logging facility
- **vmgctrl**: Virtual Media Gateway (VMG) controller facility
- **vmgctrl**: VMG Content Manager facility
- **vpn**: Virtual Private Network logging facility

- **wimax-data**: WiMAX DATA
- **wimax-r6**: WiMAX R6
- **wsg**: Wireless Security Gateway (ASR 9000 Security Gateway)
- **x2gw-app**: X2GW (X2 proxy Gateway, eNodeB) application logging facility
- **x2gw-demux**: X2GW demux task logging facility

### **level severity\_level**

**level severity\_level**: Specifies the level of information to be logged from the following list which is ordered from highest to lowest:

- **critical** - display critical events
- **error** - display error events and all events with a higher severity level
- **warning** - display warning events and all events with a higher severity level
- **unusual** - display unusual events and all events with a higher severity level
- **info** - display info events and all events with a higher severity level
- **trace** - display trace events and all events with a higher severity level
- **debug** - display all events

### **pdu-data pdu\_format**

Specifies output format for the display of packet data units as one of:

- **none** - output is in raw format (unformatted).
- **hex** - output being displayed in hexadecimal format.
- **hex-ascii** - output being displayed in hexadecimal and ASCII similar to a main-frame dump.

### **pdu-verbosity pdu\_verbosity**

Specifies the level of verbosity to use in displaying of packet data units as an integer from 1 through 5, where 5 is the most detailed.

### **proclat facility**

Shows the logs from a specific proclat facility. The available facilities are the same as those listed earlier.

### **since from\_date\_time [ until to\_date\_time ]**

Default: no limit.

**since from\_date\_time**: indicates only the log information which has been collected more recently than **from\_date\_time** is to be displayed.

**until to\_date\_time**: indicates no log information more recent than **to\_date\_time** is to be displayed. **until** defaults to current time when omitted.

*from\_date\_time* and *to\_date\_time* must be formatted as YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss. Where:

- YYYY = 4-digit year
- MM = 2-digit month in the range 01 through 12
- DD = 2-digit day in the range 01 through 31
- HH = 2-digit hour in the range 00 through 23
- mm = 2-digit minute in the range 00 through 59
- ss = 2-digit second in the range 00 through 59

*to\_date\_time* must be a time which is more recent than *from\_date\_time*.

The use of the **until** keyword allows for a time range of log information while only using the **since** keyword will display all information up to the current time.

### **{ grep grep\_options | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### **Usage Guidelines**

View log files for general maintenance or troubleshooting system issues.

### **Example**

The following command displays log information for the *allmgr* facility starting with July 1th, 2011 at midnight.

```
show logs facility allmgr since 2011:07:11:00:00
```

The following command displays the log information for call ID *FE881D32* only in active logs.

```
show logs active callid FE881D32
```

## **show lte-policy**

Displays information for Long term Evolution (LTE) policy configurations on this system including congestion action profiles, handover restriction lists, paging maps, paging profiles, subscriber maps, and tracking area identifiers (TAIs).

### **Product**

HeNBGW  
MME  
SAEGW  
S-GW

---

**Privilege** Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
show lte-policy { cause-code-group { name group_name | summary } |
congestion-action-profile { name congest_profile_name | summary } |
foreign-plmn-guti-mgmt-db { name db_name | summary } | henbgw { mme-pool
{ name mme_pool_name | summary } | qci-dscp-mapping-table { name table_name
| summary } | overload-control | s1-reset | session-recovery } |
ho-restriction-list { name ho_list_name | summary } | lte-emergency-profile
{ name emer_profile_name | summary } | mme { henbgw mgmt-db { name
henbgw_mgmt_db_name | summary } | paging cache parameters | paging-map { name
page_map_name | summary } | paging-profile { name page_profile_name | summary
} | peer-map { name sub_map_name | summary } | subscriber-map { name
sub_map_name | summary } | tai-list-db { name tai_list_name summary } |
tai-mgmt-db { name tai_name [ tai-mgmt-obj name obj_name | tai-custom-list
tac cstm_tac_value ] | summary } } [ | { grep grep_options | more } ]
```

**cause-code-group** { **name** *group\_name* | **summary** }

This MME-specific keyword displays information about the Cause Code Groups configured on this system.

**name** *group\_name*: Displays information about a specific cause code group configured on this system.

*group\_name* must be an existing cause code group, expressed as an alphanumeric string of 1 to 16 characters.

**summary**: Displays summarized information about all cause code groups configured on this system.

**congestion-action-profile** { **name** *congest\_profile\_name* | **summary** }

Displays information about MME congesting action profiles configured on this system.

**name** *profile\_name*: Displays information about a specific congestion action profile configured on this system.

*profile\_name* must be an existing HO restriction list, expressed as an alphanumeric string of 1 to 64 characters.

**summary**: Displays summarized information about all congestion action profiles configured on this system.

**foreign-plmn-guti-mgmt-db** { **name** *db\_name* | **summary** }

This MME-specific keyword displays information about LTE Foreign PLMN GUTI management databases configured on this system.

**name** *db\_name*: Displays information about a specific management database configured on this system.

*db\_name* must be an existing management database, expressed as an alphanumeric string of 1 to 64 characters.

**summary**: Displays summarized information about all Foreign PLMN GUTI management databases configured on this system.

**henbgw** { **mme-pool** { **name** *mme\_pool\_name* | **summary** } | **qci-dscp-mapping-table** { **name** *table\_name* | **summary** } | **overload-control** | **session-recovery** }

This HeNBGW keyword displays information about HeNBGW configured on this system.

**Important**

In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

**mme-pool** shows mme pool.

**name** *mme\_pool\_name*: Displays detailed information about specified MME Pool configured on this system. *mme\_pool\_name* must be an existing management database, expressed as an alphanumeric string of 1 to 63 characters.

**summary**: Displays summarized information about MME Pool configured on this system.

**qci-dscp-mapping-table** shows qci-dscp-mapping-table information.

**name** *table\_name*: Displays information for specific qci-dscp-mapping-table. *table\_name* must be qci-dscp-mapping-table expressed as an alphanumeric string of 1 to 63 characters.

**summary**: Displays summary of all qci-dscp-mapping-table.

**overload-control**: Displays information about overload control.

**s1-reset**: Displays information about s1 reset.

**session-recovery**: Displays information about session recovery.

**ho-restriction-list { name *list\_name* | summary }**

Displays information about handover restriction lists configured on this system.

**name** *ho\_list\_name*: Displays information about a specific handover restriction list configured on this system. *name* must be an existing HO restriction list, expressed as an alphanumeric string of 1 to 64 characters.

**summary**: Displays summarized information about all handover restriction lists configured on this system.

**lte-emergency-profile { name *emer\_profile\_name* | summary }**

Displays information about LTE emergency profiles configured on this system.

**name** *emer\_profile\_name*: Displays information about a specific LTE emergency profile configured on this system. *emer\_profile\_name* must be an existing LTE emergency profile, expressed as an alphanumeric string of 1 to 64 characters.

**summary**: Displays summarized information about all LTE emergency profiles configured on this system.

**mme paging cache parameters**

Displays the configured MME paging cache timeout and MME paging cache size configured with the **mme paging cache** command in the LTE Policy configuration mode.

**paging-map { name *page\_map\_name* | summary }**

Displays information about LTE paging maps configured on this system.

**name** *page\_map\_name*: Displays information about an existing LTE paging map specified as an alphanumeric string of 1 through 64 characters.

**summary**: Displays summarized information about all LTE paging maps configured on this system.

**paging-profile { name *page\_profile\_name* | summary }**

Displays information about LTE paging profiles configured on this system.

**name** *page\_profile\_name*: Displays information about an existing LTE paging profile specified as an alphanumeric string of 1 through 64 characters.

**summary**: Displays summarized information about all LTE paging profiles configured on this system.

**peer-map { name *name* | summary }**

Displays information about peer maps configured on this system.

**name** *map\_name*: Displays information about an existing peer map specified as an alphanumeric string of 1 through 64 characters.

**summary**: Displays summarized information about all peer maps configured on this system.

**subscriber-map { name *name* | summary }**

Displays information about subscriber maps configured on this system.

**name** *sub\_map\_name*: Displays information about an existing subscriber map specified as an alphanumeric string of 1 through 64 characters.

**summary**: Displays summarized information about all subscriber maps configured on this system.

**tai-list-db { name *tai\_list\_name* | summary }**

Displays information about TAI list databases configured on this system

**name** *tai\_list\_name*: Displays information about specified TAI list database as an alphanumeric string of 1 through 64 characters.

**summary**: Displays summarized information about specified TAI list databases configured on this system.

**tai-mgmt-db { name *name* [ tai-mgmt-obj name *obj\_name* | tai-custom-list tac *cstm\_tac\_value* ] | summary }**

Displays information about TAI management databases configured on this system.

**name** *tai\_name*: Displays information about an existing TAI management database specified as an alphanumeric string of 1 through 64 characters.

**tai-mgmt-obj name** *obj\_name* : Filters the information by the specified TAI Management Object name, where *obj\_name* is a string from 1 through 64 characters.

**tai-custom-list tac** *cstm\_tac\_value* : Filters the information by the specified Custom TAI List TAC, where *cstm\_tac\_value* is an integer from 0 through 65535.

**summary**: Displays summarized information about all TAI management databases configured on this system.

**{ *grep grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *CLI Overview* chapter.

---

**Usage Guidelines**

Use this command to display information for LTE policy configurations on this system including congestion action profiles, handover restriction lists, paging maps, paging profiles, subscriber maps, and tracking area identifiers (TAIs).

**Example**

The following command displays information about a subscriber map named *map3*:

```
show lte-policy subscriber-map name map3
```



---

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---





## CHAPTER 22

# Exec Mode show Commands (M-P)

The Exec Mode is the initial entry point into the command line interface system. Exec mode **show** commands are useful in troubleshooting and basic system monitoring.

### Command Modes

This section includes the commands **show mag-service** through **show ps-network statistics**.

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```



### Important

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

- [show mag-service, on page 981](#)
- [show map-service, on page 983](#)
- [show map statistics, on page 983](#)
- [show maximum-temperatures, on page 984](#)
- [show mbms bearer-service, on page 985](#)
- [show mipfa, on page 987](#)
- [show mipha, on page 989](#)
- [show mipv6ha, on page 992](#)
- [show mme-embms-service, on page 994](#)
- [show mme-hss session, on page 996](#)
- [show mme-service, on page 998](#)
- [show mme-service db record, on page 999](#)
- [show mme-service db statistics, on page 1000](#)
- [show mme-service enodeb-association, on page 1001](#)
- [show mme-service id, on page 1002](#)
- [show mme-service session, on page 1003](#)
- [show mme-service statistics, on page 1006](#)
- [show module, on page 1008](#)
- [show mpls cross-connect, on page 1009](#)
- [show mpls ftn, on page 1010](#)
- [show mpls ilm, on page 1011](#)

- [show mpls ldp](#), on page 1012
- [show mpls nexthop-label-forwarding-entry](#), on page 1013
- [show mrme-service](#), on page 1014
- [show mrme-service active-session](#), on page 1015
- [show mrme-service imsi-sticky](#), on page 1015
- [show mrme-service mac-sticky](#), on page 1016
- [show mseg-config](#), on page 1017
- [show mseg-service](#), on page 1017
- [show multicast-sessions](#), on page 1017
- [show network-requested-pdp-context](#), on page 1019
- [show network-service-entity](#), on page 1020
- [show npu arp](#), on page 1021
- [show npu error-counters](#), on page 1021
- [show npu tm](#), on page 1022
- [show npu utilization](#), on page 1023
- [show ntp](#), on page 1024
- [show nw-reachability server](#), on page 1025
- [show operator-policy](#), on page 1026
- [show orbem](#), on page 1027
- [show patch progress](#), on page 1028
- [show pcc-af service](#), on page 1029
- [show pcc-af session](#), on page 1030
- [show pcc-policy service](#), on page 1032
- [show pcc-policy session](#), on page 1033
- [show pcc-service](#), on page 1034
- [show pcc-service session](#), on page 1035
- [show pcc-service statistics](#), on page 1037
- [show pcc-sp-endpoint](#), on page 1038
- [show pcc-sp-endpoint connection](#), on page 1039
- [show pdg-service](#), on page 1040
- [show pdg-service statistics](#), on page 1041
- [show pdif-service](#), on page 1042
- [show pdn-connection-count](#), on page 1043
- [show pdsn-service](#), on page 1043
- [show pdsnclosedrp-service](#), on page 1045
- [show peer-profile](#), on page 1045
- [show pgw-service](#), on page 1046
- [show plugin](#), on page 1047
- [show port](#), on page 1048
- [show power](#), on page 1050
- [show ppp](#), on page 1051
- [show prepaid 3gpp2](#), on page 1053
- [show prepaid wimax](#), on page 1054
- [show process status](#), on page 1055
- [show profile-id-qci-mapping](#), on page 1056
- [show ps-network](#), on page 1057

- [show ps-network counters](#), on page 1058
- [show ps-network statistics](#), on page 1059

## show mag-service

Displays statistic and counter information for Mobile Access Gateway (MAG) services on this system.

<b>Product</b>	HSGW S-GW
----------------	--------------

<b>Privilege</b>	Inspector
------------------	-----------

<b>Command Modes</b>	Exec
----------------------	------

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

<b>Syntax Description</b>	<pre>show mag-service { all   name <i>service_name</i>   session [ all   callid <i>id</i>   counters   full   ip-address <i>home_ip_address</i>   msid <i>id</i>   summary   username <i>name</i> ]   statistics [ name <i>service_name</i> ] } [   { grep <i>grep_options</i>   more } ]</pre>
---------------------------	---

### all

Displays information for all configured MAG services on this system.

### name *service\_name*

Displays configuration information for a specific MAG service configured on this system.

*service\_name* must be an existing MAG service expressed as an alphanumeric string of 1 through 63 characters.

**session [ all | callid *id* | counters | full | ip-address *home\_ip\_address* | msid *id* | summary | username *name* ]**

**all:** Displays all active MAG sessions using MAG services on the system.

**callid *id*:** Displays available session information for the specific call identification number.

*id* must be an 8-digit hexadecimal number.

**counters:** Displays counters for all MAG services on the system. This keyword can also be filtered by the following:

- all
- callid
- ip-address
- msid
- summary
- username

Refer to the keyword descriptions in this command for information regarding these filters.

**full**: Displays additional session information for all active MAG sessions using MAG services on the system. This keyword includes the information in the output of the **all** keyword plus additional information. This keyword can also be filtered by the following:

- **all**
- **callid**
- **ip-address**
- **msid**
- **summary**
- **username**

Refer to the keyword descriptions in this command for information regarding these filters.

**ip-address** *home\_ip\_address*: Displays available session information for a specific home IPv4 or IPv6 address of a subscriber in a service session.

**msid** *id*: Displays available information for a specific mobile station identification number or group of numbers based on wildcard entry.

*id* must be a valid MSID number and can be a sequence of characters and/or wildcard characters ('\$' and/or '\*'). The \* wildcard matches multiple characters and the \$ wildcard matches a single character. If you do not want the wildcard characters interpreted as wildcard enclose them in single quotes (' '). For example: '\$'.

**summary**: Displays the number of MAG sessions currently active for MAG services configured on the system.

**username** *name*: Displays available session information for a specific user in a service session.

*name* must be followed by an existing user name expressed as an alphanumeric string of 1 through 127 characters.

#### **statistics [ name service\_name ]**

**name** *service\_name*: Displays MAG service statistics for an existing MAG service specified as an alphanumeric string of 1 through 63 characters.

#### **{ grep grep\_options | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to view configuration information for MAG services on this system.

### Example

The following command displays service statistics for the MAG service named *mag1*:

```
show mag-service name mag1
```

## show map-service

Displays information configured for the Mobile Application Part (MAP) services, including MAP service features and operational configuration. Also includes some related configuration information for the HLR and EIR configuration parameters.

---

**Product** SGSN

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show map-service** [ **all** | **name** *svrc\_name* ] [ | { **grep** *grep\_options* | **more** } ]

**name** *svrc\_name*

Specifies an existing MAP service as an alphanumeric string of 1 through 63 characters.

{ **grep** *grep\_options* | **more** }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines** Use this command to display all MAP service or the statistics for a particular MAP service.

### Example

The following command displays configuration information for the MAP service named *map-svc-1*:

```
show map-service name map-srv-1
```




---

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show map statistics

Displays Mobile Application Part (MAP) statistics.

---

**Product** SGSN

---

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

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show map statistics [ name svrc_name ] [ recovered-values ] [ | { grep
grep_options | more } ]
```

**name *svrc\_name***

Specifies an existing MAP service as an alphanumeric string of 1 through 63 characters.

**recovered-values**

Only displays recovered values for key KPI counters that were backed-up.

**{ **grep** *grep\_options* | **more** }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display all MAP statistics or the statistics for a particular MAP service.

**Example**

The following command displays statistics for the MAP service named *map-svc-1*:

```
show map statistics name map-svc-1
```

The following command displays combined statistics for all MAP services in the current context:

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show maximum-temperatures

Shows the maximum temperature reached by each card since the last temperature timestamp reset.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show maximum-temperatures [ verbose] [ | { grep grep_options | more } ]`

**verbose**

Indicates that the output is to contain detailed information.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines** Verify the maximum temperature reached by components in the chassis since the indicated timestamp.

**Important**

This command is not supported on all platforms.

---

**Example**

```
show maximum-temperatures
show maximum-temperatures verbose
```

## show mbms bearer-service

Displays configuration information for bearer services configured for the multimedia broadcast multicast service (MBMS) running on this system.

---

**Product** GGSN  
SGSN

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show mbms bearer-service [ all ] [ apn apn_name mcast-addr ip_address ] [ full ] [ instance instance_id ] [ service-type { broadcast | multicast } ] [ sgsn-sessions ] [ summary ] [ | { grep grep_options | more } ]`

**all**

Displays information on all bearer services configured on the system.

**apn *apn\_name* mcast-addr *ip\_address***

Displays bearer service information of the MBMS for a specific Access Point Name (APN). *apn\_name* is bound to a given BM-SC (Broadcast Multicast - Service Center) server address *ip\_address*.

*apn\_name* is the name of the APN expressed as an alphanumeric string of 1 through 62 characters that is case sensitive.

*ip\_address* is the IP address of the BM-SC server in IPv4 dotted-decimal notation bound to the APN.

**full**

Displays full information for specific or all instances of bearer service in MBMS feature on system.

**instance *instance\_id***

Displays session information filtered for an instance of a bearer service running as an MBMS session and specified an integer from 1 through 64.

**service-type { broadcast | multicast }**

Displays information for a specific type of service for MBMS.

**broadcast:** Specifies the MBMS service type as broadcast only.

**multicast:** Specifies the MBMS service type as multicast only.

**sgsn-sessions**

Displays summary information for all the SGSN multicast sessions.

**summary**

Displays summary information for specific or all instances of a bearer service.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more** options, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to verify the configuration of one or all bearer services and active instances of bearer services under MBMS. It is also useful for monitoring or troubleshooting purposes.

If this command is executed from within the local context with the **all** keyword, information for all bearer service instances running under MBMS will be displayed.

**Example**

The following command displays configuration information for all bearer service instances running on system:

```
show mbms bearer-service full all
```



**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show mipfa

Displays information for specified Mobile IP Foreign Agent (MIP-FA) calls.

**Product**

PDSN

GGSN

ASN-GW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show mipfa { [ [ counters | full | summary ] { all | callid call_id | msid
ms_id | peer-address [ operator ] peer_address | reverse-tunnel { on | off }
| username user_name } | statistics [ fa-service fa_name | peer-address [
peer_address | greater-than peer_address | less-than peer_address | > peer_address
| < peer_address ] } ] | peers fa-service service_name [ current-sessions {
{ > | greater-than } sessions [ < sessions ] | { < | less-than } sessions [ >
sessions ] | sessions } ] [ peer-address address ] } [ | { grep grep_options |
more } ]
```

**counters | full | summary**

**counters:** Displayed output includes the statistical counters.

**full:** Displays detailed information.

**summary:** Displays only summary information. this is the default setting.

These options are not available in conjunction with the **statistics** keyword.

**all | callid call\_id | msid ms\_id | peer-address peer\_ip\_address | reverse-tunnel { on | off } | username user\_name**

**all:** Displays all available information.

**callid call\_id:** Displays information only for calls with the call ID specified as a 4-byte hexadecimal number.

**msid ms\_id:** Displays information for a mobile subscriber ID expressed as a string from 7 to 16 digits for an IMSI, MIN, or RMI and/or characters \$ and \* for wildcard filter.

**show mipfa msid 01234567\$\$**

Shows any subscriber with an MSID that matches the upper 8 digits of the supplied MSID, such as 01234567, and any two digits at the remaining two places.

**peer-address** *peer\_ip\_address*: Displays information for the MIP call for the peer IP address specified using IPv4 dotted-decimal notation.

**reverse-tunnel** { **on** | **off** }: Enables the display of reverse IP tunnel information.

**username** *user\_name*: Displays MIP call user information for the username specified as an alphanumeric string of 1 through 127 characters that may include wildcard characters (\$ and \*).

**statistics** [ **fa-service** *fa\_name* | **peer-address** [ *peer\_address* | **greater-than** *peer\_address* | **less-than** *peer\_address* | **>** *peer\_address* | **<** *peer\_address* ]

Displays information for the foreign agent service specified by name or peer IP address.

**fa-service** *fa\_name* must be an alphanumeric string of 1 through 63 characters.

**peer-address** *peer\_address* must be specified using IPv4 dotted-decimal notation.

**greater-than** *peer\_address*: Specifies the range of IPv4 addresses greater than *peer\_address*.

**less-than** *peer\_address*: Specifies the range of IPv4 addresses less than *peer\_address*.

**>** *peer\_address*: Specifies the range of IPv4 addresses greater than *peer\_address*.

**<** *peer\_address*: Specifies the range of IPv4 addresses less than *peer\_address*.

**peer-address** [ *operator* ] *peer\_address*

In conjunction with the **mipfa** [ **summary** ] **peer-address** keyword, indicates a range of peers is to be displayed.

**peer-address** [ *operator* ] *peer\_address* must be specified using IPv4 dotted-decimal notation.

*operator* implies how to logically specify a range of peer-address and it must be one of the following:

- **<**: IP address is less than the specified *peer\_address*
- **>**: IP address is greater than the specified *peer\_address*
- **greater-than**: IP address is greater than the specified *peer\_address*
- **less-than**: IP address is less than the specified *peer\_address*

**peers** **fa-service** *service\_name* [ **current-sessions** { **>** | **greater-than** } *sessions* [ **<** *sessions* ] ] { **<** | **less-than** } *sessions* [ **>** *sessions* ] | *sessions* } ] [ **peer-address** *address* ]

Displays peer servers for the specified FA service.

**fa-service** *service\_name*: Specifies the name of an existing FA service for which the associated peer servers are to be displayed as an alphanumeric string of 1 through 63 characters.

**current-sessions**: Displays only peer servers with current sessions meeting the following criteria:

- **>** | **greater-than** *sessions*: Displays only peer servers currently running sessions higher than the value entered in this parameter. *sessions* must be an integer from 1 to 3000000. **Note**: the keyword "**greater-than**" and the ">" symbol are interchangeable in this instance of the command.
- **<** *sessions*: Displays only peer servers that are currently running sessions less than the **greater-than** parameter but less than the value entered in this parameter. *sessions* must be an integer from 1 to 3000000.

- `<` | `less-than sessions`: Displays only peer servers currently running sessions lower than the value entered in this parameter. `sessions` must be an integer from 1 to 3000000. **Note:** the keyword "**less-than**" and the "`<`" symbol are interchangeable in this instance of the command.
- `>` | `sessions`: Displays only peer servers that are currently running sessions lower than the **less-than** parameter but more than the value entered in this parameter. `sessions` must be an integer from 1 to 3000000.
- `sessions`: Displays only peer servers currently running sessions that are equal to the value entered in this parameter. `sessions` must be an integer from 1 to 3000000.

**peer-address** `address`: Displays only peer servers matching the IP address entered in this parameter. `address` must be specified using IPv4 dotted-decimal notation and can be followed by the netmask of the address.

### { `grep` `grep_options` | `more` }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

## Usage Guidelines

View MIP foreign agent information to support troubleshooting subscriber issues by viewing call information and filtering on the subscriber information using various methods.

### Example

The following displays the call information for all mobile IP FA calls and statistics for `fa1`, respectively:

```
show mipfa all
```

The following command displays the statistics for the foreign agent service `fa1`:

```
show mipfa statistics fa-service fa1
```

The following commands display call information for user `user6@aaa` in full detail and in summary:

```
show mipfa full username user6@aaa
show mipfa summary username user1
```

The following displays MIP FA call information for calls from mobile subscriber `4412345678` and peer address `10.2.3.4`, respectively:

```
show mipfa msid 4412345678 4412345678
show mipfa peer-address 10.2.3.4
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

# show mipha

Displays information for specified Mobile IP Home Agent (MIP-HA) calls.

---

**Product** HA

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show mipha** { [ [ **counters** | **full** | **summary** ] { **all** | **callid** *call\_id* | **imsi** *imsi\_num* | **ip-address** *ip\_addr* | **msid** *msid\_num* | **peer-address** [ *operator* ] *peer\_address* | **reverse-tunnel** { **on** | **off** } | **username** *user\_name* } | **statistics** [ **ha-service** *ha\_name* | **peer-address** *peer\_address* ] } ] | **peers** **ha-service** *service\_name* [ **current-sessions** { { **>** | **greater-than** } *sessions* [ **<** *sessions* ] | { **<** | **less-than** } *sessions* [ **>** *sessions* ] | *sessions* } ] [ **peer-address** *address* ] } [ | { **grep** *grep\_options* | **more** } ]

### **counters | full | summary**

Default: concise output.

**counters:** Displayed output includes the statistical counters.

**full:** Displays detailed information.

**summary:** Displays only summary information.

These options are not available in conjunction with the **statistics** keyword.

### **msid** *msid\_num*

Displays information for the subscriber with the supplied MSID on HA.

**msid** *msid\_num* specifies a mobile subscriber ID for which information is to be displayed. *ms\_id* must be from 7 to 16 digits for an IMSI, MIN, or RMI and /or characters \$ and \* for wildcard filtering.

If **enforce imsi-min equivalence** is enabled on the chassis and MIN or IMSI numbers are supplied, this keyword/ filter will show subscribers with a corresponding MSID (MIN or IMSI) whose lower 10 digits matches the lower 10 digits of the supplied MSID.

**show mipha msid** *ABCD0123456789* or

**show mipha msid** *0123456789*

Shows any subscriber with a MSID that match the lower 10 digits of MSID supplied, such as 0123456789.

**show mipha msid** *01234567\$\$*

Shows any subscriber with a MSID that match the upper 8 digits of the supplied MSID, such as 01234567 and any two digits at the remaining two places.

**all** | **callid** *call\_id* | **imsi** *imsi\_num* | **ip-address** *ip\_addr* | **msid** *msid\_num* | **peer-address** [ *operator* ] *peer\_address* | **reverse-tunnel** { **on** | **off** } | **username** *user\_name*

**all:** Displays all available information.

**callid** *call\_id*: Displays information only for calls with the call ID specified as a 4-byte hexadecimal number.

**imsi** *imsi\_num*: Specifies an IMSI (international mobile subscriber ID) for which information is to be displayed. The IMSI is a 15-character field which identifies the subscriber's home country and carrier.

**ip-address** *ip\_addr*: Displays statistics for a call with the IP address specified in IPv4 dotted-decimal notation.

**msid** *msid\_num*: Specifies a mobile subscriber ID only for which information is to be displayed. *ms\_id* must be from 7 to 16 digits specified as an IMSI, MIN, or RMI.

**peer-address** *peer\_address*: Displays statistical information for the peer IP address specified using IPv4 dotted-decimal notation.

**reverse-tunnel** { **on** | **off** }: Enables the display of reverse IP tunnel information.

**username** *user\_name*: Displays user MIP call information for the username specified as an alphanumeric string of 1 through 127 characters including wildcard characters (\$ and \*).

### **peer-address [ operator ] peer\_address**

In conjunction with **mipha [ summary ] peer-address** keyword, indicates a range of peers is to be displayed. *peer\_address* must be specified using IPv4 dotted-decimal notation.

*operator* implies how to logically specify a range of peer-addresses and it must be one of the following:

- <: IP address is less than the specified *peer\_address*
- >: IP address is greater than the specified *peer\_address*
- **greater-than**: IP address is greater than the specified *peer\_address*
- **less-than**: IP address is less than the specified *peer\_address*

### **statistics [ ha-service ha\_name | peer-address peer\_address ]**

Displays statistical information for the home agent service specified by its name (an alphanumeric string of 1 through 63 characters) or peer IP address (IPv4 notation).

### **peers ha-service service\_name [ current-sessions { { > | greater-than } sessions [ < sessions ] | { < | less-than } sessions [ > sessions ] | sessions } ] [ peer-address address ]**

Displays peer servers for the specified HA service.

**ha-service** *service\_name*: Specifies the name of an existing HA service for which the associated peer servers are to be displayed as an alphanumeric string of 1 through 63 characters.

**current-sessions**: Displays only peer servers with current sessions meeting the following criteria:

- > | **greater-than** *sessions*: Displays only peer servers currently running sessions higher than the value entered in this parameter. *sessions* must be an integer from 1 to 3000000. **Note**: the keyword "**greater-than**" and the ">" symbol are interchangeable in this instance of the command.
- < *sessions*: Displays only peer servers that are currently running sessions higher than the **greater-than** parameter but less than the value entered in this parameter. *sessions* must be an integer from 1 to 3000000.
- < | **less-than** *sessions*: Displays only peer servers currently running sessions lower than the value entered in this parameter. *sessions* must be an integer from 1 to 3000000. **Note**: the keyword "**less-than**" and the "<" symbol are interchangeable in this instance of the command.

- `> sessions`: Displays only peer servers that are currently running sessions lower than the **less-than** permitter but more than the value entered in this parameter. `sessions` must be an integer from 1 to 3000000.
- `sessions`: Displays only peer servers currently running sessions that are equal to the value entered in this parameter. `sessions` must be an integer from 1 to 3000000.

**peer-address** *address*: Displays only peer servers matching the IP address entered in this parameter. *address* must be specified using IPv4 dotted-decimal notation and can be followed by the netmask of the address.

### { **grep** *grep\_options* | **more** }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

#### Usage Guidelines

View MIP home agent information to support troubleshooting subscriber issues by viewing call information and filtering on the subscriber information using various methods.

#### Example

The following displays the call information for all mobile IP HA calls and statistics for *ha1*, respectively:

```
show mipha all
show mipha statistics ha-service ha1
```

The following commands displays call information for user *ispluser1* in full detail and in summary:

```
show mipha full username ispluser1
show mipha summary username user1
```

The following displays MIP-HA call information for calls from mobile subscribers with reverse tunneling *off* and peer address *10.2.3.4*, respectively:

```
show mipha reverse-tunnel off
show mipha peer-address 10.2.3.4
```



#### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show mipv6ha

Displays information for specified Mobile IPv6 Home Agent (MIPv6-HA) calls.

#### Product

PDSN

HA

#### Privilege

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show mipv6ha [ all | callid callid | counters filter | full filter |
ipv6-address ip_addr | statistics mipv6ha-service mipv6ha-service_name | summary
filter | username user_name ]
```

**all**

Displays all information for MIPv6-HA calls.

**callid** *call\_id*

Specifies the Call Identification number as an 8-digit hexadecimal number.

**counters** [ **all** | **callid** | **ipv6-address** | **username** ]

Displays the counters associated with the MIPv6-HA service. The following filters are available:

- **all**
- **callid:**
- **ipv6-address**
- **username**

**full** [ **all** | **callid** | **ipv6-address** | **username** ]

Displays all available information for the associated display or filter keyword.

The following filters are available:

- **all**
- **callid:**
- **ipv6-address**
- **username**

**ipv6-address** *ip\_addr*

Displays information for subscribers connected via the packet control function for a specific or range of IPv6 addresses. The address must be specified using the IPv6 colon-separated-hexadecimal notation.

- **<**: Filters output so that only information less than the specified IPv6 address value is displayed.
- **>**: Filters output so that only information greater than the specified IPv6 address value is displayed.
- **less-than**: Filters output so that only information less than the specified IPv6 address value is displayed.
- **greater-than**: Filters output so that only information greater than the specified IPv6 address value is displayed.

**statistics [ mipv6ha-service mipv6ha-service\_name ]**

Displays all information collected for specific protocol since last the **restart** or **clear** command.

This can be filtered according to a specified **mipv6ha-service**.

**summary [ all | callid | ipv6-address | username ]**

Displays summary information for defined sessions, based on defined parameters.

The following filters are available:

- **all**
- **callid:**
- **ipv6-address**
- **username**

**username user\_name**

Displays session information for a specific username.

**Usage Guidelines**

View MIPv6 home agent information to support troubleshooting subscriber issues by viewing call information and filtering on the subscriber information using various methods.

**Example**

The following displays the call information for all mobile IPv6 HA calls:

```
show mipv6ha all
```

The following command displays call information for user *mipv6hauser1* in full detail and in summary:

```
show mipv6ha full username mipv6hauser1
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show mme-embms-service

Displays configuration information for MME-eMBMS services on this system. MME-eMBMS is the LTE version of Multimedia Broadcast/Multicast Service (eMBMS) on the Cisco Mobility Management Entity (MME).

**Product**

MME

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:



```
[local]host_name#
```

### Syntax Description

```
show mme-embms-service { all | all-session-info [ summary ] | m3ap
statistics { all [ verbose ] | name mme_embms_service_name } | mce-association
{ all [ summary ] | full | name mme_embms_service_name [ summary ] | path-info
{ all | name mme_embms_service_name } } | mce-session-association { plmn-id
mcc mcc mnc mnc mce-id mce_id | tmgi-service-id tmgi_serv_id [ mbms-flow-id
mbms_flow_id ] } | name mme_embms_service_name | sctp statistics { all | name
mme_embms_service_name } }
```

#### ***mme\_embms\_service\_name***

Identifies the name of a specific MME-eMBMS service. The name comprises a string of 1 to 63 alphanumeric characters.

#### **all**

Lists all configured MME-eMBMS service instances on the system and displays upper-level service information for each of the services.

#### **all-session-info [ summary ]**

Lists all active eMBMS sessions currently being handled by the MMEmgr. Optionally, the display can provide a summary of eMBMS information for each session.

#### **m3ap statistics { all [ verbose ] | name }**

Displays all M3AP statistics available for the MME or displays the M3AP statistics for the named “active” MME-eMBMS service. With the **all** keyword, the command output is used to clarify status of MBMS sessions with the following counters in the output:

- MBMS Session Start Request
- MBMS Session Start Response
- MBMS Session Start Response Failure

#### **mce-association { all | full | name | path-info }**

Displays peer MCE associations for either all eMBMS services or specifically for the named eMBMS service. Filters are included in the CLI to control the level of detail in the output.

When the **mce-association** and **path-info** keywords are used together, the output displays path information for the MCEs associated with either all or only with the named MME-eMBMS service(s).

#### **mce-session-association { plmn-id mcc mcc mnc mnc mce-id mce\_id | tmgi-service-id tmgi\_service\_id mbms-flow-id mbms\_flow\_id }**

Displays the MCE session associations for either

- a specific carrier, identified by the PLMN ID
- specific session attributes, such as Temporary Mobile Group Identity (TMGI) and/or Flow Identifier

**name** *mme\_embms\_service\_name* [ **summary** ]

Displays the configuration for the named eMBMS service.

**sctp statistics** { **all** | **name** *mme\_embms\_service\_name* }

Displays Sctp statistics for all or named “active” eMBMS service(s)

[ { **grep** *grep\_options* | **more** } ]

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to view configuration information for MME-eMBMS services on this system and to monitor status of the MCE associations and sessions.

### Example

The following command displays MCE session information filtered by the TMGI 42949672:

```
show mme-embms-service mce-session-association tmgi-service-id 42949672
```

## show mme-hss session

Displays session information of Mobility Management Entity-Home Subscriber Server (MME-HSS) service(s) running on a peer or local system.

**Product** MME

**Privilege** Inspector

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **show mme-hss session** [ **summary** | **full** ] [ **all** | **call-id** *call\_identifier* | **mdn** *mdn\_string* | **nai** *nai\_string* ] [ **verbose** ] [ | { **grep** *grep\_options* | **more** } ]

### summary

This keyword displays the summarized output of this command.

### full

This keyword displays detailed output of this command.

**all**

This keyword displays information of all MME-HSS sessions running on this system.

**call-id *call\_identifier***

Displays summarized or detailed statistics of MME-HSS sessions running and filtered by the call identifier with an MME-HSS service configured on this system.

*call\_identifier* must be an existing call identity in eight character Hex digit format running on an MME service on system.

**mdn *mdn\_string***

Displays summarized or detailed statistics of MME-HSS sessions running and filtered by mobile directory Number (MDN) with an MME-HSS service configured on this system.

*mdn\_string* must be an alphanumeric string of 1 to 100 characters.

**nai *nai\_string***

Displays summarized or detailed statistics of MME-HSS sessions running and filtered by Network Access Identifier (NAI) with an MME service configured on this system.

*nai\_string* must be an alphanumeric string of 1 to 128 characters.

**verbose**

This keyword displays the comprehensive information of specific or set of arguments.

**{ *grep grep\_options* | *more* }**

This argument searches the output of the root command and selects the lines matching one or more patterns/options. The types of patterns are controlled by the options specified with *grep\_options*.

For details on the usage of the **grep** and **more** commands, refer to the Regulating a Command's Output section in CLI Overview chapter of the Command Line Interface Reference.

---

**Usage Guidelines**

Use this command to view detailed or summarized session statistics of MME-HSS sessions running on MME-HSS services on a system. This command also provides the various filter criteria to display the session statistics.

**Example**

The following command displays information of all MME-HSS sessions of MME-HSS services running on a system:

```
show mme-hss session all
```



---

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

The following command displays summarized session information of all MME-HSS sessions running on a system:

```
show mme-hss session summary all
```

## show mme-service

Displays configuration information for Mobility Management Entity (MME) services on this system.

---

**Product** MME

---

**Privilege** Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show mme-service { all | name svc_name [ offload statistics ] } [ | { grep grep_options | more } ]`

### all

Displays configuration information for all MME services configured on this system.

### name *service\_name*

Displays configuration information for an existing MME service specified as an alphanumeric string of 1 through 63 characters.

### offload statistics

Displays configuration information for the MME load rebalancing feature (UE offload), as well as current statistics about any active offloading processes.

This keyword option is only available in Release 14.0 and higher.

### | { *grep* *grep\_options* | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

---

**Usage Guidelines** Use this command to view configuration information for MME services on this system.

### Example

The following command displays service statistics for the MME service named *mme1*:

```
show mme-service name mme1
```



**Important** Output descriptions for these commands are available in the *Statistics and Counters Reference*.

## show mme-service db record

Displays the Mobile Management Entity (MME) database records for MME sessions grouped in session instances on this system and filtered with IMSI or GUTI as criteria.

**Product** MME

**Privilege** Inspector

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `show mme-service db record { all | call-id call_id | guti plmn plmn_id group-id mme_grp_id code mme_code m-tmsi mtmsi_value | imsi imsi_identifier }`

### **all**

Displays all database records of a session instance used for MME service.

### **call-id *call\_id***

Displays database records filtered by the call ID specified as an 8-digit hexadecimal number

### **guti plmn *plmn\_id* group-id *mme\_grp\_id* code *mme\_code* m-tmsi *mtmsi\_value***

Displays database records filtered by the Globally Unique Temporary Identifier (GUTI). The GUTI is constructed from the GUMMEI and the M-TMSI.

The GUMMEI is constructed from the public land mobile network (PLMN) ID [MMC and MNC] and the MME Group ID (MMEGI). Within the MME, the mobile is identified by the M-TMSI.

A GUTI has: 1) a unique identity for the MME which allocated the GUTI; and 2) the unique identity of the UE within the MME that allocated the GUTI.

The MME Identifier (MMEI) is constructed from an MME Group ID (MMEGI) and an MME Code (MMEC).

### **imsi *imsi\_identifier***

Displays database records filtered by International Mobile Subscriber Identity (IMSI).

*imsi\_identifier* is a 15-character IMSI field which identifies the subscriber's home country and carrier. Wildcard characters \$ and \* are allowed. The \* wildcard matches multiple characters and the \$ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes ( ' ). For example; '\$'.

**Usage Guidelines**

Use this command to view database records for all or a particular instance of session manager for MME services on this system with IMSI or GUTI as a filter criteria.

**Example**

The following command displays the summary database records of a session instance for a subscriber having IMSI as *123455432112345* in the MME service:

```
show mme-service db record imsi 123455432112345
```

**Important**

Output descriptions for these commands are available in the *Statistics and Counters Reference*.

## show mme-service db statistics

This command displays the Mobile Management Entity (MME) database statistics for all or specific MME sessions on this system.

**Product**

MME

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show mme-service db statistics [ instance smgr_instance ]
```

**instance *smgr\_instance***

Displays MME database statistics for a specific instance of a session manager running the MME service.

*smgr\_instance* is an instance ID specified as an integer from 0 through 4294967295. If an instance is not specified, summary statistics are displayed.

**Usage Guidelines**

Use this command to view database statistics for all or a particular instance of session manager for MME services on this system.

**Example**

The following command displays summary database statistics for the MME service running on a system:

```
show mme-service db statistics
```

**Important**

Output descriptions for these commands are available in the *Statistics and Counters Reference*.

# show mme-service enodeb-association

Displays configuration information for an eNodeB association within an MME service.

---

**Product** MME

---

**Privilege** Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
show mme-service enodeb-association [ summary | full [ wf1 ] | path-info
[ wf1 ] ] [ all | enodeb-name enodeb_name | henbgw | ipsec |
mme-service-name mme_svc_name | peer-address peer_ip_address | peer-id
peer_identifier ] [ | { grep grep_options | more } ]
```

## summary

Displays summarized output for this command.

## full

Displays detailed output for this command.

## wf1

Displays output in a tabular format.

## path-info

Displays S1 path association information of eNodeBs associated with MME services on this system.

## all

Displays information of all eNodeBs associated with MME services on this system.

## enodeb-name *enodeb\_name*

Displays information for the specified eNodeB associated with MME services on this system.

## henbgw

Displays information for Home eNodeB Gateways (HeNB-GWs) associated with MME services on this system.




---

### Important

In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

**ipsec**

Displays information of all IPSec enabled eNodeBs associated with MME services on this system.

**mme-service-name** *mme\_svc\_name*

Displays summarized or detailed configuration information for eNodeBs associated with an existing MME service specified as an alphanumeric string of 1 through 63 characters.

**peer-address** *peer\_ip\_address*

Displays summarized or detailed configuration information of eNodeBs associated with an existing MME peer IP address configured with an MME service and expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**peer-id** *peer\_identifier*

Displays summarized or detailed configuration information for eNodeBs associated with a an existing MME peer ID configured with an MME service and specified as an integer from 1 through 4294967295.

**{ grep grep\_options | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view configuration information of eNodeBs associated with an MME service on this system.

**Example**

The following command displays detailed service statistics for associated eNodeBs within the MME service named *ingress*:

```
show mme-service enodeb-association full mme-service-name ingress
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

# show mme-service id

This command displays the current number of MME-assigned and eNodeB-assigned S1AP session IDs.

<b>Product</b>	MME
<b>Privilege</b>	Inspector
<b>Command Modes</b>	Exec



The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
show mme-service id summary [ service-name name [ sessmgr instance ] ] | [ peer-id id [ sessmgr instance ] ] [ | { grep grep_options | more } ]
```

**id summary**

Displays the current number of MME-assigned and eNodeB-assigned S1AP session IDs.

**service-name** *name*

Filters the output of the command by for an existing MME service name specified as an alphanumeric string of 1 through 63 characters.

**peer-id** *id*

Filters the output of the command by a MME peer identifier specified as an integer from 1 through 4294967295.

**sessmgr** *instance*

Filters the output of the command by the specified session manager instance as an integer from 1 through 4294967295.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Use this command to display the current number of MME-assigned and eNodeB-assigned S1AP session IDs.

## show mme-service session

Displays session information for Mobile Management Entity (MME) service(s) running on a peer or local system.

---

**Product**

MME

---

**Privilege**

Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
show mme-service session [ summary | full | counters ] [ all | callid call_identifier | imei imei_id | imsi imsi_id | ipsec | mme-service service_name | msisdn number | pdn-address pdn_ip_address | s1-peer s1_peer_ip_address |
```

```
s11-peer s11_peer_ip_address | vlr-name vlr_name | ue-ecm-state { connected | idle } ] [ | { grep grep_options | more } ]
```

**summary**

Displays summarized output for this command.

**full**

Displays detailed output for this command.

**counters**

Displays all counters for related events and messages for an MME session running on a system.

**all**

Displays information for all MME sessions running on this system.

**callid** *call\_identifier*

Displays summarized or detailed configuration information for an MME session filtered by a call identifier within an MME service configured on this system.

*call\_identifier* must be an existing call identity in 8-digit hexadecimal format running in an MME service on this system.

**imei** *imei\_id*

Displays summarized or detailed configuration information about MME sessions running and filtered by an International Mobile Equipment Identification (IMEI) number within an MME service configured on this system.

*imei\_id* must be an existing IMEI in an existing MME service on the system. *imei\_id* must contain an 8-digit TAC (Type Allocation Code) and a 6-digit SNR (Serial Number).

**imsi** *imsi\_id*

Displays summarized or detailed configuration information about MME sessions running and filtered by an International Mobile Subscriber Identity (IMSI) number within an MME service configured on the system.

*imsi\_id* must be an existing IMSI in an existing MME service on the system. *imsi\_id* is a 15-character IMSI field which identifies the subscriber's home country and carrier.

Wildcard characters \$ and \* are allowed. The \* wildcard matches multiple characters and the \$ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes ( ' ). For example; '\$'.

**ipsec**

Displays information for all IPsec enabled sessions using MME services on the system.

**mme-service** *service\_name*

Displays summarized or detailed configuration information about MME sessions running and filtered by an MME service name configured on the system.

*service\_name* must be a configured MME service on the system, expressed as an alphanumeric string of 1 through 63 characters.

**msisdn *number***

Displays summarized or detailed configuration information about MME sessions running and filtered by a Mobile Station International ISDN Number.

*number* must be a combination of the CC (Country Code) and National (significant) mobile number, not exceeding 15 digits.

**pdn-address *pdn\_ip\_address***

Displays summarized or detailed configuration information about MME sessions running and filtered by the IP address of a connected PDN(s) within an MME service configured on this system.

*pdn\_ip\_address* must be a configured IP address of a PDN expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation within an existing MME service on the system.

**s1-peer *s1\_peer\_ip\_address***

Displays summarized or detailed configuration information of MME sessions running and filtered by the IP address of a peer connected through an S1 interface within an MME service configured on this system.

*s1\_peer\_ip\_address* must be a configured IP address of a peer on S1 interface expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation within an existing MME service on this system.

**s11-peer *s11\_peer\_ip\_address***

Displays summarized or detailed configuration information of MME sessions running and filtered by IP address of a peer connected through S11 interface with an MME service configured on this system.

*s11\_peer\_ip\_address* must be a configured IP address of a peer on S11 interface expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation within an existing MME service on this system.

**vlr-name *vlr\_name***

Displays summarized or detailed configuration information of MME sessions running and filtered by Visitor Location Register (VLR) name.

*vlr\_name* must be an alphanumeric string of 1 through 63 characters.

**ue-ecm-state { *connected* | *idle* }**

Displays summarized or detailed configuration information about MME sessions running and filtered by the UE's EPS Connected Management (ECM) state.

**connected:** Specifies that summarized or detailed configuration information about MME sessions is to be displayed based on the UE ECM state of "connected".

**idle:** Specifies that summarized or detailed configuration information about MME sessions is to be displayed based on the UE ECM state of "idle".

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to view information for MME sessions within MME services on this system.

### Example

The following command displays detailed session statistics for an MME service running on this system:

```
show mme-service session full
```



### Important

Output descriptions for these commands are available in the *Statistics and Counters Reference*.

The following command displays detailed session counters for an MME service running on this system:

```
show mme-service session counters
```

## show mme-service statistics

This command displays MME service statistics specified by various criteria.

### Product

MME

### Privilege

Security Administrator, Administrator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show mme-service statistics [ dcnr | decor [ decor-profile profile_name ] |
  emm-only | esm-only | handover | mme-service mme_svc_name | paging-profile
  [ profile-name paging_profile_name ] | peer-id peer_identifier | recovered-values
  | slap | sctp | tai taidb db_name mcc mcc mnc mnc tac tac ] + [ verbose ]
[ | { grep grep_options | more } ]
```

#### dcnr

Displays the dual connectivity NR statistics.

#### decor [ decor-profile profile\_name ]

Displays the Decor statistics for all the configured Decor profile(s).

**decor-profile profile\_name:** Displays Decor statistics for the specified Decor profile. *profile\_name* must be an alphanumeric string of 1 through 63 characters.

**emm-only**

Displays only EPS mobility management (EMM) related statistics, or filters EMM statistics for a specific MME service name or a specific eNodeB association peer identifier.

**esm-only**

Displays only EPS session management (ESM) related statistics, or filters ESM statistics for a specific MME service name or a specific eNodeB association peer identifier.

**handover**

Displays only handover related statistics (such as Intra-MME, EUTRAN<->EUTRAN via S10, EUTRAN<->UTRAN via GnGp, EUTRAN<->GERAN via GnGp, and EUTRAN<->UTRAN via S3), or filters handover statistics for a specific MME service name or a specific eNodeB association peer identifier.

**mme-service *mme\_svc\_name***

Displays MME service statistics for only the specified MME service name.

**paging-profile [ *profile-name paging\_profile\_name* ]**

Displays the paging profile statistics for all the configured paging-profile(s) one after another.

**profile-name** *paging\_profile\_name*: Displays the paging profile statistics for the given profile name. *paging\_profile\_name* must be an alphanumeric string of 1 through 63 characters.

**peer-id *peer\_identifier***

Displays MME service statistics for only the specified eNodeB association peer identifier.

**recovered-values**

Enables the display of recovered counter values if the backup and recovery of statistics has been enabled. This keyword can be combined with the **emm-only**, the **esm-only**, or the **peer-id** options. For details on this feature, refer to the *Backup and Recovery of Key KPI Statistics* feature chapter in the *MME Administration Guide*.

**slap**

Displays only S1-AP related statistics, or filters S1-AP statistics for a specific MME service name or a specific eNodeB association peer identifier..

**sctp**

Displays only SCTP related statistics, or filters SCTP statistics for a specific MME service name or a specific eNodeB association peer identifier.

**tai taidb *db\_name* mcc *mcc* mnc *mnc* tac *tac***

Displays only TAI statistics stored for the specified TAI management database name and MCC/MNC/TAC .

*db\_name* : Specifies the name of the TAI management database as an alphanumeric string of 1 through 64 characters.

*mcc*: specifies the mobile country code (MCC) portion of a PLMN identifier as an integer from 100 through 999.

*mnc*: specifies the mobile network code (MNC) portion of a PLMN identifier as a 2- or 3-digit integer from 00 through 999.

*tac*: specifies the Tracking Area Code portion of the TAI as an integer from 1 through 65535.



#### Important

For the MME to report TAI level statistics, you must first issue the MME Service Configuration Mode command: **statistics collection-mode tai**. Only those MME Services which are configured accordingly will provide TAI based statistics. When the collection-mode is configured to **tai**, the **peer-id** keyword will no longer report valid statistics (All values will be shown as ZERO).



#### Caution

Changing this collection mode will restart the MME service and will clear all statistics at the MME service and eNodeB level.

#### verbose

Displays comprehensive information for a specific argument or set of arguments.

#### { **grep** *grep\_options* | **more** }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

#### Usage Guidelines

This command is used to display the statistical information of MME services based on various filter criteria.

#### Example

The following command displays all service statistics for all MME services on a system:

```
show mme-service statistics
```

The following command displays the service statistics of all MME services on a system related to S1-AP:

```
show mme-service statistics slap
```

The following command displays only EMM related statistics for the only the MME service named **ingress**:

```
show mme-service statistics mme-service ingress emm-only
```

## show module

Displays the current status of the Version Priority List (VPL) for one or all plugin modules installed on the system. This command is associated with the dynamic software upgrade process.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<b>show module</b> [ <i>plugin_name</i> ]  <b><i>plugin_name</i></b> Filters the output of the VPL by an existing plugin name expressed as an alphanumeric string of 1 through 16 characters.
<b>Usage Guidelines</b>	Display the priority, load status, location, installation timestamp and download status of one or all plugin modules. A plugin module is a shared object library that can be dynamically updated or rolled back. Refer to the <i>System Administration Guide</i> for additional information on dynamic software updates.
	<b>Example</b> The following command displays the VPL status of all plugin modules currently installed on the system:  <b>show module</b>

## show mpls cross-connect

Displays Multiprotocol Label Switching (MPLS) cross-connect information.

<b>Product</b>	GGSN
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<b>show mpls cross-connect</b> [   { <b>grep</b> <i>grep_options</i>   <b>more</b> } ]  <b>{ <i>grep grep_options</i>   more }</b> Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.  For details on the usage of the <b>grep</b> and <b>more</b> commands, refer to the <i>Regulating a Command's Output</i> section in the <i>Command Line Interface Overview</i> chapter.

**Usage Guidelines**

This command displays MPLS cross-connect information. MPLS tunnel cross-connects between interfaces and Label-Switched Paths (LSPs) connect two distant interface circuits of the same type by creating MPLS tunnels that use LSPs as the conduit.

**Example**

The following command displays MPLS cross-connect information:

```
show mpls cross-connect
```

**Important**

Output descriptions for these commands are available in the *Statistics and Counters Reference*.

## show mpls ftn

Displays MPLS FEC-to-NHLFE (FTN) table information.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show mpls ftn [ vrf vrf_name ] [ | { grep grep_options | more } ]
```

**vrf vrf\_name**

Displays FTN information for the Virtual Routing and Forwarding (VRF) specified as an alphanumeric string of 1 through 63 characters.

**| { grep grep\_options | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

**Usage Guidelines**

This command displays MPLS FEC (Forward Error Correction)-to-NHLFE (Next-Hop label Forwarding Entry) table information.

**Example**

The following command displays MPLS FTN information:

```
show mpls ftn
```





**Important** Output descriptions for these commands are available in the *Statistics and Counters Reference*.

## show mpls ilm

Displays MPLS Incoming Label Map (ILM) table information.

**Product** GGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `show mpls ilm [ fec | label label_value | verbose ][ | { grep grep_options | more } ]`

### fec

Displays Forwarding Equivalency Class (FEC) information.

### label label\_value

Displays MPLS ILM information for the specified label. label\_value is an integer from 16 through 1048575.

### verbose

Displays detailed information for the MPLS ILM table.

### { grep grep\_options | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

**Usage Guidelines** This command displays MPLS Incoming Label Map (ILM) table information.

### Example

The following command displays information for MPLS ILM information:

```
show mpls ilm
```



**Important** Output descriptions for these commands are available in the *Statistics and Counters Reference*.

## show mpls ldp

Displays MPLS Label Distribution Protocol (LDP) information.

**Product** GGSN

**Privilege** Security Administrator, Administrator

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `show mpls ldp { bindings { ldp-id IPv4_addr | local [ ldp-id | local | prefix | remote ] | prefix IPv4_addr | remote } | discovery | neighbor { detail | ldp-id } }`

### bindings

Displays the MPLS LDP label bindings.

### ldp-id

Displays label values for a specific peer LDP ID.

### local

Displays locally assigned label values.

### prefix

Displays label values for a specific prefix.

### remote

Displays remotely assigned label values.

### discovery

Displays the MPLS LDP discovery information.

### neighbor

Displays the MPLS LDP peer information.

**detail**

Displays the MPLS LDP peer information in details. The displayed information includes, Local LDP ID, Peer LDP ID, Transport address, State (for example, Established), Role (for example, Active), Uptime, Keepalive negotiated hold time, Proposed Local/Peer, Remaining Keepalive hold time, and Address advertised.

**Usage Guidelines**

This command displays statistical information for an MPLS Label Distribution Protocol configuration. The information includes Prefix, LDP ID, Label, Nexthop, and Egress\_if\_index for all MPLS LDP Bindings configurations.

**Example**

The following command displays information about MPLS LDP protocol related configurations:

```
show mpls ldp discovery neighbor ldp-id 10.2.3.4 detail bindings ldp-id
31.32.33.34 prefix 192.168.102.232 local remote
```

The following command displays the MPLS LDP discovery information, including, LDP Peer IDs, Hold time (in seconds), Proposed Local/Peer, and Remaining (time in seconds):

```
show mpls ldp discovery
```

The following command displays the remotely assigned label values in the MPLS LDP binding configuration:

```
show mpls ldp bindings remote
```

**Important**

Output descriptions for these commands are available in the *Statistics and Counters Reference*.

## show mpls nexthop-label-forwarding-entry

Displays MPLS Next-Hop Label Forwarding Entry (NHLFE) table information.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show mpls nexthop-label-forwarding-entry [ | { grep grep_options | more } ]
```

```
{ grep grep_options | more }
```

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

**Usage Guidelines**

This command displays MPLS Next-Hop Label Forwarding Entry (NHLFE) table information.

**Example**

The following command displays MPLS NHLFE information:

```
show mpls nexthop-label-forwarding-entry
```

**Important**

Output descriptions for these commands are available in the *Statistics and Counters Reference*.

## show mrme-service

Displays configuration and/or statistical information for MRME services on this system.

**Product**

SaMOG

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Syntax Description**

```
show mrme-service { all | name name | statistics { all [ verbose ] |
dns-stats | name name [ dns-stats ] } } [ | { grep grep_options | more } ]
```

**all**

Displays all MRME services.

**name *name***

Displays information for specific MRME service name.

*name* is a string of size 1 to 63.

**statistics**

Displays Node level Statistics for MRME.

**verbose**

Specifies Detailed statistics.

**dns-stats**

Specifies the information related to theDNS selection of P-GW.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to displays configuration and/or statistical information for MRME services on this system.

**Example**

```
show mrme-service all
```

## show mrme-service active-session

Displays configuration and statistical information of the data stored in the active session entry (if present) of the specified User Equipment's (UE) MAC address.

**Product**

SaMOG

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Syntax Description**

```
show mrme-service active-session mac mac_address [ | { grep grep_options |  
more } ]
```

**mac *mac\_address***

Specifies the MAC address.

*mac\_address* must be an alpha-numeric string of 1 to 15 characters and should not be separated by a colon or hyphen.

**{ **grep** *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display the configuration and statistical information of the data stored in the active session entry (if present) of the specified User Equipment's (UE) MAC address.

**Example**

```
show mrme-service active-session mac 001d33227310
```

## show mrme-service imsi-sticky

Displays configuration and statistical information of the IMSI to session manager mapping (if available) in the mapping table of the IPSP manager.

**Product**

SaMOG

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Syntax Description** `show mrme-service imsi-sticky imsi imsi_value [ | { grep grep_options | more } ]`

**imsi *imsi\_value***

Specifies the International Mobile Subscriber Identity (IMSI) value.

*imsi\_value* must be an integer from 1 to 15 digits.

**{ **grep** *grep\_options* | **more** }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines** Use this command to display configuration and statistical information of the IMSI to session manager mapping (if available) in the mapping table of the IPSP manager.

**Example**

```
show mrme-service imsi-sticky imsi 123456789 all
```

## show mrme-service mac-sticky

Displays configuration and statistical information of the User Equipment (UE) MAC address to IMSI mapping (if available) in the mapping table of the IPSP manager.

---

**Product** SaMOG

---

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

---

**Syntax Description** `show mrme-service mac-sticky mac mac_address [ | { grep grep_options | more } ]`

**mac *mac\_address***

Specifies the MAC address.

*mac\_address* must be an alpha-numeric string of 1 to 15 characters and should not be separated by a colon or hyphen.

**{ **grep** *grep\_options* | **more** }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display the configuration and statistical information of the User Equipment (UE) MAC address to IMSI mapping (if available) in the mapping table of the IPSG manager.

**Example**

```
show mrme-service mac-sticky mac 001d33227310
```

## show mseg-config

This command is not supported in this release.

## show mseg-service

This command is not supported in this release.

## show multicast-sessions

Displays information for multicast sessions defined by the specified keywords.

**Product**

PDSN

GGSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show multicast-sessions [ command_keyword ] [ filter_keywords ] [ | { grep grep_options | more } ]
```

***command\_keyword***

The following keywords are base commands that each have a distinct display output. Only one keyword can be entered on the command line.

**debug-info { *callid id* | *flowid id* }**

Displays internal call troubleshooting information for multicast sessions defined by the specified keywords.

**callid id**: Displays subscriber information for the call specified as an 8-digit hexadecimal number.

**flowid id**: Displays information for a specific BCMCS flow, defined by The flow ID as a hexadecimal number.

**full**

Displays all available multicast session information. The following filter keywords are valid for this command: active, all, callid, card-num, dormant, flowid, flowid-type, mcast-address, pcf, pdsn-service, grep, more

**summary**

Only displays a summary of multicast session information. The following commands are valid for this command: active, all, callid, card-num, dormant, flowid, flowid-type, mcast-address, pcf, pdsn-service, grep, more

**filter\_keywords**

The following keywords are filters that modify or filter the output of the Command Keywords. Not all filters are available for all Command Keywords. Multiple Filter Keywords can be entered on a command line.

When multiple Filter Keywords are specified, the output conforms to all of the Filter Keywords specifications.

**active**

Only displays information for multicast sessions that are currently active.

**all**

If no keywords are specified before **all**, information for all multicast sessions is displayed. If keywords are specified before **all**, all information is displayed with no further options being allowed.

**callid id**

Displays multicast session information for the call specified by *id*. The call must be specified as an 8-digit hexadecimal number.

**card-num card\_num**

The slot number of the processing card by which the subscriber session is processed. *card\_num* is a slot number from 1 through 7 or 10 through 16 on the ASR 5000, or 1 through 4 or 7 through 10 on the ASR 5500.

**dormant**

Shows information for subscriber sessions that are dormant (not transmitting or receiving data).

**flowid id**

Displays information for a specific BCMCS flow, defined by *id*. The flow ID must be a hexadecimal number.

**flowid-type [ flow | program ]**

Displays information for multicast sessions according to the type of flow.

**flow:** Shows all multicast sessions for the flow ID type "flow".

**program:** Shows all multicast sessions for the flow ID type "program".



**mcast-address *ipv4\_address***

Show multicast sessions for a specific multicast address. Must be followed by the IP address of an interface, using IPv4 dotted-decimal notation.

**pct *ipv4\_address***

Displays information for multicast sessions connected via the packet control function, defined by *ipv4\_address*. The address must be specified using IPv4 dotted-decimal notation.

**pdsn-service *svc\_name***

Displays information for multicast session connected to the packet data service *svc\_name*. The packet data service must have been previously configured and expressed as an alphanumeric string of 1 through 63 characters.

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

Please refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

**Usage Guidelines**

Use this command to view information about multicast sessions.

The output of this command may be considered for part of a periodic system auditing program by verifying active and dormant sessions.

**Example**

The following command displays the all broadcast-multicast sessions active in a context/system:

```
show multicast-sessions all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show network-requested-pdp-context

Displays information for the specified network-requested packet data protocol (PDP) context.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `show network-requested-pdp-context imsi imsi_value`

**imsi *imsi\_value***

Specifies that information will be displayed for a particular International Mobile Subscriber Identity (IMSI). *imsi\_value* is an integer from 1 to 15 digits.

**Usage Guidelines** Use this command to display information pertaining to network-requested PDP contexts.

### Example

The following command displays network-requested PDP context information for a subscriber with an IMSI of 123456789:

```
show network-requested-pdp-context imsi 123456789
```

## show network-service-entity

Displays information regarding the network service entities (NSEs) in the network.

**Product** SGSN

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

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `show network-service-entity { consolidated-status | fr-config [ peer-nsei nsei] | ip-config [ nsvl { all | instance value } ] }`

### consolidated-status

Displays Network Service Virtual Connection (NSVC) status information for all network service entities in the network. This keyword is particularly useful for troubleshooting.

### fr-config [ peer-nsei *nsei*]

Displays network service configurations for NSEs using Frame Relay configurations.

**peer-nsei *nsei*** limits the display to a specific peer NSE identified as an integer from 0 through 65535.

### ip-config [ nsvl { all | instance *value* } ]

Displays network service configurations for NSEs using IP configurations.

Including the **nsvl** keyword limits the display to all or a single (instance 0 to 3) of a network service virtual link.

**Usage Guidelines** Use this command to display NSE information pertaining to the NSVCs of the NSEs in the networks or NSEs configured for Frame Relay or IP.

**Example**

The following command displays the status of all the NSVCs for all the NSEs in the network.

```
show network-service-entity consolidated-status
```

## show npu arp

Displays an Address Resolution Protocol (ARP) for a specified VPN identifier.

**Product**

ASR 5000 only

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show npu arp lookup vpnid identifier nexthop ip_address slot slot_number
```

***identifier***

Specifies a valid VPN identifier as an integer from 0 through 2114.

***nexthop ip\_address***

Specifies a valid nexthop IP address in IPv4 dotted decimal or IPv6 colon-separated-hexadecimal notation.

***slot slot\_number***

Specifies the slot number of the card for which the lookup is being form. *slot* is one of the following integers: 1, 2, 8 or 9.

**Usage Guidelines**

Use this command to perform an aRP lookup of a valid VPNid.

**Example**

The following command displays ARP lookup information for VPN 234:

```
show npu arp lookup vpnid 234 nexthop 10.1.1.1 slot 8
```

## show npu error-counters

Displays packet error counters.

**Product**

ASR 5000 only

<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<b>show npu error-counters [   { grep <i>grep_options</i>   more } ]</b>  <b>  { grep <i>grep_options</i>   more }</b> Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent. For details on the usage of <b>grep</b> and <b>more</b> , refer to the <i>Regulating a Command's Output</i> section of the <i>Command Line Interface Overview</i> chapter.
<b>Usage Guidelines</b>	View network timing protocol information to troubleshooting system clock issues by displaying the associations and status of the local NTP client.

**Example**

The following displays the NPU information.

```
show npu error-counters
show npu error-counters |grep qwe
```

## show npu tm

Displays queue status and performance statistics from the Traffic Manager (TM) component of an MIO NPU.

<b>Product</b>	ASR 5500 only
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<b>show npu tm { queue <i>card/cpu/npu</i> [ mode { both   hex   text } ]   statistics <i>card/cpu/npu</i> [ reset ] [   { grep <i>grep_options</i>   more } ]</b>  <b>queue [ mode { both   hex   text } ]</b> Displays the TM queuing information for the specified NPU. The <b>mode</b> option allows you to specify hexadecimal, ASCII text or both types of display values.  <b>statistics [ reset ]</b> Displays TM-related operational statistics. The <b>reset</b> option allows you to clear the statistical counters.

**card/cpu/npu**

Specifies the card slot (5 or 6), CPU number (0), and NPU number (1 through 4).

**{ grep grep\_options | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display queue status and performance statistics from the Traffic Manager (TM) component of an MIO NPU.

**Example**

The following command displays cumulative TM statistics for all NPUs associated with CPU 0 on the MIO in slot 5:

```
show npu tm statistics 5/0
```

The following command displays individual statistics for NPU 3 associated with CPU 0 on the MIO in slot 5.

```
show npu tm statistics 5/0/3
```

## show npu utilization

Displays NPU utilization information.

**Product**

ASR 5000, ASR 5500, VPC

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show npu utilization table [ | { grep grep_options | more } ]
```

**{ grep grep\_options | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Displays NPU manager state table information.

For the VPC, this command displays IFTASK core statistics for each active and standby SF. Statistics are reported for the past five seconds, past five minutes and past 15 minutes.

### Example

The following displays the NPU information.

```
show npu utilization table
show npu utilization table | grep qwe
```

## show ntp

Displays the network timing protocol (NTP) associations and status.

### Product

All

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show ntp { associations | status } [ address ip_address ] [ | { grep
grep_options | more } ]
```

#### associations

Displays the current NTP server associations and related statistics.

#### status

Displays the client permeates configured and the synchronization status.

#### address ip\_address

Specifies the IP address of an NTP server/client in the current context in IPv4 dotted-decimal notation.

#### { grep grep\_options | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

View network timing protocol information to troubleshooting system clock issues by displaying the associations and status of the local NTP client.

**Example**

The following displays the NTP associations and status, respectively.

```
show ntp associations
show ntp status
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show nw-reachability server

Displays the configuration of network reachability servers for the current context.

**Product**

HA

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show nw-reachability server { all | ipv4-only | ipv6-only | name server_name
}
```

**all**

Displays configuration information for all network reachability servers in the current context.

**ipv4-only**

Displays IPv4 Network Reachability Detection servers.

**ipv6-only**

Displays IPv6 Network Reachability Detection servers.

**name server\_name**

Displays configuration information for an existing network reachability server specified as an alphanumeric string of 1 through 15 characters.

**Usage Guidelines**

Use this command to display configuration information on network reachability servers configured in the current context.

**Example**

The following command displays information on all network reachability servers in the current context:

```
show nw-reachability server all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show operator-policy

Displays the information configured for an operator policy.

**Product**

MME  
SAEGW  
S-GW  
SGSN

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show operator-policy { all | full { all | name op_policy_name } | name op_policy_name } [ | { grep grep_options | more } ]
```

**all**

Displays a list of all operator policies configured on the system.

**full { all | name *op\_policy\_name* }**

**full**: Displays a full set of available information for the specified operator policy (policies).

**all**: Displays a full set of available information for all operator policies configured on the system.

**name** *op\_policy\_name*: Displays a full set of available information for an existing operator policy specified as an alphanumeric string of 1 through 64 characters.

**name *op\_policy\_name***

Displays a full set of available information for an existing operator policy specified as an alphanumeric string of 1 through 64 characters.



**{ `grep` *grep\_options* | `more` }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display information for operator policies configured on the system. Operator policies are configured through the Global Configuration Mode and in the Operator Policy Configuration Mode. For more information regarding operator policy commands, refer to the *Operator Policy Configuration Mode Commands* chapter.

### Example

The following command displays all available information for an operator policy named *policy-5*:

```
show operator-policy full name policy-5
```

## show orbem

Displays information and statistics for the Object Request Broker Element Manager (ORBEM) interface in the current context.

### Product

All

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show orbem { client { id client_name | table } | event-notif-service filters
  | session { id session_name | table } | status } [ | { grep grep_options |
more } ]
```

#### **client { id *client\_name* | table }**

Indicates the Common Object Request Broker Architecture (CORBA) client information is to be displayed. The keyword **table** is used to output to the display information on all configured clients. The keyword **id** is used to specify a specific client for which information is to be displayed specified as *client\_name*.

*client\_name* must refer to an existing client which is found using the **table** keyword option.

#### **event-notif-service filters**

Displays information pertaining to filters configured for the ORB Notification Service.



### Important

In 18.0 and later releases, this keyword is obsolete.

**session { id *session\_name* | table }**

Indicates session information is to be displayed. The keyword **table** is used to output to the display information on all configured clients. The keyword **id** is used to specify a specific session for which information is to be displayed specified as *session\_name*.

*session\_name* must refer to an existing session which is found using the **table** keyword option.

**status**

Indicates that the ORBEM server status information is to be displayed.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Display current sessions when ORBEM system response may appear sluggish. This command is also useful in periodic verification of the server status.

**Example**

The following commands will display the information for all clients.

```
show orbem client table
```

The following commands display the information for the *clientName* and *sessionID*, respectively:

```
show orbem client id clientName
```

```
show orbem session id sessionId
```

The following command displays the ORBEM server status:

```
show orbem status
```

The following command displays the information for all sessions:

```
show orbem session table
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

# show patch progress

Displays the status of the on-going software patch installation.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`**Syntax Description****show patch progress****Usage Guidelines**

Use this command to show the status of an on-going software patch installation.

**Important**

Software Patch Upgrades are not supported in this release.

## show pcc-af service

Displays the statistical and configuration information of configured Policy and Charging Control- Application Function (PCC-AF) services configured in a context.

**Product**

IPCF

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`**Syntax Description****show pcc-af service [ statistics ] { all | name *pcc\_af\_svc\_name* | summary } [ | { grep *grep\_options* | more } ]****all****all:** displays information for all configured PCC-AF services.**name *pcc\_af\_svc\_name***

Displays information only for an existing PCC-AF service specified as an alphanumeric string of 1 through 79 characters

**statistics**

Displays the statistical information for a specific service or all PCC-AF services configured in a context.

**summary**

Displays the summarized output of this command.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display the statistical and configuration information of configured PCC-AF services configured in a context.

Display can further be filtered for specific PCC-AF service name or summarized output of the command.

### Example

The following command displays the information for the PCC-AF service named *pccApp1* in summarized output:

```
show pcc-af service name pccApp1 summary
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show pcc-af session

Displays the active/dormant session information about Policy and Charging Control- Application Function (PCC-AF) service instances configured and running on this system based on different filter criteria.

### Product

IPCF

### Privilege

Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show pcc-af sessions [ full | summary] [ all ] [ apn | call-id call_id |
ip-address pcc_af_ip_address | service pcc_af_svc_name | sipuri sip_uri ] ] [ |
{ grep grep_options | more } ]
```

#### full

Displays the full information of specific registered IP Connectivity Access Network (IP-CAN) session(s) on a PCC-AF service instance running on system. Display can be filtered based on given filtering criteria.

#### summary

Displays summarized information for specific registered IP-CAN session(s) on a PCC-AF service instance running on system. Display can be filtered based on given filtering criteria.

#### all

Displays summarized or full information for all registered IP-CAN session(s) on a PCC-AF service instance running on system. Display can be filtered based on given filtering criteria.

**apn *apn\_name***

Displays information for PCC-AF service sessions connected via an existing APN at the Policy and Charging Enforcement Function (PCEF).

**ip-address *pcc\_af\_ip\_address***

Filters the display of full or summarized session statistics for IP-CAN session(s) based on the IP address of a registered PCC-AF server on a PCC-AF service instance.

*pcc\_af\_ip\_address* is an IP address expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**call-id *call\_id***

Filters the display of full or summarized session statistics for IP-CAN session(s) based on the registered call ID on a PCC-AF service instance for the IP-CAN session subscriber in 8-digit hexadecimal format.

**pcc-af-service *pcc\_af\_svc\_name***

Filters the display of session statistics for a registered IP-CAN session(s) based on an existing PCC-AF service name specified as an alphanumeric string of 1 through 63 characters.

**sipuri *sip\_uri***

Displays summarized or full information for IP-CAN session(s) based on the SIP-URI on a PCC-AF service instance.

*sip\_uri* is the Session Initiation Protocol (SIP) addressing schema to call another person. It resembles an e-mail address and is written in the SIP URI format as *sip:x@y:Port* format, where *x* = username and *y* = host (domain or IP)

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Use this command to view the session statistics of all or specific registered IP-CAN session(s) or in selected part of user session for PCC-AF services configured and running on this system.

**Example**

The following command displays the summarized session statistics for all registered IP-CAN sessions on the PCC-AF service named *pccAF1*:

```
show pcc-af sessions summary all service pccAF1
```



---

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

# show pcc-policy service

Displays the statistical and configuration information of configured PCC-Policy services configured in a context.

<b>Product</b>	IPCF
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **show pcc-policy service [ statistics] { all | name *pcc\_plcy\_svc\_name* | summary } [ | { **grep** *grep\_options* | more } ]**

## all

**all**: displays information for all configured PCC-Policy services.

## name *pcc\_plcy\_svc\_name*

Displays information for an existing PCC-Policy service specified as an alphanumeric string of 1 through 79 characters.

## statistics

Displays statistical information for a specific or all PCC-Policy services configured in a context.

## summary

Displays summarized output for this command.

## | { **grep** *grep\_options* | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

## Usage Guidelines

Use this command to display the statistical and configuration information of configured PCC-Policy services configured in a context.

Display can further be filtered for specific PCC-Policy service name or summarized output of the command.

## Example

The following command displays the information for the PCC-Policy service named *pcc\_policy1* in summarized output:

```
show pcc-policy service name pcc_policy1 summary
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show pcc-policy session

Displays active/dormant session information about PCC-Policy service instances configured and running on this system based on different filter criteria.

<b>Product</b>	IPCF
----------------	------

<b>Privilege</b>	Inspector
------------------	-----------

<b>Command Modes</b>	Exec
----------------------	------

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show pcc-policy sessions [ full | summary ] [ all ] [ apn | call-id call_id
| imsi imsi_id | ip-address pcc_pcef_ip_address | service pcc_plcy_svc_name ] ]
[ | { grep grep_options | more } ]
```

**full**

Displays full information for a specific registered IP Connectivity Access Network (IP-CAN) session(s) on a PCC-Policy service instance running on system. Display can be filtered based on given filtering criteria.

**summary**

Displays summarized information for a specific registered IP-CAN session(s) on a PCC-Policy service instance running on system. Display can be filtered based on given filtering criteria.

**all**

Displays summarized or full information for all registered IP-CAN session(s) on a PCC-Policy service instance running on system. Display can be filtered based on given filtering criteria.

**apn *apn\_name***

Displays information for PCC-Policy service sessions connected via an existing APN on the PCEF.

**imsi *imsi\_id***

Displays summarized or full information for IP-CAN session(s) based on the International Mobile Subscriber Identity (IMSI) of a subscriber in a PCC-Policy service instance.

*imsi\_id* is the IMSI and must be a 15-character field which identifies the subscriber's home country and carrier.

**ip-address *pcc\_pcef\_ip\_address***

Filters the display of full or summarized session statistics for IP-CAN session(s) based on the IP address of the registered PCEF node specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**call-id *call\_id***

Filters the display of full or summarized session statistics display for an IP-CAN session(s) based on the registered call ID in a PCC-Policy service instance.

*call\_id* must be an existing call identifier in the IP-CAN session subscriber expressed in 8-digit hexadecimal format.

**pcc-policy-service *pcc\_plcy\_svc\_name***

Filters the display of session statistics for registered IP-CAN session(s) based on an existing PCC-Policy service name specified as an alphanumeric string of 1 through 63 characters.

**| { *grep grep\_options* | *more* }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view the session statistics for all or a specific registered IP-CAN session(s) for PCC-Policy services configured and running on this system.

**Example**

The following command displays summarized session statistics for all registered IP-CAN sessions on the PCC-Policy service named *pccPolicy1*:

```
show pcc-policy sessions summary all service pccPolicy1
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show pcc-service

Displays the configuration information for Policy and Charging Control (PCC) services configured in a context.

**Product**

IPCF

**Privilege**

Security Administrator Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```



**Syntax Description**

```
show pcc-service { summary | all | service-name pcc_svc_name } [ | { grep
grep_options | more } ]
```

**all**

**all:** displays information for all configured PCC services.

**service-name *pcc\_svc\_name***

Displays information for an existing PCC service specified as an alphanumeric string of 1 through 79 characters.

**summary**

Displays the summarized output of this command.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display statistical and configuration information for configured PCC services in a context.

Display can further be filtered for a specific PCC- service name.

**Example**

The following command displays the information for the PCC service named *pcc\_svc1*:

```
show pcc-service service-name pcc_svc1 summary
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show pcc-service session

Displays active/dormant session information about Policy and Charging Control (PCC) service instances configured and running on this system based on different filter criteria.

**Product**

IPCF

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show pcc-service sessions [ full | summary ] [ all emergency-only ] [
call-id call_id | instance instance_id | service-name pcc_svc_name ] [ | {
grep grep_options | more } ]
```

**full**

Displays full information for a specific registered IP Connectivity Access Network (IP-CAN) session(s) in a PCC service instance running on system. Display can be filtered based on given filtering criteria.

**summary**

Displays summarized information for a specific registered IP-CAN session(s) in a PCC service instance running on system. Display can be filtered based on given filtering criteria.

**all**

Displays summarized or full information for all registered IP-CAN sessions on a PCC service instance running on system. Display can be filtered based on given filtering criteria.

**emergency-only**

Displays summarized or full information for all IP-CAN sessions on a PCC service instance running on system which are using emergency APN for emergency services. Display can be filtered based on given filtering criteria.

**instance *instance\_id***

Displays summarized or full information for an IP-CAN session(s) based on the PCC service instance identifier on an IPCF/PCRF node specified as an integer from 1 through 512.

**service-name *pcc\_svc\_name***

Filters the display of session statistics display of registered IP-CAN session(s) based on an existing PCC service name specified as an alphanumeric string of 1 through 63 characters.

**| { *grep grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view session statistics for all or a specific registered IP-CAN session(s) in PCC services configured and running on this system.

**Example**

The following command displays summarized session statistics for all registered IP-CAN sessions in the PCC service named *pccsvc1*:

```
show pcc-service sessions summary service-name pccsvc1
```



**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show pcc-service statistics

Displays the statistical information for Policy and Charging Control (PCC) services configured in a context.

**Product** IPCF

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

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **show pcc-service statistics** { **all** | **service-name** *pcc\_svc\_name* [ **profile-name** *pcc\_profile\_name* ] } [ | { **grep** *grep\_options* | **more** } ]

### **all**

Displays statistical information for all configured PCC services on a system.

### **service-name** *pcc\_svc\_name*

Displays information for an existing PCC service specified as an alphanumeric string of 1 to 79 characters. It can be further filtered by the PCC profile name used in an IP-CAN session.

### **profile-name** *pcc\_profile\_name*

Displays information for an existing PCC profile in an IP-CAN session.

### { **grep** *grep\_options* | **more** }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

### **Usage Guidelines**

Use this command to display the statistical information for PCC services configured in a context.

Display can further be filtered for a specific Profile name used in a session.

### **Example**

The following command displays the information for the PCC service named *pcc\_svc1* using PCC profile named *pcc\_profile\_default*:

```
show pcc-service statistics service-name pcc_svcl profile-name
pcc_profile_default
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show pcc-sp-endpoint

Displays statistical and configuration information for a configured PCC Sp-Endpoint instance in a context.

**Product**

IPCF

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show pcc-sp-endpoint [statistics] [all | name sp_endpt_name] [ | [grep
grep_options | more]] [connection [all | name sp_endpt_name]]
```

**all**

Displays statistical information for all configured PCC Sp-Endpoint instances on a system.

**name *sp\_endpt\_name***

Displays information for an existing PCC Sp-Endpoint instance specified as an alphanumeric string of 1 through 79 characters.

**{*grep grep\_options* | more}**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

**connection**

Displays statistics for the configured connection values along with peer selection success and failures.

**Usage Guidelines**

Use this command to display statistical information and peer name for a configured PCC Sp-Endpoint instance in a context.

**Important**

If the secondary peer is not configured, then N/A is printed in the output.

Display can further be filtered for a specific PCC Sp-Endpoint instance used in a session.

### Example

The following command displays statistical information for the PCC Sp-Endpoint instance named *Sp\_Intf1*:

```
show pcc-sp-endpoint statistics name Sp_Intf1
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show pcc-sp-endpoint connection

Displays statistical and configuration information for an Sp interface connection in a PCC Sp-Endpoint instance.

### Product

IPCF

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show pcc-sp-endpoint connection [ all | name sp_endpt_name [ peer sp_peer_name ] ] [ | { grep grep_options | more } ]
```

#### all

Displays statistical information for all configured PCC Sp-Endpoint instances on a system.

#### name *sp\_endpt\_name*

Displays information for an existing PCC Sp-Endpoint instance specified as an alphanumeric string of 1 through 79 characters. It can further be filtered with an Sp Endpoint peer (SSC/SPR) name used for the IP Connectivity Access Network (IP-CAN) session.

#### peer *ssc\_name*

Displays information only for the PCC Sp-Endpoint instance within an existing Subscriber Service Controller/Subscriber Profile Repository (SSC/SPR) as a peer for an IP-CAN session.

*ssc\_name* is the name of the SSC/SPR node used by the Sp Endpoint interface.

#### { grep *grep\_options* | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display statistical information for Sp interface connections in PCC Sp-Endpoint instances. Display can further be filtered for a specific peer name (SSC/SPR).

### Example

The following command displays the Sp interface connection related statistical information for the PCC Sp-Endpoint instance named *Sp\_Intfl* using peer name *SSC1*:

```
show pcc-endpoint connection name Sp_Intfl peer SSC1
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show pdg-service

Displays configuration information about PDG services configured on the system.

### Product

PDG/TTG

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show pdg-service { all | name service_name }
```

#### all

Displays information for all configured Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG) services.

#### name *service\_name*

Displays information only for an existing PDG service specified as an alphanumeric string of 1 through 63 characters.

#### { **grep** *grep\_options* | **more** }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display information for PDG services.

**Example**

The following command displays available information for all active PDG services:

```
show pdg-service all
```

## show pdg-service statistics

Displays statistics for the Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG) since the last **restart** or **clear** command. The output includes the number of each type of Extensible Authentication Protocol (EAP) messages.

**Product**

PDG/TTG

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show pdg-service statistics [ name service_name | peer-address ipv4_address ]
```

**name *service\_name***

Displays statistics for an existing PDG service specified an alphanumeric string of 1 through 63 characters.

**peer-address *ipv4\_address***

Displays statistics for a specific subscriber with the WLAN IP address specified in IPv4 dotted-decimal notation.

**{ *grep grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display PDG service statistics.

**Example**

The following command displays statistics for all active PDG services:

```
show pdg-service statistics
```

# show pdif-service

Displays configuration information about Packet Data Interworking Function (PDIF) services configured on the system.

---

**Product**

PDIF

---

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
show pdif service { all [ counters ] | name name [ counters ] | statistics
  [ name name | peer-address address ] } [ | { grep grep_options | more } ]
```

**all [ counters ]**

Displays configuration information and statistical counters for all PDIF services in the system.

**name *name* [ counters ]**

Displays configuration information and statistical counters for an existing PDIF service specified as an alphanumeric string of 1 through 63 characters.

**statistics [ name *name* | peer-address *address* ]**

**name *name***: Displays service statistics for an existing PDIF service specified as an alphanumeric string of 1 through 63 characters.

**peer-address *address***: Displays service statistics for a peer server IP address specified in IPv4 dotted-decimal notation.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Use this command to display configuration information and statistics about PDIF services on the system.

**Example**

The following example displays configuration information about a PDIF service named *pdif23*:

```
show pdif service name pdif23
```





**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show pdn-connection-count

Displays the current number of PDN connections for each of the Restoration-Priority-Level values received from AAA across S6b interface.

### Product

P-GW  
SAEGW

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec  
The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show pdn-connection-count restoration-priority-level { priority_level | all
}
```

**restoration-priority-level** { *priority\_level* | **all** }

Restoration priority associated with PDN connection.

*priority\_level*: Restoration priority level must be an integer from 1 through 8.

In StarOS 21.0 and later, priority levels 1 through 16 are supported.

**all**: Displays the number of PDN connections associated with all restoration priorities.

### Usage Guidelines

To distinguish between VoLTE enabled IMS PDN connections and non-VoLTE enabled IMS PDN connections, the P-GW supports receiving AVP "Restoration-Priority-Indicator" from AAA server over the S6b interface. The P-GW also provides KPIs based on the AVP value.

### Example

The following command displays the number of PDN connections associated with restoration priority level 2:

```
show pdn-connection-count restoration-priority-level 2
```

## show pdsn-service

Displays information for configured packet data services in the current context.

### Product

PDSN

<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<pre>show pdsn-service { all   name pdsn_name } [ pcf-status [ address ip_address   filter [ all   icmp-monitored   no-calls   summary   up ] ] ] [   { grep grep_options   more } ]</pre> <p><b>all   name <i>pdsn_name</i></b> <b>all:</b> Displays information for all configured packet data services. <b>name <i>pdsn_name</i>:</b> Displays information only for an existing PDSN service specified as an alphanumeric string of 1 through 79 characters.</p> <p><b>pcf-status [ address <i>ip_address</i>   filter [ all   icmp-monitored   no-calls   summary   up ] ]</b> <b>pcf-status:</b> Displays summary information for all Packet Control Functions (PCFs). <b>address <i>ip_address</i>:</b> Only lists information for the PCF with the IP address specified in IPv4 dotted-decimal notation. <b>filter:</b> Filters the output so only the specified information is displayed. If a filter is specified with no keywords, summary information for all PCFs is displayed.</p> <ul style="list-style-type: none"> <li>• <b>all:</b> Displays information for all the PCFs</li> <li>• <b>icmp-monitored:</b> Displays information only for PCFs which are ICMP monitored</li> <li>• <b>no-calls:</b> Displays information only for PCFs which have no active sessions</li> <li>• <b>summary:</b> Displays only a summary of the status of the PCFs</li> <li>• <b>up:</b> Displays information only for PCFs which are alive</li> </ul> <p><b>[ { grep <i>grep_options</i>   more } ]</b> Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent. For details on the usage of <b>grep</b> and <b>more</b>, refer to the <i>Regulating a Command's Output</i> section in the <i>Command Line Interface Overview</i> chapter.</p>
<b>Usage Guidelines</b>	Show the PDSN service information for standard system monitoring or troubleshooting.

**Example**

The following will display the information for all configured services and *sampleService*, respectively:

```
show pdsn-service all
show pdsn-service name sampleService
```

# show pdsnclosedrp-service

Displays information on configured Closed R-P services for the current context.

---

**Product** PDSN

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show pdsn-service { all | name *name* }**

**all | name *name***

**all:** Displays information for all configured Closed R-P services.

**name *name*:** Displays information for an existing Closed R-P service specified as an alphanumeric string of 1 through 79 characters.

---

**Usage Guidelines** Show the Closed R-P service information for standard system monitoring or troubleshooting.

## Example

The following command displays information for the Closed R-P service named *SampleRP* and for all configured services, respectively.

```
show pdsn-service all
show pdsn-service name SampleRP
```

# show peer-profile

Displays configuration of the specified peer profile.

---

**Product** GGSN

P-GW

SAEGW

S-GW

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `show peer-profile { all | full { all | name profile_name } | name profile_name } [ | { grep grep_options | more } ]`

**all**

Displays a list of all peer profiles configured on the system, arranged by service type.

**full { all | name *profile\_name* }**

Displays detailed peer profile configuration information.

**all:** Displays detailed configuration information for all peer profiles configured on the system.

**name *profile\_name*:** Displays detailed configuration information for the specified peer profile.

*profile\_name* is an alphanumeric string of 1 through 64 characters.

**name *profile\_name***

Lists the specified peer profile, and the service type to which it belongs.

*profile\_name* is an alphanumeric string of 1 through 64 characters.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display configuration information for the peer profiles created on the system.

Refer to the **peer-profile** command in the *Global Configuration Mode Commands* chapter and the *Peer Profile Configuration Mode Commands* chapter for more information.

**Example**

The following command displays detailed configuration information for the *pp2* peer profile.

```
show peer-profile full name pp2
```

## show pgw-service

Displays configuration information for PDN Gateway (P-GW) services on this system.

**Product**

P-GW

SAEGW

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

```
show pgw-service { all | name service_name | statistics { all | name service_name } [ verbose ] } [ | { grep grep_options | more } ]
```

#### **all**

Displays configuration information for all P-GW services configured on this system.

#### **name** *service\_name*

Displays configuration information for an existing P-GW service specified as an alphanumeric string of 1 through 63 characters.

#### **statistics** { **all** | **name** *service\_name* } [ **verbose** ]

Displays P-GW service statistics.

**all**: Displays statistics for all P-GW services on the system.

**name** *service\_name*: Displays statistics for an existing P-GW service specified as an alphanumeric string of 1 through 63 characters.

If **verbose** is also specified, the information is displayed in more detail.

#### [ { **grep** *grep\_options* | **more** } ]

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

---

### Usage Guidelines

Use this command to view configuration information for P-GW services on this system.

#### **Example**

The following command displays service statistics for the P-GW service named *pgw1*:

```
show pgw-service name pgw1
```

## show plugin

Displays the current configuration of one or all plugin modules installed on the system. This command is associated with the dynamic software upgrade process.

---

### Product

All

---

### Privilege

Security Administrator, Administrator

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show plugin [ plugin_name ]`

***plugin\_name***

Filters the output by an existing plugin name expressed as an alphanumeric string of 1 through 16 characters.

---

**Usage Guidelines** Displays the attribute settings, priority and version for one or all plugin modules. A plugin module is a shared object library that can be dynamically updated or rolled back. Refer to the *System Administration Guide* for additional information on dynamic software updates.

**Example**

The following command displays the configuration status of all plugin modules currently installed on the system:

```
show plugin
```

## show port

Displays information on configured parameters and operational statistics for physical and logical ports in the system.

---

**Product** All

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show port { datalink counters [ slot/port ] | info [ slot/port ] [ vlan vlan_id ] | npu counters [ slot/port [ tagged | untagged | vlan tag_id ] ] | table | transceiver slot/port | utilization table [ verbose ] } [ | { grep grep_options | more } ]`  
`show port info { slot/port } [ vlan vlan_id ] [ | { grep grep_options | more } ]`  
`show port dinet`

**datalink counters *slot/port***

Displays the physical layer information for all data links or only the one specified by the slot/port location of a previously configured port.

**info [ slot/port ] [ vlan vlan\_id ]**

Displays detailed information for all ports within the chassis or only the one specified by slot/port location of a previously configured port.

**vlan vlan\_id:** Displays detailed information about all Virtual Local Area Networks (VLANs) in the port/slot. If the optional vlan\_id is not specified, this keyword displays port information for all VLANs in the slot/port location.

**npu counters [ slot/port [ tagged | untagged | vlan tag\_id ] ] | bound | unbound ]**

Displays the information for Network Processing Unit (NPU) ports. The information for all ports is output or only the one specified by the slot/port location of a previously configured port.

For ASR 5500 MIO ports, this command displays the combined statistics for the specified port and its paired port (virtual pair).

**tagged:** Display statistics for all tagged packets.

**untagged:** Display statistics for all untagged packets.

**vlan tag\_id:** Display NPU counters for a previously configured VLAN ID.

**bound:** Displays individual and cumulative NPU port counters for the bound ports within the current context. If the command is invoked in the local context, all of the bound ports for all contexts and cumulative counter values for all contexts are displayed.

**unbound:** Displays individual and cumulative NPU port counters for all unbound ports within system.

**table**

Displays information for all physical ports on rear-installed cards with physical interfaces.

**transceiver slot/port**

Displays diagnostic information for all SFP+ transceivers connected to a specified subscriber traffic port on the MIO card.

**utilization table [ verbose ]**

Shows average port utilization in Mbps. The output is a table that lists the current utilization average, a 5-minute average, and a 15-minute average, for all enabled ports.

The **verbose** option displays port utilization with kilobyte accuracy using decimal points.

**{ grep grep\_options | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

**dinet**

Displays the DI-network port statistics.

**Usage Guidelines**

Display port information for troubleshooting of network communications by viewing statistics and configuration information for physical ports.

**Example**

The following displays detailed information for port 1 in slot 17:

```
show port info 17/1
show port table
```

The following displays information for the data link port 33/1:

```
show port datalink counters 33/1
show port npu counters 33/1
```

The following displays detailed information for port 11 in slot 5:

```
show port info 5/11
show port table
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

# show power

Displays information about the power on/off status of individual cards and the operating status of installed power filter units.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show power [ all | chassis | card_num ] [ | { grep grep_options | more } ]
```

**all | chassis | card\_num**

**all**: Displays power on/off state for all cards in the chassis.

**chassis**: Displays the operating status of installed power filter units. This is the default setting.

**card\_num**: Displays the power on/off state for a single card specified an integer from 1 through 48 for the ASR 5000 or 1 through 20 for the ASR 5500.

**| { grep grep\_options | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.



For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

### Usage Guidelines

View power source information to quickly check the power for all cards within a chassis.



#### Important

On some platforms, only **show power** is supported with no other keywords or variables.

### Example

The following displays power supply status for the chassis:

```
show power
```

The following command displays the power status for all slots:

```
show power all
```

## show ppp

Displays the point-to-point protocol (PPP) information, detailed or summarized, for one or all connections by the use of filtering options.

### Product

PDSN  
GGSN

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show ppp { [ counters | full | summary ] { all | callid call_id | imsi id
| msid ms_id | username user_name } | statistics [ pcf-address [ pcf_ip_addr
| all ] | pdsn-service pdsn_name ] } [ | { grep grep_options | more } ]
```

#### counters | full | summary

Filters the output for the level and type of information with the options described below.

**counters**: Displays PPP statistics.

**full**: Displays all available information.

**summary**: Displays only a summary of available information.

```
all | callid call_id | imsi imsi_id | msid ms_id | username user_name }
```

**all**: Displays all available information.

**callid** *call\_id*: Displays PPP information only for the call ID specified as a 4-digit hexadecimal number.

**imsi** *id*: Displays PPP information only for the subscriber with the specified IMSI (International Mobile Subscriber Identity). *id* is a 15-digit field which identifies the subscriber's home country and carrier.

**msid** *ms\_id*: Displays information for a mobile subscriber ID specified as 7 to 16 digits for an IMSI, MIN, or RMI.

**username** *user\_name*: Displays user PPP information for the specified username.

**statistics [ pcf-address [ pcf\_ip\_addr | all ] | pdsn-service pdsn\_name ]**

Displays statistics for all packet data services.

**pcf-address** [ *pcf\_ip\_addr* | **all** ]: Displays statistics only for the time the session is connected to the specified PCF (Packet Control Function) or for all PCFs. *pcf\_ip\_addr* must be specified using IPv4 dotted-decimal notation.

**psdn-service** *psdn\_name*: Display statistics only for an existing PDSN service specified as an alphanumeric string of 1 through 63 characters.

**{ grep grep\_options | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

## Usage Guidelines

View Point-to-Point Protocol information to support troubleshooting subscriber connections by viewing information on PPP connections for a specific subscriber.

### Example

The following displays the PPP summary for all connections.

```
show ppp summary all
```

The following outputs the point-to-point detailed information for the user *user1*.

```
show ppp full username user1
```

The following command displays the standard information for the call with ID *FF0E11CD*.

```
show ppp callid ff0e11cd
```

The following command displays the PPP statistics for *psdn1*.

```
show ppp statistics pdsn-service psdn1
```

The following command provides summarized information for the PPP statistics.

```
show ppp
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

# show prepaid 3gpp2

Displays prepaid accounting information for all services or only the service specified.

---

## Product

PDSN

GGSN

---

## Privilege

Security Administrator, Administrator, Operator, Inspector

---

## Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

## Syntax Description

```
show prepaid 3gpp2 statistics all [ | { grep grep_options | more } ]
show prepaid 3gpp2 statistics { ggsn-service | ha-service | lns-service
| pdsn-service | pdsnclosedrp-service } { all | name service_name } [ | {
grep grep_options | more } ]
show prepaid 3gpp2 statistics per-service-summary } [ | { grep grep_options
| more } ]
```

### all

Displays prepaid statistics for all services.

### ggsn-service

Displays statistics for GGSN service(s).

### ha-service

Displays statistics for HA service(s).

### lns-service

Displays statistics for LNS service(s).

### pdsn-service

Displays statistics for PDSN service(s).

### pdsnclosedrp-service

Displays statistics for PDSN Closed-RP service(s).

### { all | name *service\_name* }

**all**: Displays statistics for all services of the specified type.

**name *service\_name***: Displays statistics for an existing service specified an alphanumeric string of 1 through 63 characters.

**per-service-summary**

Displays prepaid statistics per service summary for all services.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage Guidelines**

Displays Pre-paid statistics for a particular named service or for all services.

**Example**

To display statistics for a PDSN service named *PDSN1*, enter the following command:

```
show prepaid 3gpp2 statistics pdsn-service name PDSN1
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show prepaid wimax

This command displays prepaid WiMAX accounting information for all services or only the service specified.

**Product**

ASN-GW

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show prepaid wimax statistics { all | asngw-service { all | name service_name
} | ha-service { all | name service_name } | per-service-summary } [ | {
s grep_options | more } ]
```

**all**

This keyword displays prepaid statistics for all services.

**asngw-service**

Displays prepaid statistics for Access Service Network-Gateway (ASN-GW) service(s).

**ha-service**

Displays prepaid accounting statistics for Home Agent (HA) service(s).

**{ all | name *service\_name* }**

**all**: Displays statistics for all services of the specified type.

**name *service\_name***: Displays statistics for an existing service specified as an alphanumeric string of 1 through 63 characters.

**per-service-summary**

Displays prepaid statistics per service summary for all services.

**{ *grep grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display prepaid WiMAX accounting statistics for named service or for all services.

**Example**

The following command displays prepaid WiMAX accounting statistics for an ASN-GW service named *asn1*:

```
show prepaid wimax statistics asngw-service name asn1
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show process status

Displays information on process listings in the system.

**Product**

All

**Privilege**

Security Administrator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show process status [ card card_number [ cpu cpu_number ] ]
```

**card** *card\_number*

Displays the process listing for the specific card in the system.

**cpu** *cpu\_number*

Displays the process listing for the specific card and CPU in the system.

**Usage Guidelines**

Displays information on process listings in the system.

**Note**

Only the Security Administrator can run this command.

**Example**

The following displays the list of processes running on card 1 on cpu 0:

```
show process status card 1 cpu 0
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show profile-id-qci-mapping

Displays QoS Class Identifier-Radio Access Network (QCI-RAN) mapping tables configured on this system.

**Product**

HSGW

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show profile-id-qci-mapping table { all | name table_name } [ | { grep  
grep_options | more } ]
```

**all**

Displays information for all QCI-RAN mapping tables configured on this system.

**name** *table\_name*

Displays information for an existing QCI-RAN table specified as an alphanumeric string of 1 through 63 characters.

**{ { grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display the contents of a specific QCI-RAN mapping table or all mapping tables configured on this system.

### Example

The following command displays the contents of a QCI-RAN mapping table named *table1*:

```
show profile-id-qci-mapping table name table1
```

## show ps-network



### Important

In Release 20 and later, HNBNW is not supported. This command must not be used for HNBNW in Release 20 and later. For more information, contact your Cisco account representative.

Displays statistics for the Packet Switched (PS)-network(s) instance configured on a chassis for HNB-GW service sessions.

### Product

HNBNW

### Privilege

Security Administrator, Administrator, Operator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show ps-network { all | name ps_name } [ status ] [ | { grep grep_options | more } ]
```

#### **all**

Displays status counters for all PS (packet switched) networks configured for HNB-GW service sessions on a chassis.

#### **name** *ps\_name*

Displays status counters for a PS network configured for HNB-GW service specified as an alphanumeric string of 1 through 127 characters that is case sensitive

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.

### Usage Guidelines

Use this command to display the status of any or all PS-network(s) instance configured on a chassis for HNB-GW service sessions.

### Example

The following command displays the output for PS network instance status named *ps\_1\_hnb*:

```
show ps-network name ps_1_hnb status
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show ps-network counters



### Important

In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Displays the session counter information for a PS Network associated with Home-NodeB Gateway (HNBGW) services configured and running on a system.

### Product

HNBGW

### Privilege

Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show ps-network counters [ name ps_svc_name [ sgsn sgsn_point_code ] ] [ | {  
grep grep_options | more } ]
```

**name *ps\_svc\_name***

Filters the counter display based on an existing HNB-PS Network service name associated with an HNB-GW service running on system. *ps\_svc\_name* is an alphanumeric string of 1 through 63 characters.



***sgsn sgsn\_point\_code***

Filters the counter display filtered on the basis of SGSN address provided in the SS7 point code that is connected to a particular HNB-PS Network service. *sgsn\_point\_code* must be the address of an SGSN in SS7 point code notation.

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view the session counter information for HNB-PS Network services configured and SGSNs connected on a system.

**Example**

The following command displays the counters for the HNB-PS Network service named *hnb\_ps\_svc1*:

```
show ps-network counters name hnb_ps_svc1
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show ps-network statistics

**Important**

In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Displays the Packet Switched session statistics for Home-NodeB Gateway (HNB-GW) services configured and running on this system.

**Product**

HNBGW

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show ps-network statistics [ name ps_svc_name [ sgsn sgsn_point_code ] ] [
gtpu-only | ranap-only | sccp-only ] [ | { grep grep_options | more } ]
```

**name *ps\_svc\_name***

Filters the session statistics display based on an existing HNB-PS Network service name that is associated with an HNB-GW service running on this system. *ps\_svc\_name* is an alphanumeric string of 1 through 63 characters.

**sgsn *sgsn\_point\_code***

Filters the counter display filtered on the basis of SGSN address provided in the SS7 point code that is connected to a particular HNB-PS Network service. *sgsn\_point\_code* must be the address of an SGSN in SS7 point code notation.

**gtpu-only**

Filters the session statistics to display only GTP-U traffic for the specified HNB-PS Network service which is configured and associated with an HNB-GW service running on this system.

**ranap-only**

Filters the session statistics to display only Radio Access Network Application Protocol (RANAP) traffic for an HNB-PS Network service which is configured and associated with an HNB-GW service running on this system.

**sccp-only**

Filters the session statistics to display only Signaling Connection Control Part (SCCP) traffic for the specified HNB-PS Network service which is configured and associated with an HNB-GW service running on this system.

**| { *grep grep\_options* | *more* }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in *Command Line Interface Overview* chapter of the *Command Line Interface Reference*.

**Usage Guidelines**

Use this command to view the session statistics for overall session or in selected part of user session for HNB-GW services configured and running on this system.

**Example**

The following command displays the session statistics for the HNB-PS Network service named *hnb\_ps1*:

```
show ps-network statistics name hnbps1
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.



## CHAPTER 23

# Exec Mode show Commands (Q-S)

The Exec Mode is the initial entry point into the command line interface system. Exec mode **show** commands are useful in troubleshooting and basic system monitoring.

### Command Modes

This chapter includes the commands **qci-qos-mapping** through **show system uptime**.

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```



### Important

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

- [show qci-qos-mapping](#), on page 1063
- [show qos ip-dscp-iphb-mapping](#), on page 1064
- [show qos l2-mapping-table](#), on page 1064
- [show qos npu inter-subscriber traffic](#), on page 1065
- [show qos npu stats](#), on page 1065
- [show radius](#), on page 1066
- [show radius charging servers](#), on page 1068
- [show radius client](#), on page 1069
- [show radius counters](#), on page 1069
- [show rct stats](#), on page 1071
- [show resources](#), on page 1072
- [show rlf-context-statistics](#), on page 1073
- [show rlf-memcache-statistics](#), on page 1075
- [show rlf-template](#), on page 1075
- [show rohc counters](#), on page 1076
- [show rohc statistics](#), on page 1077
- [show route-map](#), on page 1079
- [show rp](#), on page 1079
- [show rp service-option](#), on page 1081
- [show rp statistics](#), on page 1082
- [show rsvp counters](#), on page 1083

- [show rsvp statistics](#), on page 1084
- [show requirement pac daughtercard](#), on page 1084
- [show s102-service](#), on page 1085
- [show s4-sgsn statistics](#), on page 1086
- [show saegw-service](#), on page 1087
- [show samog-service](#), on page 1088
- [show sbc-service](#), on page 1089
- [show sbc statistics](#), on page 1090
- [show sccp-network](#), on page 1091
- [show sccp statistics](#), on page 1092
- [show scsf-service statistics](#), on page 1093
- [show sctp-param-template](#), on page 1094
- [show security](#), on page 1095
- [show service all](#), on page 1096
- [show session counters historical](#), on page 1096
- [show session counters pcf-summary](#), on page 1099
- [show session disconnect-reasons](#), on page 1100
- [show session duration](#), on page 1102
- [show session progress](#), on page 1104
- [show session recovery status](#), on page 1108
- [show session setup-time](#), on page 1109
- [show session subsystem](#), on page 1110
- [show session trace](#), on page 1113
- [show session-event-record](#), on page 1114
- [show sf](#), on page 1115
- [show sgs-service](#), on page 1115
- [show s4-sgsn statistics](#), on page 1117
- [show sgsn fsm-statistics](#), on page 1117
- [show sgsn sessmgr](#), on page 1118
- [show sgsn-fast-path](#), on page 1119
- [show sgsn-map-app](#), on page 1120
- [show sgsn-mode](#), on page 1120
- [show sgsn-operator-policy](#), on page 1121
- [show sgsn-pool](#), on page 1121
- [show sgsn-service](#), on page 1122
- [show sgtp-service](#), on page 1123
- [show sgtpc statistics](#), on page 1124
- [show sgtpu statistics](#), on page 1125
- [show sgw-service](#), on page 1127
- [show sls-service](#), on page 1128
- [show sms statistics](#), on page 1129
- [show sndcp statistics](#), on page 1130
- [show snmp](#), on page 1131
- [show software authenticity](#), on page 1133
- [show srp](#), on page 1134
- [show ss7-routing-domain](#), on page 1136

- [show ssh](#), on page 1139
- [show ssl cipher-suite](#), on page 1140
- [show ssl connection](#), on page 1140
- [show ssl map](#), on page 1141
- [show ssl statistics](#), on page 1142
- [show subscribers](#), on page 1143
- [show subscribers samog-only](#), on page 1196
- [show subscribers wsg-service](#), on page 1197
- [show super-charger](#), on page 1197
- [show supplementary-service statistics](#), on page 1198
- [show support collection](#), on page 1199
- [show support details](#), on page 1200
- [show support record](#), on page 1202
- [show system ssh key status](#), on page 1203
- [show system uptime](#), on page 1204
- [show sx peers](#), on page 1204

## show qci-qos-mapping

Displays QoS Class Identifier-Quality of Service (QCI-QoS) mapping tables configured on this system.

### Product

ePDG  
HSGW  
P-GW  
SAEGW  
S-GW

### Privilege

Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show qci-qos-mapping table { all | name table_name } [ | { grep_options | more } ]
```

#### **all**

Displays information for all QCI-QoS mapping tables configured on this system.

#### **name *table\_name***

Displays information for an existing QCI-QoS mapping table specified as an alphanumeric string of 1 through 63 characters.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

#### Usage Guidelines

Use this command to display the contents of a specific QCI-QoS mapping table or all mapping tables configured on this system.

#### Example

The following command displays the contents of a QCI-QoS mapping table named *table1*:

```
show qci-qos-mapping table name table1
```

## show qos ip-dscp-iphb-mapping

Displays mapping QoS information in a packet to internal-qos marking.

---

#### Product

ePDG  
HSGW  
P-GW  
SAEGW  
S-GW

---

#### Privilege

Inspector

---

#### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

#### Syntax Description

**show qos ip-dscp-iphb-mapping**

---

#### Usage Guidelines

Use this command to display mapping QoS information in a packet to internal-qos marking.

## show qos l2-mapping-table

Displays named table for the internal to L2 mapping values, like 802.1p and MPLS.

---

#### Product

ePDG  
HSGW  
P-GW  
SAEGW

S-GW

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show qos l2-mapping-table { name table_name | system-default }
```

**name *table\_name***

Displays information for an existing QoS L2 mapping table.

*table\_name* is an existing table specified as an alphanumeric string of 1 through 80 characters.

**system-default**

Displays information for the default system internal mapping to L2 values.

**Usage Guidelines**

Use this command to display named table for the internal to L2 mapping values, like 802.1p and MPLS.

**Example**

The following command displays the contents of a QOS L2 mapping table named *l2table*:

```
show qos l2-mapping-table name l2table
```

## show qos npu inter-subscriber traffic

This command is only supported on PACs running on ST16 platforms. It has been deprecated for use on ASR 5x00 platforms.

## show qos npu stats

Displays Network Processing Unit (NPU) QoS statistics per priority queue for a particular processing card:

**Product**

GGSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show qos npu stats inter-subscriber traffic slot slot_num
```

**slot slot\_num**

Displays statistics for the processing card identified by its slot number as an integer from 1 through 8 and 10 through 16 on the ASR 5000, or 1 through 4 and 7 through 10 on the ASR 5500.

**Usage Guidelines**

This command displays packet and byte counts per NPU QoS priority queue on a per-processing card basis. For additional information on the NPU QoS functionality, refer to the *System Administration Guide*.

**Important**

This functionality is not supported for use with the PDSN at this time.

**Example**

The following command displays NPU QoS priority queue statistics for a processing card installed in chassis slot number 2:

```
show qos npu stats inter-subscriber traffic slot 2
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show radius

Displays and statistic information for RADIUS accounting and/or authentication.

**Product**

PDSN  
HA  
GGSN  
ASN-GW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show radius { accounting servers | authentication servers } [ detail ] [
  admin-status { enabled | disabled } ] [ | { grep grep_options | more } ]
[ radius group group_name [ detail ] [ | { grep grep_options | more } ] ]
```

**accounting servers**

Lists information for configured accounting servers and their current state.



**authentication servers**

Lists information for configured authentication servers and their current state.

**[ detail ]**

Displays historical state information for configured servers of the specified type.

**admin-status { enabled | disabled }**

Displays information for accounting and/or authentication servers with an administrative status of "enabled" or "disabled".

**radius group *group\_name***

Displays the authentication/authorization RADIUS server group information for an existing server group specified as an alphanumeric string of 1 through 63 characters.

**{ *grep grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Display the RADIUS server information as part of periodic monitoring of the health of the system.

**Example**

The following displays the information on configured accounting servers:

```
show radius accounting server
```

The following command displays detailed information for RADIUS accounting servers:

```
show radius accounting servers detail
```

The following command displays detailed information for RADIUS server group *star1* used for authentication:

```
show radius authentication servers radius group star1 detail
```

The following command displays detailed information for RADIUS server group *star1* used for accounting:

```
show radius accounting servers radius group star1 detail
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

# show radius charging servers

This command displays the RADIUS authentication and accounting servers or server group that are configured for use by charging services.

---

## Product

PDSN  
HA  
GGSN  
ASN-GW

---

## Privilege

Security Administrator, Administrator, Operator, Inspector

---

## Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

## Syntax Description

```
show radius charging servers [ radius group group_name ] [ | { grep grep_options | more } ]
```

### **radius group** *group\_name* **all**

Displays all RADIUS counter information for an existing server group configured for use by charging services. *group\_name* is specified as an alphanumeric string of 1 through 63 characters.

### | { **grep** *grep\_options* | **more** }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

## Usage Guidelines

Use this command to display information about RADIUS servers or server group configured for use by Charging Services.

## Example

The following command displays RADIUS servers configured for Charging Services:

```
show radius charging servers
```




---

## Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

# show radius client

Displays information about the RADIUS client configured on the system.

---

## Product

PDSN  
HA  
GGSN  
ASN-GW

---

## Privilege

Security Administrator, Administrator, Operator, Inspector

---

## Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

## Syntax Description

```
show radius client status [ | { grep grep_options | more } ]
```

### **status**

Displays a status summary for the RADIUS client.

### **{ { grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

## Usage Guidelines

Configuring the RADIUS protocol on the system enables RADIUS client functionality. This command displays information pertaining to the status of the client.

### **Example**

The following command displays detailed information pertaining to the system's RADIUS client:

```
show radius client status
```




---

### **Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

# show radius counters

Displays RADIUS server and statistic information for accounting and/or authentication.

<b>Product</b>	PDSN HA GGSN ASN-GW
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<p><b>show radius counters</b> { <b>all</b>   <b>dynamic-auth</b>   <b>radius group</b> <i>group_name</i> [ <b>all</b>   <b>server</b> <i>ip_address</i> [ <b>port</b> <i>number</i> ]   <b>summary</b> [ <b>all-contexts</b> [ <b>verbose</b> ] ] } [   { <b>grep</b> <i>grep_options</i>   <b>more</b> } ]</p> <p><b>counters</b> { <b>all</b>   <b>server</b> <i>ip_address</i> [ <b>port</b> <i>number</i> ] }</p> <p><b>all</b>: Displays statistics for all servers.</p> <p><b>server</b> <i>ip_address</i>: Displays statistics for the server specified by its IPv4 address.</p> <p><b>port</b> <i>number</i>: Displays statistics for a port on the server specified as an integer from 0 through 65535.</p> <p><b>radius group</b> <i>group_name</i> <b>all</b></p> <p>Displays all RADIUS counter information for an existing server group specified as an alphanumeric string of 1 through 63 characters.</p> <p><b>all</b>: Displays statistics for all servers.</p> <p><b>dynamic-auth</b></p> <p>Displays Dynamic Authorization counters for configured RADIUS servers.</p> <p><b>summary</b> [ <b>all-contexts</b> [ <b>verbose</b> ] ]</p> <p>Displays a summary of RADIUS statistics for all the RADIUS servers configured in a specific context.</p> <p><b>all-contexts</b>: Displays a summary of RADIUS statistics for all RADIUS servers configured in all context. If <b>verbose</b> is also specified, the information is displayed in more detail.</p> <p>  { <b>grep</b> <i>grep_options</i>   <b>more</b> }</p> <p>Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.</p> <p>For details on the usage of the <b>grep</b> and <b>more</b> commands, refer to the <i>Regulating a Command's Output</i> section of the <i>Command Line Interface Overview</i> chapter.</p>
<b>Usage Guidelines</b>	Display the RADIUS server information as part of periodic monitoring of the health of the system.

**Example**

The following command displays detailed information pertaining to the RADIUS server group *star1* with in current context:

```
show radius counters radius group star1 all
```

The following displays the statistics for the server with IP address *10.2.3.4*, then just port *7777*, followed by **all** services.

```
show radius counters server 10.2.3.4
show radius counters server 10.2.3.4 port 7777
show radius counters all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show rct stats

Displays statistics associated with Recovery Control Task (RCT) events, including migrations, switchovers and shutdowns. RCT statistics are associated with card-to-card session recovery activities.

**Product**

All products supporting the Session Recovery feature

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show rct stats [verbose] [ | { grep grep_options | more } ]
```

**[verbose]**

Displays full details about RCT events, current status, time stamps and other associated information. This mode is only available if a session recovery event has occurred on the system. The default mode is to display a brief summary of RCT events.

**{ grep grep\_options | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display RCT statistics in Summary or Detailed (verbose) mode. The Detailed output includes the following information:

- Recovery action taken – Migration, Shutdown, Switchover
- Type of event – Planned or Unplanned
- From card to card – slot numbers
- Start time – YYYY-MMM-DD+hh:mm:sss.sss
- Duration – seconds
- Card failure device (such as CPU $n$ )
- Card failure reason
- Card is in usable state or not failed
- Recovery action status – Success or failure reason
- If recovery action failed, failure time stamp
- If recovery action failed, failure task facility name
- If recovery action failed, failure instance number

### Example

The following command displays detailed statistics for RCT events:

```
show rct stats verbose
```



### Important

Output descriptions for **show** commands are available in the *Statistics and Counters Reference*. For additional information, see the *System Administration Guide*.

## show resources

Displays the resource information by CPU or session.

### Product

All

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show resources { cpu | npu | session } [ | { grep grep_options | more } ]
```

#### cpu | npu | session

**cpu**: Displays resource information by CPU.

**npu**: Displays resource information by network processing unit (NPU).

**session**: Displays resource information by session.

**{ { grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

View resource utilization as part of troubleshooting systems which appear sluggish or are having excessive connection timeouts or other connection issues.

### Example

The following display the resource information by CPU and session, respectively.

```
show resources cpu
show resources session
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show rlf-context-statistics

Displays the statistics for all active RLF contexts.

### Product

GGSN  
P-GW  
SaMOG

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show rlf-context-statistics { diamproxy [ facility_num | [ endpoint
endpoint_name [ peer-realm realm_name [ peer-host host_name ] ] ] | sessmgr [
gtpc-context-name gtpccontext_name | instance facility_num ] } [ | summary |
verbose ] [ | { grep grep_options | more } ]
```

#### *facility\_num*

Displays the context information for the specified facility. *num* must be an integer from 1 through 16.

#### *endpoint endpoint\_name*

Displays the context information only for the endpoint specified as a string of size ranging from 1 through 63 characters.

**realm *realm\_name***

Displays the context information only for the realm specified as a string of size ranging from 1 through 127 characters.

**peer-host *host\_name***

Displays the context information only for the host specified as a string of size ranging from 1 through 63 characters.

**gtpc-context-name *gtpccontext\_name***

Displays RLF statistics of GTPC services PGW and GGSN

**instance *facility\_num***

Displays the facility information for specific instance.

**summary**

Displays summary information.

**verbose**

Specifies to display detailed (all available) information. If not specified, concise information is displayed.

Displays the instance level stats. When multiple diamproxies are active, an RLF context's instance is created on each diamproxy or session manager for each peer.

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display RLF statistics for all active RLF contexts.

An RLF context is created only when –

- A peer is bound to a RLF template.
- The peer is in "OPEN" state.

Failure of any of these conditions will cause the RLF context to be deleted.

**Example**

The following command displays RLF statistics for all active RLF contexts:

```
show rlf-context-statistics diamproxy
show rlf-context-statistics sessmgr instance 1 gtpc-context-name ingress

show rlf-context-statistics sessmgr gtpc-context-name ingress
```



## show rlf-memcache-statistics

Displays the memory used by RLF for processing the messages.

---

### Product

GGSN  
P-GW

---

### Privilege

Security Administrator, Administrator, Operator, Inspector

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

```
show rlf-memcache-statistics { diamproxy facility_num | sessmgr [ instance
facility information for specific instance ] } [ | { grep grep_options | more } ]
```

#### ***facility\_num***

Displays the information for the specified facility. *num* must be an integer from 1 through 16.

#### **{ *grep grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

### Usage Guidelines

Use this command to display the memory used by RLF for processing the messages. The output will be displayed only if the memcache is used.

#### **Example**

The following commands displays memory cache statistics for DIAMPROXY and session manager facility:

```
show rlf-memcache-statistics diamproxy
show rlf-memcache-statistics sessmgr instance 1
```

## show rlf-template

Displays the statistics for all active RLF templates.

---

### Product

GGSN  
P-GW

---

### Privilege

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show rlf-template { all | name template_name } [ | { grep grep_options | more } ]
```

**all**

Displays the statistics information for all the configured RLF templates.

**name *template\_name***

Displays the statistics information for the specified RLF template. *template\_name* must be an integer from 1 through 127 characters.

**{ **grep** *grep\_options* | **more** }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display statistics for all or specified RLF template(s).

**Example**

The following command displays statistics for all RLF templates:

```
show rlf-template all
```

## show rohc counters

Displays Robust Header Compression (ROHC) counters for all active calls.

**Product**

PDSN

HSGW

ASN-GW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show rohc counters [ all | callid call_id | imsi imsi_num | ip-address ip_addr | msid msid_num | username user_name ] [ | { grep grep_options | more } ]
```

**all**

Displays all information.

**callid *call\_id***

Displays the information only for the call ID specified as a 4-byte hexadecimal number.

**imsi *imsi\_num***

Displays information for the specified IMSI (International Mobile Subscriber Identity). The IMSI is an up to 15-digit field which identifies the subscriber's home country and carrier: 3 digits of Mobile Country Code (MCC), 2 or 3 digits of Mobile Network Code (MNC), followed by the Mobile Subscriber Identification Number MSIN. Example: 123-45-678910234. May also be entered as 12345678910234.

**ip-address *ip\_addr***

Displays information only for the mobile subscriber IP address specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**msid *msid\_num***

Displays information only for a mobile subscriber ID from 7 to 16 digits for an IMSI, MIN, or RMI.

**username *user\_name***

Displays radio-packet (R-P) interface information only for a specified username.

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Use this command to display ROHC counters for all active calls.

**Example**

The following command displays ROHC counters for all active calls:

```
show rohc counters all
```

## show rohc statistics

Displays statistics and counters for Robust Header Compression (ROHC) IP header compression.

---

**Product**

PDSN

HSGW

ASN-GW

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show rohc statistics** [ **pdsn-service** *pdsnsvc\_name* ] [ **asngw-service** *asngwsvc\_name* ] [ **hsgw-service** *hsgwsvc\_name* ] [ | { **grep** *grep\_options* | **more** } ]




---

**Important**

Keywords available for this command are license-driven. For example, if a PDSN license is loaded, the **pdsn-service** option is visible.

---

**pdsn-service** *pdsnsvc\_name*

Displays ROHC statistics and counters for the an existing PDSN service specified as an alphanumeric string of 1 through 63 characters.

**asngw-service** *asngwsvc\_name*

Displays ROHC statistics and counters for an existing ASN-GW service specified as an alphanumeric string of 1 through 63 characters.

**hsgw-service** *hsgwsvc\_name*

Displays ROHC statistics and counters for an existing HSGW service specified as an alphanumeric string of 1 through 63 characters.

| { **grep** *grep\_options* | **more** }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Use this command to display ROHC statistics for all services or for a specific ASN-GW, PDSN, or HSGW.

**Example**

The following command displays ROHC statistics for the PDSN service named pdsn1:

```
show rohc statistics pdsn-service pdsn1
```




---

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

# show route-map

Displays entries for all route maps or a specific route map.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

**show route-map** [ **name** *route-map name* ] [ | { **grep** *grep\_options* | **more** } ]

**name** *route-map name*

Displays information for a route-map specified as an alphanumeric string of 1 through 79 characters.

{ **grep** *grep\_options* | **more** }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Use this command to see the rules configured in all route-maps for the current context.

**Example**

The following command displays the route-map information for prefix list *Prefix100*:

```
show route-map Prefix100
```

Refer to the **match** and **set** command descriptions in the *Route-map Configuration Mode Commands* chapter for descriptions of the various entries listed.

# show rp

Displays radio-packet (R-P) interface statistics using the filtering options specified.

---

**Product**

PDSN

---

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show rp [ counters | full | summary ] { all | callid call_id | msid ms_id
| peer-address peer_ip_address | username user_name } [ | { grep grep_options |
more } ]
```

**counters | full | summary**

Provides an optional modifier to the output for the desired level and type of information.

**counters:** Displays R-P protocol statistics.

**full:** Displays all available information.

**summary:** Displays only a summary of available information.

These options are not available in conjunction with the keywords **statistics** or **service-option statistics**.

**all | callid *call\_id* | msid *ms\_id* | peer-address *peer\_ip\_address* | username *user\_name***

**all:** Displays all R-P information.

**callid *call\_id*:** Displays only the information for the call ID specified as a 4-digit hexadecimal number.

**msid *ms\_id*:** Displays information only for a mobile subscriber ID specified by 7 to 16 digits for an IMSI, MIN, or RMI.

**peer-address *peer\_ip\_address*:** Displays R-P information for the peer IP address of the PCF specified in IPv4 dotted-decimal notation.

**username *user\_name*:** Displays R-P information for the specified username.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

View the R-P interface statistics for the current context.

**Example**

The following displays the summary for all connections.

```
show rp summary all
```

The following outputs the R-P interface detailed information for the user *isp1user1*.

```
show rp full username isp1user1
```

The following command displays the standard information for the call with ID *FF0E11CD*.

```
show rp callid ff0e11cd
```

The following displays the statistics summary for the R-P facility.

```
show rp
```



**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show rp service-option

Displays the radio-packet (R-P) service option statistics using the filtering options specified.

**Product** PDSN

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

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **show rp service-option statistics** [ **number** *svc\_option\_num* | **pdsn-service** *pdsn\_name* ] [ | { **grep** *grep\_options* | **more** } ]

**number** *svc\_option\_num* | **pdsn-service** *pdsn\_name*

Default: display statistics for all service option numbers and associated packet data services.

**number** *svc\_option\_num*: Displays statistics for the specified service option number.

**pdsn-service** *pdsn\_name*: Displays statistics for the specified packet data service.

{ **grep** *grep\_options* | **more** }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines** View the R-P service option statistics for the current context.

### Example

The following displays the statistics for all service options.

```
show rp service-option statistics
```

The following displays the statistics for service option 5.

```
show rp service-option statistics number 5
```

The following command displays the statistics for all service options in collected for the packet data service *sampleService*.

```
show rp service-option statistics pdsn-service sampleService
```

# show rp statistics

Displays the radio-packet (R-P) protocol statistics using the filtering options specified.

---

**Product**

PDSN

---

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
show rp statistics [ hsgw-service hsgw-name | pcf-summary [ wf1 ] |
pdsn-service pdsn_name | peer-address { peer_address | all } ] [ include-bcmcs
] [ verbose ] [ | { grep grep_options | more } ]
```

**hsgw-service***hsgw\_name*

Specifies an eHRPD Serving Gate Way service followed by the name of an HSGW service specified as an alphanumeric string of 1 through 63 characters.

**pcf-summary** [ **wf1** ]

Displays a session summary of Packet Control Function (PCF) statistics.

The **wf1** option displays PCF statistics in wide-format number 1.

**pdsn-service** *pdsn\_name*

Displays the statistics information for the pdsn-service specified as an alphanumeric string of 1 through 63 characters.

**peer-address** { *peer\_address* | | **all** }

- *peer\_address*: Displays statistics only for the peer specified by its IP address in IPv4 dotted-decimal notation.
- **all**: Displays statistics for all peers.

**verbose**

Displays more detailed statistics.

| { **grep** *grep\_options* | **more** }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

View the R-P statistics for the current context.



**Example**

The following displays all collected R-P statistics.

```
show rp statistics
```

The following displays the R-P statistics associated with the peer address *10.2.3.4*.

```
show rp statistics peer-address 10.2.3.4
```

The following command displays the R-P statistics for the packet data service *PCFnet*.

```
show rp statistics pdsn-service PCFnet
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show rsvp counters

Displays Resource Reservation Protocol (RSVP) counters using the filtering options specified.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show rsvp counters [ all | callid call_id | msid ms_id | username user_name ]
```

**all** | **callid** *call\_id* | **msid** *ms\_id* | **username** *user\_name*

**all**: Displays all RSVP information.

**callid** *call\_id*: Displays information only for the call ID specified as a 4-digit hexadecimal number.

**msid** *ms\_id*: Displays information for a mobile subscriber ID specified a string of 7 to 16 digits for an IMSI, MIN, or RMI.

**username** *user\_name*: Displays RSVP information only for the specified username.

**Usage Guidelines**

View the RSVP counters for the current context.

**Example**

The following displays all collected RSVP counters.

```
show rsvp counters all
```

## show rsvp statistics

Displays Resource Reservation Protocol (RSVP) statistics using the filtering options specified.

---

**Product**

PDSN

---

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

**show rsvp counters [ pdsn-service *service* | sessmgr instance *instance* ]**

**pdsn-service *service* | sessmgr instance *instance***

**pdsn-service *service***: Displays statistics for the service specified as an alphanumeric string of 1 through 63 characters.

**sessmgr instance *instance***: Displays statistics for the specified session manager instance.

---

**Usage Guidelines**

View the RSVP statistics for the current context.

**Example**

The following displays collected RSVP statistics for a *sampleService*.

```
show rsvp statistics pdsn-service sampleService
```

## show requirement pac daughtercard

Displays the system-level status indicating whether or not the encryption daughter card (EDC) is required on PACs within chassis.

---

**Product**

PDSN

GGSN

ASN-GW

---

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

**show requirement pac daughtercard**

**Usage Guidelines**

This command displays whether or not the EDC is required on PACs within the chassis.

**Important**

This command is not supported on all platforms

**Example****show requirement pac daughtercard**

When the EDC requirement is enabled, the output of this command matches this example:

```
[local]chicago# show requirement pac daughtercard
The encryption daughtercard is required for all PACs
[local]chicago#
```

When the EDC requirement is disabled, the output of this command matches this example:

```
[local]chicago# show requirement pac daughtercard
The encryption daughtercard is not required for all PACs
[local]chicago#
```

## show s102-service

Displays the configuration information for the S102 service(s).

**Product**

MME

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show s102-service { all | name s102_service_name | statistics { all | name s102_service_name } }
```

**all**

Displays information for all S102 service configurations.

**name *s102\_service\_name***

Displays configured information for the specified S102 service configuration.

*s102\_service\_name* Enter a string of 1 through 63 alphanumeric characters to identify the uniquely named S102 service.

**statistics { all | name *s102\_service\_name* }**

Generates statistical output indicating the status and activity of the interface for either all S102 services configured on the MME or for the specific named S102 service.

*s102\_service\_name* Enter a string of 1 through 63 alphanumeric characters to identify the uniquely named S102 service.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to verify the parameters set for one or all S102 service configurations.

### Example

The following commands displays the configuration for the S102 service named *s102test*:

```
show s102-service name s102test
```

## show s4-sgsn statistics

Displays statistics related to S4 functionality on the SGSN.

### Product

SGSN

### Privilege

Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show s4-sgsn statistics [ all | smgr-instance <instance_number> ]
```

#### all

Show all S4-SGSN statistics from all session managers.

#### smgr-instance

Show the statistics for a session manager instance of the SGSN service. *<instance\_number>* must be specified as an integer between 1 and 65535.



### Important

If no option is specified, then S4-SGSN statistics from all session managers will be added up and the cumulative totals will be shown.

### Usage Guidelines

Use this command to display information for S4-SGSN related services.

**Example**

The following commands display and clear S4-SGSN-related statistics for all services on the system:

```
show s4-sgsn statistics all
clear s4-sgsn statistics all
```

## show saegw-service

Displays configuration information and node-level statistics for System Architecture Evolution Gateway (SAEGW) services on this system.

<b>Product</b>	SAEGW
----------------	-------

<b>Privilege</b>	Inspector
------------------	-----------

<b>Command Modes</b>	Exec
----------------------	------

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

<b>Syntax Description</b>	<pre>show saegw-service { all   name <i>service_name</i>   statistics { all   name <i>service_name</i> } [ function { pgw [ interface { GnGp   S2a   S5S8 } ]   sgw } ] [ verbose ] } [   { grep <i>grep_options</i>   more } ]</pre>
---------------------------	---

**all**

Displays configuration information for all SAEGW services configured on this system.

**name *service\_name***

Displays configuration information for an existing SAEGW service specified as an alphanumeric string of 1 through 63 characters.

**statistics { all | name *service\_name* } [ function { pgw [ interface { GnGp | S2a | S5S8 } ] | sgw } ] [ verbose ] }**

Displays node-level statistics for SAEGW.

**all:** Displays consolidated node-level statistics for all SAEGW services on the system.

**name *service\_name*:** Displays node-level statistics for an existing SAEGW service specified as an alphanumeric string of 1 through 63 characters.

**function:** Displays node-level statistics of one of the following functions:

- **pgw:** Displays node-level statistics of P-GW function within SAEGW.
- **sgw:** Displays node-level statistics of S-GW function within SAEGW.

**interface:** Displays node-level statistics of P-GW function with respect to one of the following interfaces:

- **GnGp:** Displays node-level statistics of P-GW function with respect to GnGp interface.

- **S2a**: Displays node-level statistics of P-GW function with respect to S2a interface.
- **S5S8**: Displays node-level statistics of P-GW function with respect to S5S8 interface.

If **verbose** is also specified, the information is displayed in more detail.

### **| { grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

### **Usage Guidelines**

Use this command to view configuration information and node-level statistics for SAEGW services on this system.

### **Example**

The following command displays configuration information for the SAEGW service named *saegw1*:

```
show saegw-service name saegw1
```

## show samog-service

Displays configuration and/or statistical information for SaMOG services on this system.

### **Product**

SaMOG

### **Privilege**

Security Administrator, Administrator, Operator, Inspector

### **Syntax Description**

```
show samog-service { all | name name | statistics [ name name ] } [ | {  
  grep grep_options | more } ]
```

### **all**

Displays all SaMOG services.

### **name *name***

Displays information for specific SaMOG service name.

*name* is a string of size 1 to 63.

### **statistics**

Displays Node level Statistics for SaMOG.

### **verbose**

Specifies Detailed statistics.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display configuration and/or statistical information for SaMOG services on this system.

### Example

```
show samog-service all
```

## show sbc-service

Displays information about SBc interface services configured on this system.

### Product

MME

### Privilege

Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show sbc-service { all | cbc-associations { all | sbc-service-name  
sbc_svc_name [ path-info | summary ] } | sbc-service-name sbc_svc_name } [ |  
{ grep grep_options | more } ]
```

#### **all**

Displays information about all SBc interface services configured on this system.

#### **cbc-associations { all | sbc-service-name *sbc\_svc\_name***

Displays information about the SBc interface associations with the Cell Broadcast Centers (CBC).

**all** shows information about all CBC associations.

**sbc-service-name *sbc\_svc\_name*** shows information only for CBC associations for the SBc service name specified as an alphanumeric string of 1 through 63 characters.

#### **sbc-service-name *sbc\_svc\_name***

Displays information only for the SBc service specified as an alphanumeric string of 1 through 63 characters.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display information about SBC services configured on this system.

Refer to the **show sbc statistics** Exec Mode command to display statistics for SBC interface.

### Example

The following command displays information about the CBC associations for the SBC service named *sbc1*

```
show sbc-service cbc-associations sbc-service-name sbc1
```

## show sbc statistics

Displays statistics about SBC interface services configured on this system.

### Product

MME

### Privilege

Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show sbc statistics { all | peer-id peer_id | sbc-service-name sbc_svc_name } [ verbose | { | grep grep_options | more } ]
```

#### all

Displays statistics for all SBC services configured on this system.

#### peer-id peer\_id

Displays statistics for a Cell Broadcast Center (CBC) peer association specified as an integer value from 0 through 4294967295.

Use the **show sbc-service cbc-associations all** command to display the available CBC association peer IDs.

#### sbc-service-name sbc\_svc\_name

Displays statistics for an SBC service specified as an alphanumeric string of 1 through 63 characters.

#### verbose

Displays expanded statistics.



**{ `grep` *grep\_options* | `more` }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display statistics about SBC services configured on this system.

### Example

The following command displays verbose (expanded) statistics for an SBC service named *sbc1*

```
show sbc statistics sbc-service-name sbc1 verbose
```

## show sccp-network

Displays SS7 Signaling Connection Control Part (SCCP) network configuration and status information.

### Product

SGSN

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show sccp-network { ntwk_index | all } [ status [ all | dpc ] ]
```

#### ***ntwk\_index***

Displays configuration and status information for the SCCP network configuration with the network index specified as an integer from 1 through 12.

#### **all**

Displays all available configuration and status information for all SCCP networks.

#### **status all**

Displays all status information for specified SCCP networks.

#### **status dpc**

Displays status information for the device in the SCCP network identified by the destination point-code (DPC).

### Usage Guidelines

Use this command to display global SCCP statistics or to display SCCP statistics for a specified service or network.

**Example**

The following command displays global SCCP statistics:

```
show sccp-network all
```

The following command displays information for an SCCP network configuration with the network index of *I*:

```
show sccp-network I
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show sccp statistics

Displays SS7 Signaling Connection Control Part (SCCP) statistics for services that use the SCCP protocol.

**Product**

SGSN

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show sccp statistics [ iups-service iups_srvc_name | map-service map_srvc_name
| sccp-network ntwk_index [ dpc dpc [ ssn ssn ] | global-title-translation
{ address-map instance add_map_inst | association instance assoc_inst } [
sessmgr instance sessmgr_inst ] ] [ | { grep grep_options | more } ]
```

**iups-service iups\_srvc\_name**

Displays SCCP protocol statistics for an existing IuPS service in the current context specified as an alphanumeric string of 1 through 63 characters.

**map-service map\_srvc\_name**

Displays SCCP protocol statistics for the an existing Mobile Application Part (MAP) service in the current context specified as an alphanumeric string of 1 through 63 characters.

**sccp-network ntwk\_index**

Displays SCCP protocol statistics for the SSCP network configuration with a network index specified as an integer from 1 through 12.

The following filters can be added to fine tune the display of SCCP network statistics:

- **dpc dpc**: Enter a standard pointcode address to limit the display of SCCP network statistics to those for the identified DPC.

- **ssn** *ssn*: Enter an integer from 1 to 255 to limit the display of SCCP network statistics to those for the identified subsystem number.
- **global-title-translation address-map instance** *add\_map\_inst*: Enter an integer from 1 to 4096 to limit the display of SCCP network statistics to those for the identified GTT address-map.
- **global-title-translation association instance** *assoc\_inst*: Enter an integer from 1 to 16 to limit the display of SCCP network statistics to those for the identified GTT association.
- **sessmgr instance** *sessmgr\_inst*: Enter an integer from 1 to 384 to limit the display of SCCP network statistics to those for the identified session manager.

### Usage Guidelines

Use this command to display global SCCP statistics or to display SCCP statistics for a specified service or SCCP network.

### Example

The following command displays global SCCP statistics:

```
show sccp statistics
```

The following command displays SCCP statistics for the IuPS service named *iups-serv1*:

```
show sccp statistics iups-service iups-serv1
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show scsf-service statistics

Displays SCEF Service configuration and status information.

### Product

MME

### Privilege

Security Administrator, Administrator, Operator, Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show scsf-service statistics { all | name service_name | summary }
```

#### all

Displays all available configuration and status information for all SCEF Services.

#### name *service\_name*

Displays all status information for a specified SCEF service name.

**summary**

Displays the summary of the available SCEF service statistics.

**Usage Guidelines**

Use this command to display SCEF service information and its statistics.

**Example**

The following command displays all SCEF service statistics:

```
show scef-service statistics all
```

The following command displays information for an SCEF service configuration with the service name *Test*:

```
show scef-service statistics name Test
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show sctp-param-template

Displays configuration information for Stream Control Transmission Protocol (SCTP) parameter templates configured on this system.

**Product**

MME

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show sctp-param-template { all | name template_name } [ | { grep grep_options | more } ]
```

**all**

Displays configuration information for all SCTP parameter templates configured on this system.

**name *template\_name***

Displays configuration information for an existing SCTP parameter template specified as an alphanumeric string of 1 through 63 characters.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to view configuration information for SCTP parameter templates on this system.

### Example

The following command displays configured parameters for an SCTP parameter template named *sctp\_pt3*:

```
show sctp-param-template name sctp_pt3
```

## show security

Displays information related to the security settings of the system, such as whether this StarOS version is a Trusted build. This command also displays information about the Talos Intelligence Server.

### Product

All

### Privilege

Security Administrator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show security category url url | configuration | server talos-intelligence
  server_name [ verbose ]
```

#### category url *url*

Displays Talos Intelligence categorization information for the specified URL. *url* must be an alphanumeric string from 1 through 512 characters.

#### configuration

Displays information for StarOS trusted builds. This keyword only provides information if the StarOS build is a trusted build. Refer to the *System Administration Guide* for more details about trusted builds.

#### server talos-intelligence *server\_name* [ **verbose** ]

Displays Talos Intelligence server information. *server\_name* must be specified as a case-sensitive alphanumeric string from 1 through 31 characters.

#### verbose

Displays operational status of each database instance.

### Usage Guidelines

Use this command to display security information, such as whether or not the platform is running a Trusted build.




---

**Important** This command can only be executed by a Security Administrator.

---

**Example**

The following command displays security-related configuration information for trusted builds:

```
show security configuration
```

## show service all

Displays configuration information for all services currently configured on this system.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show service all
```

**Usage Guidelines**

Use this command to view configuration information for all services configured on this system.

**Example**

The following command displays information about all services configured on this system:

```
show service all
```

## show session counters historical

Displays historical information for session-related counters based on data collected in bulk statistics.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show session counters historical { all | arrived | callops | connected |
  disconnected | failed | handoff | rejected | renewal } [ all-intervals
  | recent-intervals ] [ cumulative | incremental ] [graph | table] [ 2g |
  3g | 3g-ha | 4g | all | ehrpd | wifi ] [ | { grep grep_options | more } ]
```

**all**

Displays data for all counters either as a single, wide table or multiple graphs.

**arrived**

Displays only data for "total calls arrived" counters. This is based on the "sess-ttlarrived" statistic in the system schema.

**callops**

Displays data for all call operations. This is a calculated value based on the following formula:

(arrived + rejected + disconnected + failed + handoffs + renewals)

**connected**

Displays only data for "total calls connected" counters. This is based on the "sess-ttlconnected" statistic in the system schema.

**disconnected**

Displays only data for "total calls disconnected" counters. This is based on the "sess-ttldisconn" statistic in the system schema.

**failed**

Displays only data for "total calls failed" counters. This is based on the "sess-ttlfailed" statistic in the system schema.

**handoff**

Displays only data for "total handoffs" counters. This is based on the "sess-ttlhandoff" statistic in the system schema.

**rejected**

Displays only data for "total calls rejected" counters. This is based on the "sess-ttlrejected" statistic in the system schema.

**renewal**

Displays only data for "total renewal" counters. This is based on the "sess-ttlrenewal" statistic in the system schema.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Output Options

The following output options are available for this command:

- **all-intervals**: Displays all available historical information from all samples. This filter is used by default.
- **cumulative**: Displays total data for all samples up to and including the last one. In this view, values increase over time.
- **graph**: Displays data in graphical form.
- **incremental**: Displays data changes for each specific sample. The data for each sample is the amount of change since the previous sample. This filter is used by default.
- **recent-intervals**: Displays historical information for only recent samples.
- **table**: Displays data in tabular form. This is the default view.

### Access Technology Categories

The following options display session counters as categorized by access technology type:

- **all**: Displays session counters for all access technology categories.
- **2g**: Displays session counters for calls using 2G GERAN access technology.
- **3g**: Displays session counters for calls using 3G UTRAN access technology.
- **3g-ha**: Displays session counters for 3G-HA (High Availability) sessions.
- **4g**: Displays session counters for calls using 4G EUTRAN access technology.
- **ehrpdp**: Displays session counters for eHRPD (evolved High Rate Packet Data) calls.
- **wifi**: Displays session counters for WiFi calls.

### Usage Guidelines

This command provides the ability to track key session-related statistic information over time. This information can be used as part of system performance monitoring and capacity planning.



### Important

The information provided in the output of this command requires that bulk statistics functionality be enabled on the system. Refer to the *System Administration Guide* for more information on configuring and enabling bulk statistics support.

The output of this command displays historical data collected at various sample intervals. The interval length is 15 minutes and is not user-configurable. Up to 192 samples (two days' worth of data) are maintained.



**Important**

Data collection is "best-effort" over these intervals. Data is preserved on the SMC or MIO card switchovers. As with all counters, certain session failures can cause inaccuracies with counters, including counters which appear to go backwards.

Each sample is identified by a timestamp that displays the approximate time the data was gathered. the timestamp is in the format YYYY:MM:DD:hh:mm:ss.

Data acquired during the sample may be marked with an "S" appended to the end of the timestamp or to the counter value. The "S" indicates that the data is suspect (potentially bad). Occurrences of this result from events like changes to the real time clock, which can cause an interval to be an atypical length. Instances of suspect data should be rare. Additionally, there may be occasions in which a sample may be marked as "invalid". "invalid" identifies bad data, a situation that could result when the polling has not run long enough, or because of an unexpected error retrieving data.

Since baseline values must be obtained prior to collecting interval samples, the first interval of data will not be available until up to twice the interval period.

**Example**

The following command displays cumulative total calls arrived information for the most recent intervals and displays the output in graphical format:

```
show session counters historical arrived recent-intervals cumulative graph
```

The following command displays historical data for all counters for all intervals and displays the output in tabular format:

```
show session counters historical all
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show session counters pcf-summary

Displays the Packet Control Function (PCF) summary which include the number of calls, call types, and Tx/Rx packets/octets statistics.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `show session counters pcf-summary [ call-types | data | wfl [ pcf pcf_address  
| [ | { grep grep_options | more } ] ] ]`

**call-types**

Displays the number of calls and the types of calls.

**data**

Displays the number of successful calls and Tx/Rx packets/octets statistics.

**pcf pcf\_address**

Displays the given PCF summary for a particular address.

**wfl**

Displays the PCF summary in a single very wide line.

**| { grep grep\_options | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines** Use this command to display a summary of all PCFs.

**Example**

```
show session counters pcf-summary
```

## show session disconnect-reasons

Displays a list of the reasons for call disconnects and the number of calls disconnected for each reason.

**Product** All

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

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** `show session disconnect-reasons [ buckets | gprs-only | pgw-only |  
sgsn-only | sgw-only | verbose ] [ | { grep grep_options | more } ] ]`

**buckets**

Displays additional disconnect reasons in pre-configured bucket-intervals.

**gprs-only**

Only supported on the SGSN.

This keyword limits the display to session disconnect reasons for the SGSN's 2G MM and PDP context disconnects.

**pgw-only**

Supported on the GGSN, P-GW, and SAEGW only.

Displays cumulative session disconnect reason statistics specific to P-GW/GGSN calls. The following call types fall under this category:

- P-GW Call
- GGSN Call (both standalone GGSN service as well as GGSN service associated with P-GW service)
- SAEGW Call (P-GW-Anchored)
- SAEGW Call (GGSN-Anchored)
- SAEGW Call (Co-located)

**sgw-only**

Supported on the SAEGW and S-GW only.

Displays cumulative session disconnect reason statistics specific to S-GW calls. S-GW calls include:

- S-GW calls
- SAEGW calls that are S-GW anchored only

**sgsn-only**

Only supported on the SGSN.

Displays session disconnect reasons for the SGSN's 3G MM and PDP context disconnects.

**verbose**

List all disconnect reasons even if the values are zero (0).

**Important**

The **verbose** option is not supported for the **buckets** keyword.

**{ *grep grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display a list of the reasons why calls were disconnected.

### Example

To view session disconnect statistics, enter the following command:

```
show session disconnect-reasons
```

To view a list of the disconnect reasons with verbose output, enter the following command:

```
show session disconnect-reasons verbose
```

## show session duration

Displays session duration information for the current context filtered by the options specified.

### Product

All

### Privilege

Security Administrator, Administrator, Inspector, Operator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show session duration [ session_filter ] [ | { grep grep_options | more } ]
```

#### *session\_filter*

Specifies the name of the entity whose session duration information is to be filtered and displayed. This options are:

- **apn** *apn\_name*: Displays session information for an existing Access Point Name (APN) specified as an alphanumeric string of 1 through 62 characters that is case sensitive.
- **asn-peer-address** *ip\_address*: Displays session information for the ASN GW peer whose IP address is specified in IPv4 dotted-decimal notation.
- **asngw-service** *service\_name*: Displays session information for the specified ASN-GW service.
- **asnpc-peer-address** *ip\_address*: Displays session information for the Access Service Network Paging Controller (ASN PC) peer whose IP address is specified in IPv4 dotted-decimal notation.
- **asnpc-service** *service\_name*: Displays session information for the specified ASN PC service.
- **dhcp-server** *dhcp\_address*: Displays session information for the Dynamic Host Configuration Protocol (DHCP) server specified by its IP address in IPv4 dotted-decimal notation.
- **epdg-service** *service\_name*: Displays session information for ePDG service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

- **fa** *fa\_address*: Displays session information for the foreign agent (FA) whose IP address is specified in IPv4 dotted-decimal notation.
- **fa-service** *fa\_name*: Displays session information for the named foreign agent service.
- **fng-service** *fng\_name*: Displays session information for the named Femto Network Gateway service.
- **ggsn-service** *ggsn\_name*: Displays session information for an existing GGSN service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.
- **gprs-only**: Limits the display to the session information for the SGSN's 2G MM and PDP contexts.
- **ha** *ha\_address*: Displays session information for the home agent specified by its IP address in IPv4 dotted-decimal notation.
- **ha-service** *ha\_name*: Displays session information for the named home agent (HA) service.
- **hnbgw-only**: Displays session information for the HNB-GW service related sessions instances (such as HNB, IuPS, IuCS).




---

**important** In Release 20 and later, HNBGW is not supported. This keyword must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

---

- **hsgw-service** *service\_name*: Displays session information for an existing HSGW service specified as an alphanumeric string of 1 through 63 characters.
- **lma-service** *service\_name*: Displays session information for an existing Local Mobility Anchor (LMA) service specified as an alphanumeric string of 1 through 63 characters.
- **mag-service** *service\_name*: Displays session information for an existing Mobile Access Gateway (MAG) service specified as an alphanumeric string of 1 through 63 characters.
- **mme-service** *service\_name*: Displays session information for an existing Mobility Management Entity (MME) service specified as an alphanumeric string of 1 through 63 characters.
- **pcc-service** *service\_name*: Displays session information for an existing Policy and Charging Control service specified as an alphanumeric string of 1 through 63 characters.
- **pcf** *pcf\_address*: Displays session information for the packet control function specified by its IP address in IPv4 dotted-decimal notation.
- **pdif-service** *service\_name*: Displays session information for the named Packet Data Interworking Function service.
- **qci** { **all** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **non-std** } \*: Displays the length of time a dedicated bearer is established on the network for a given QCI. More than one QCI value can be specified.
- **pdsn-service** *pdsn\_name*: Displays session information for the named packet data service.




---

**Important**

If no PCF address or PDSN service is specified, the session information for all sessions is displayed.

---

- **pdsnclosedrp-service** *service\_name*: Displays all L2TP tunnels in the specified Closed R-P service.

- **qci** *std\_value* [ **all** ] [ **non-std** ] Displays session duration information for a specified or all QoS Class Index (QCI) values. The standard QCI value is an integer from 1 through 9.
- **sgsn-address** *sgsn-address*: Displays session information for the SGSN specified by its IP address in IPv4 dotted-decimal notation.
- **sgsn-only**: Limits the display to the session information for the SGSN's 3G MM and PDP contexts.
- **sgw-service** *service\_name*: Displays session information for an existing S-GW service specified as an alphanumeric string of 1 through 63 characters.
- **wsg-service** *service\_name*: Displays session information for an existing Security Gateway (wsg-service) service specified as an alphanumeric string of 1 through 63 characters.

### | { **grep** *grep\_options* | **more** }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

#### Usage Guidelines

View the session information to troubleshoot subscriber problems and for general monitoring for orphaned sessions.

#### Example

The following commands display the duration for the session connected to the packet control function with address *10.2.3.4*, packet data service *sampleService*, and for all sessions, respectively.

```
show session duration pcf 10.2.3.4
show session duration pdsn-service sampleService
show session duration
```

## show session progress

Displays session progress information for the current context filtered by the options specified.

#### Product

All

#### Privilege

Security Administrator, Administrator, Inspector, Operator

#### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

#### Syntax Description

```
show session progress [ apn apn_name | asn-peer-address ip_address |
asngw-service service_name | asnpc-service service_name | asnpc-peer-address
ip_address | dhcp-server dhcp_address | epdg-service service_name | fa fa_address
| fa-service fa_name | ggsn-service ggsn_name | ha ha_address | ha-service ha_name
```

```

| hsgw-servie service_name | lma-service service_name | mag-service service_name
| mipv6-service service_name | mme-address mme_address | pcc-address service_name |
pcf { pcf_address pdif-service service_name | pdsn-service pdsn_name service_name
| pgw-address ip_address | saegw-service service_name | samog-service service_name
| sgsn-address sgsn_address | sgw-service service_name | wsg-service service_name
} [ | { grep grep_options | more } ]

```

**apn apn\_name**

Displays session information for an existing Access Point Name (APN) specified as an alphanumeric string of 1 through 62 characters that is case sensitive.

**asn-peer-address ip\_address**

Displays session information for the Access Service Network-Gateway (ASN-GW) peer specified by its IP address in IPv4 dotted-decimal notation.

**asn-gw-service service\_name**

Displays session information for an existing ASN-GW service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**asnpc-service service\_name**

Displays session information for an existing Access Service Network Paging Controller (ASN PC) service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**asnpc-peer-address ip\_address**

Displays session information for the ASN PC peer specified by its IP address in IPv4 dotted-decimal notation.

**dhcp-server dhcp\_address**

Displays session information for a Dynamic Host Configuration Protocol (DHCP) server specified by its IP address in IPv4 dotted-decimal notation.

**epdg-service service\_name**

Displays session information for an existing Evolved Packet Data Gateway (ePDG) service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**fa fa\_address**

Displays session information for the foreign agent (FA) whose IP address is specified in IPv4 dotted-decimal notation.

**fa-service fa\_name**

Displays session information for an existing FA service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**ggsn-service *ggsn\_name***

Displays session information for an existing Gateway GPRS Support Node (GGSN) service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**ha *ha\_address* | ha-service**

Displays session information for the home agent specified by its IP address in IPv4 dotted-decimal notation.

**ha-service *ha\_name***

Displays session information for an existing Home Agent (HA) service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**hsgw-service *service\_name***

Displays session information for an existing HRPD Serving Gateway (HSGW) service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**lma-service *service\_name***

Displays session information for an existing Local Mobility Anchor (LMA) service specified as an alphanumeric string of 1 through 63 characters.

**mag-service *service\_name***

Displays session information for an existing Mobile Access Gateway (MAG) service specified as an alphanumeric string of 1 through 63 characters.

**mipv6ha-service-service *service\_name***

Displays session information for an existing Mobile Internet Protocol version 6 (MIPv6) Home Agent (HA) service specified as an alphanumeric string of 1 through 63 characters.

**mme-address *mme\_address***

Displays session progress information for the Mobility Management Entity (MME) specified by its IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**pcc-service *service\_name***

Displays session information for an existing Policy Charging Control (PCC) service specified as an alphanumeric string of 1 through 63 characters.

**pcf *pcf\_address***

Displays session information for the Packet Control Function (PCF) specified by its IP address in IPv4 dotted-decimal notation.

**pdif-service *service\_name***

Displays session information for an existing Packet Data Interworking Function (PDIF) service specified as an alphanumeric string of 1 through 63 characters.



**pdsn-service *service\_name***

Displays session information for an existing Packet Data Serving Node (PDSN) service specified as an alphanumeric string of 1 through 63 characters.

**pgw-address *ip\_address***

Displays session progress information for the PDN-Gateway (P-GW) specified by its IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**saegw-service *service\_name***

Displays session information for an existing System Architecture Evolution-Gateway (SAE-GW) service specified as an alphanumeric string of 1 through 63 characters.

**samog-service *service\_name***

Displays session progress information for an existing S2a Mobility over GTP (SaMOG) service specified as an alphanumeric string of 1 through 63 characters.

**sgsn-address *sgsn\_address***

Displays session information for the Serving GPRS Support Node (SGSN) specified by its IP address in IPv4 dotted-decimal notation.

**sgw-service *service\_name***

Displays session progress information for an existing Serving Gateway (S-GW) service specified as an alphanumeric string of 1 through 63 characters.

**wsg-service *service\_name***

Displays session progress information for an existing Wireless Security Gateway (WSG) service specified as an alphanumeric string of 1 through 63 characters.

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

View the session information to troubleshooting subscriber problems and for general monitoring for orphaned sessions.

**Example**

The following commands display the status information for the session connected to the packet control function with address *10.2.3.4*, packet data service *sampleService*, and for all sessions, respectively.

```
show session progress pcf 10.2.3.4
show session progress pdsn-service sampleService
show session progress
```

**Important**

Output descriptions for this command are available in the *show session* chapter of the *Statistics and Counters Reference*.

## show session recovery status

Displays session recovery status information for the current context filtered by the options specified.

**Product**

All

**Privilege**

Security Administrator, Administrator, Inspector, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show session recovery status [ verbose ] [ | { grep grep_options | more } ]
```

**recovery status**

Displays the current status of the system's ability to recover from a hardware or software fault that requires the recovery of home agent-based Mobile IP session(s).

**verbose**

Includes per-CPU Session Recovery status.

**| { grep grep\_options | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

View the session information for troubleshooting subscriber problems and for general monitoring for orphaned sessions.

**Example**

To display the session recovery status information, enter the following command:

```
show session recovery status
```

Adding the optional verbose keyword to this command provides more details.

```
show session recovery status verbose
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show session setuptime

Displays session setup time information for all sessions or sessions associated with the specified Access Gateway (AGW).

### Product

ePDG  
PDSN  
HNB-GW  
SGSN

### Privilege

Operator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show session setuptime [ epdg-only [ verbose ] | hnbgw-only | pcf pcf_address
| gprs-only | sgsn-address sgsn_address | sgsn-only ] [ | { grep grep_options
| more } ]
```

```
[ epdg-only [ verbose ] hnbgw-only | mme-only | pcf pcf_address | gprs-only | sgsn-address sgsn_address
| sgsn-only ]
```

Displays the call setup times aggregated into basic ranges of time.

- **epdg-only**: Display ePDG Session Statistics. **verbose**: Displays session setup times in verbose mode.
- **hnbgw-only**: Filters and displays the call setup information for HNB-GW calls only.



### Important

In Release 20 and later, HNBGW is not supported. This keyword must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

- **pcf pcf\_address**: displays call setup data for the packet control function whose IP address is specified as *pcf\_address*. *pcf\_address* must be specified using IPv4 dotted-decimal notation. The call setup times for all PCFs is displayed when no specified PCF is specified.
- **gprs-only**: Displays 2G call setup data for the for the SGSN for the MM and PDP contexts.

- **sgsn-address** *sgsn\_address*: Displays call setup times for the specified SGSN. *sgsn\_address* is the IP address of the SGSN and must be expressed in IPv4 dotted-decimal notation. This keyword is used by the GGSN.
- **sgsn-only**: Displays 3G call setup data for the for the SGSN for the MM and PDP contexts.

### | { **grep** *grep\_options* | **more** }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

View the session information to troubleshooting subscriber problems and for general monitoring for orphaned sessions.

When no keywords are specified, the information shown is cumulative for all sessions that have been facilitated by the system.

### Example

The following command shows setup time statistics for all sessions from the PCF at IP address *192.168.10.3*:

```
show session setuptime pcf 192.168.10.3
```

## show session subsystem

Displays session information for system subsystems. If no keywords are specified, information for all subsystems is displayed.

### Product

All

### Privilege

Security Administrator, Administrator, Inspector, Operator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show session subsystem [ full | facility facility [ all | instance id ] ]
[ verbose ] [ | { grep grep_options | more } ]
```

### [ full | facility *facility* [ all | instance *id* ] ]

- **full**: Indicates that a full statistics summary of all subsystems is to be displayed.
- **facility** *facility*: Specifies the facility for which subsystem statistics is to be displayed where *facility* is specified as one of:
  - **a11mgr**: A11 Manager

- **aaamgr**: Accounting and Authentication Manager
- **aaaproxy**: AAA Proxy Manager
- **alcapmgr**: ALCAP Manager
- **asngwmgr**: ASN Gateway Manager
- **asnpcmgr**: ASN Paging/Location-Registry Manager
- **dgmbmgr**: Diameter Gmb Application Manager
- **diamproxy**: Diameter Proxy Application Manager [Release 12.0 and earlier versions only]
- **egtpegmgr**: EGTP Egress Demux Manager
- **egtpinmgr**: EGTP Ingress Demux Manager
- **famgr**: Foreign Agent Manager
- **gtpcmgr**: GTP-C Manager
- **gtpumgr**: GTP-U Demux Manager
- **hamgr**: Home Agent Manager
- **henbgwdemux**: Home eNodeB Gateway demux manager




---

**Important** In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

- **henbgwmgr**: Home eNodeB Gateway Manager




---

**Important** In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

- **hnbmgr**: HNBGW HNB Manager




---

**Important** In Release 20 and later, HNBGW is not supported. This keyword must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

---

- **imsimgr**: SGSN IMSI Manager
- **ipsgmgr**: IP Services Gateway Manager
- **l2tpdemux**: L2TP Demux Manager
- **l2tpmgr**: L2TP Manager

- **linkmgr**: SGSN/SS7 Master Manager
- **magmgr**: Mobile Access Gateway Manager
- **megadiammgr**: MegaDiameter Manager
- **mmedemux**: MME Demux Manager
- **mmemgr**: MME Manager
- **mmgr**: SGSN/SS7 Master Manager
- **pdgmgr**: PDG Manager
- **phsgwmgr**: PHS Gateway Manager
- **phspcmgr**: PHS Paging Controller Manager
- **sessmgr**: Session Manager
- **sgtpcmgr**: SGSN GTP-C Manager

- **all** | **instance** *id*: the keyword **all** indicates all instances of the specified facility are to be displayed whereas the keyword **instance** specifies a specific instance for which information is to be displayed where *id* must be specified as an integer from 0 through 4294967295. If all or instance is not specified summary statistics are displayed.

### verbose

Displays everything the **show session subsystem** command displays with the exception that the Setup Time statistics are reported in 100 millisecond increments from 100 ms up to 9600 ms.

### { **grep** *grep\_options* | **more** }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

View the session information to troubleshooting subscriber problems and for general monitoring for orphaned sessions.

If this command is entered with no keywords, the information displayed is cumulative for all sessions facilitated by the system.

### Example

The following commands display the statistics information summarized for all sessions, then for the *famgr* facility (all sessions), and finally only for the session ID *127589* for the *hamgr* subsystem.

```
show session subsystem full
show session subsystem facility famgr all
show session subsystem facility hamgr instance 127589
```



**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show session trace

Displays status and statistics for the session trace application.

### Product

GGSN  
MME  
P-GW  
SAEGW  
S-GW

### Privilege

Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show session trace { statistics | subscriber network-element { ggsn | mme  
| pgw | sgw } trace-ref value | tce-address ip_address tce-index num |  
tce-summary | trace-summary } [ | { grep grep_options | more } ]
```

#### **statistics**

Displays summary statistics for the session trace subsystem.

#### **subscriber network-element { ggsn | mme | pgw | sgw } trace-ref value**

Displays status and statistics for a specified session trace using the network element type; GGSN, MME, P-GW, and S-GW, and a valid trace reference of 12 characters.

#### **tce-address ip\_address tce-index num**

Displays status and statistics for an existing Trace Collection Entity (TCE) connection specified by its IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**tce-index num**: Specifies a TCE index of the trace collection entity as an integer from 0 through 7.

#### **tce-summary**

Displays a summary of all active TCE connections.

#### **trace-summary**

Displays a summary of all active session traces.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display status and statistics for the session trace application.

### Example

The following command displays status and statistics for a subscriber session trace on a P-GW with a trace reference of *32223398765*:

```
show session trace subscriber network-element pgw trace-ref 32223398765
```

The following command displays status and statistics for a subscriber session trace on an MME with a trace reference of *32221234567*:

```
show session trace subscriber network-element mme trace-ref 32223398765
```

The following command displays status and statistics for a subscriber session trace on an GGSN with a trace reference of *1203398765*:

```
show session trace subscriber network-element ggsn trace-ref 1203398765
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show session-event-record

Displays session event module statistics and file space usage information.

### Product

S-GW  
SAEGW

### Privilege

Operator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show session-event-record { file-space-usage | statistics }
```

#### file-space-usage

Displays session event module file storage limits and capacities.



**statistics**

Displays session event module statistics regarding the handling and transfer of event records to an external collection server.

**Usage Guidelines**

View the session event information to troubleshoot handling and transfer problems and for general monitoring for file storage use.

**Example**

The following command displays the file storage limit and use for all event modules on the system:

```
show session-event-record file-space-usage
```

## show sf

Displays switch fabric task (SFT) information associated with packet processing cards.

**Product**

All

**Privilege**

Inspector

**Syntax Description**

```
show sf stats sft [ historical ]
```

**historical**

Displays historical information regarding SFT performance.

**Usage Guidelines**

Use this command to display information and statistics about the switch fabric task.

**Example**

The following command displays statistics for the SFT:

```
show sf stats sft
```

## show sgs-service

Displays information and statistics about Visitor Location Register (VLR) SGs interface services configured on this system.

**Product**

MME

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show sgs-service { all | name name | offload-status [ service-name
sgs_svc_name ] | statistics { all | name name } | vlr-status [ service-name
sgs_svc_name ] [ vlr-name name ] [ full [ wf1 ] ] [ | { grep grep_options |
more } ]
```

**all**

Displays information about all SGs interface services configured on this system.

**name *name***

Displays information about an existing SGs service specified as an alphanumeric string of 1 through 63 characters.

**offload-status *sgs\_svc\_name***

Displays statistics for all VLRs flagged for offload for an existing SGs service specified as an alphanumeric string of 1 through 63 characters.

**statistics { all | name *name* }**

Displays statistics for SGs services configured on this system.

**all**: Displays statistics for all SGs services configured on this system.

**name *name***: Displays statistics for an existing SGs service specified as an alphanumeric string of 1 through 63 characters.

**vlr-status [ service-name *name* ] [ vlr-name *name* ] [ full [ wf1 ] ]**

Displays status information about VLRs configured in SGs services on this system.

**service-name *sgs\_svc\_name***: Displays names and states of VLRs configured in an existing SGs service specified as an alphanumeric string of 1 through 63 characters.

**vlr-name *name***: Displays the name and state of an existing VLR configured in SGs services on this system and specified as an alphanumeric string of 1 through 63 characters.

**full**: Displays additional information about VLRs configured in SGs services on this system. Additional information includes ports, addresses and peer IDs.

**wf1**: Displays the output in a tabular format.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display information and statistics about SGs services configured on this system.

**Example**

The following command displays statistics for an SGs service named *sgs3*:

```
show sgs-service name sgs3
```

The following command displays VLR status information for a configured VLR named *vlr-main*:

```
show sgs-service vlr-status vlr-name vlr-main
```

## show s4-sgsn statistics

Displays statistics related to S4 functionality on the SGSN.

---

**Product** SGSN

---

**Privilege** Inspector

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show s4-sgsn statistics [ all | smgr-instance <instance\_number> ]**

### all

Show all S4-SGSN statistics from all session managers.

### smgr-instance

Show the statistics for a session manager instance of the SGSN service. *<instance\_number>* must be specified as an integer between 1 and 65535.




---

**Important**

If no option is specified, then S4-SGSN statistics from all session managers will be added up and the cumulative totals will be shown.

---



---

**Usage Guidelines**

Use this command to display information for S4-SGSN related services.

### Example

The following commands display and clear S4-SGSN-related statistics for all services on the system:

```
show s4-sgsn statistics all
clear s4-sgsn statistics all
```

## show sgsn fsm-statistics

The output of this command provides information on 3G SGSN (both Gn and S4) application FSM statistics.

---

**Product** SGSN

<b>Privilege</b>	Inspector, Operator, Administrator, Security Administrator
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<b>show sgsn fsm statistics { umts-sm   umts-pmm   all }</b>  <b>umts-sm</b> Displays 3G Session Management Access Side FSM statistics.  <b>umts-pmm</b> Displays 3G Mobility Management PMM FSM statistics.  <b>all</b> Displays all SGSN application FSM statistics.
<b>Usage Guidelines</b>	Use this command to track 3G SGSN (both Gn and S4) application FSM statistics. The SGSN application FSM statistics will help collect the FSM usage information to quantify which events / state collisions happen most often in the field.
<b>Example</b>	Enter this command to display all SGSN FSM statistics: <b>show sgsn fsm statistics all</b>

## show sgsn sessmgr

Displays session manager (SessMGR) statistics specific to the SGSN service.

<b>Product</b>	SGSN
<b>Privilege</b>	Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<b>show sgsn sessmgr { all   instance smgr_inst }</b>  <b>all</b> Displays all SessMGR statistics specific to the system's SGSN services.

**instance *smgr\_inst***

Displays the statistics for a session manager instance of the SGSN service specified as an integer between 1 and 10000000.

**Usage Guidelines**

Use this command to display information for SGSN services.

**Example**

The following command displays SGSN SessMGR statistics for all SGSN services on the system:

```
show sgsn sessmgr all
```

## show sgsn-fast-path

Displays information related to SGSN fast-path.

**Note**

This command is not supported by SGSN from software release 16.2 onwards as the NPU FastPath feature is not supported by SGSN from the 16.2 release.

**Product**

SGSN

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show sgsn-fast-path statistics [ all | smgr-instance smgr_inst ] [ [ | { grep grep_options | more } ]
```

**all**

Displays fast-path statistics for all session managers.

**smgr-instance *smgr\_inst***

For releases prior to 14.0, this keyword displays the fast-path statistics for a session manager instance specified as an integer between 1 and 65535.

For releases 14.0 and higher, this keyword displays the fast-path statistics for a session manager instance specified as an integer between 1 and 384.

**{ **grep** *grep\_options* | **more** }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display statistics for SGSN fast-path configurations.

### Example

The following command displays fast-path statistics for all SGSN session managers:

```
show sgsn sessmgr all
```

## show sgsn-map-app

Displays collected statistics for the SGSN Mobile Application Part (MAP).

### Product

SGSN

### Privilege

Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show sgsn-map-app statistics [ | { grep grep_options | more } ]
```

### all

Displays collected statistics for the SGSN MAP application.

### { grep *grep\_options* | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display statistics for the SGSN MAP application.

### Example

The following command displays SGSN MAP statistics:

```
show sgsn-map-app statistics
```

## show sgsn-mode

Displays the SGSN global configuration.

<b>Product</b>	SGSN
<b>Privilege</b>	Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<pre>show sgsn-mode [   { grep grep_options   more } ]</pre> <pre>{ { grep grep_options   more }</pre> <p>Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.</p> <p>For details on the usage of the <b>grep</b> and <b>more</b> commands, refer to the <i>Regulating a Command's Output</i> section of the <i>Command Line Interface Overview</i> chapter.</p>
<b>Usage Guidelines</b>	Use this command to display the configuration created with the commands in the SGSN Global Configuration mode.
	<p><b>Example</b></p> <p>The following command displays the SGSN global configuration:</p> <pre>show sgsn-mode</pre>

## show sgsn-operator-policy

This command has been deprecated. Refer to the **show operator-policy** command.

## show sgsn-pool

Displays collected pooling statistics for either GPRS services or SGSN services.

<b>Product</b>	SGSN
<b>Privilege</b>	Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<pre>show sgsn-pool statistics { gprs-service srv_name   sgsn-service srv_name } { nri-value nri_value   peer-non-broadcast-lac lac rac rac   target-load-in-progress [ smgr-instance smgr_instance   target-nri target_nri</pre>

```
 ] | target-offloaded-to-peer [ target-nri target_nri ] } [ | { grep
grep_options | more } ]
```

```
| { grep grep_options | more }
```

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display the collected statistics for pooling in either GPRS or SGSN services. The outputs can be filtered to focus the statistics displayed.

### Example

The following command displays the:

```
show sgsn-pool statistics sgsn-service sgsn1 nri-value 3
```

## show sgsn-service

Displays information about the configured SGSN services in the current context.

### Product

SGSN

### Privilege

Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show sgsn-servie { all | name svc_name }
```

#### all

Displays information for all SGSN services in the current context.

#### name *svc\_name*

Displays information for an existing SGSN service specified as an alphanumeric string of 1 through 63 characters.

### Usage Guidelines

Use this command to display information for SGSN services.

### Example

The following command displays information for all SGSN services in the current context:

```
show sgsn-service all
```



The following command displays information for an SGSN service in the current context that is named *sgsn1*:

```
show sgtn-service name sgtn1
```


**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show sgtp-service

Displays information about the configured GPRS Tunnelling Protocol (SGTP) services in the current context, including GTP-C and GTP-U operational configuration.

**Product**

SGSN  
PDG/TTG  
MME

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show sgtp-service all [ gtpu-table ] |{ ggsn-table [
smgr-instance smgr_instance ] | mbms-bearers | name svc_name [ gtpu-table ]
| }sgsn-table
```

**all [ gtpu-table ]**

Displays configuration information for all of the SGTP services defined for the current context.

**gtpu-table**: Limits the output to GTPU information for all SGTP services.

**ggsn-table [ smgr-instance svc\_name ]**

Displays GGSN information configured for the SGTP service(s) in the current context.

**smgr-instance** *svc\_name* enter an integer from 1 through 384 to limit the GGSN output to information for a specific session manager.

**mbms-bearers**

This keyword is specific to the SGSN and is not yet supported.

**name *svc\_name* [ gtpu-table ]**

Displays information for the specified SGTP service in the current context. *svc\_name* must be an alphanumeric string of 1 through 63 characters that identifies a configured SGTP service.

**gtpu-table:** Limits the output to GTPU information for a specific SGTP service.

### sgsn-table

Displays SGSN information configured for the SGTP service(s) in the current context.

### Usage Guidelines

Use this command to control the display of SGTP services information.

### Example

The following command displays information for all SGTP services in the current context:

```
show sgtp-service all
```

The following command displays the GGSN information in SGTP services in the current context:

```
show sgtp-service ggsn-table
```

The following command displays the SGSN information in SGTP services in the current context:

```
show sgtp-service sgsn-table
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show sgtpc statistics

Displays all statistics, for SGSN GPRS Tunnelling Protocol (SGTP) interface parameters, collected since the last restart or last use of a **clear** command.

### Product

SGSN  
PDG/TTG  
MME

### Privilege

Inspector

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show sgtpc statistics [ all | gsn-address ipv4_address | sgtp-service  
sgtp_srvc_name ] [ verbose ][ | { grep grep_options | more } ]
```

### all

Displays configuration information for all of the SGTP services defined for the current context.

**gsn-address *ipv4\_address***

Displays statistics for an SGSN specified by its IP address in IPv4 dotted-decimal notation. This must be an existing and active interface.

**sgtp-service *sgtp\_srvc\_name***

Displays statistics for an existing SGTP service specified as an alphanumeric string from 1 through 63 characters.

**verbose**

Causes the system to display more detailed level of statistics.

**{ *grep grep\_options* | *more* }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display information for SGSN services.

**Example**

The following command displays statistics for the SGTP service named *sgtp1*:

```
show sgtpc statistics sgtp-service sgtp1
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show sgtpu statistics

Displays all transmission and reception statistics for pre-defined and active GTP-U interfaces collected since the last restart or last use of a **clear** command.

**Product**

SGSN  
PDG/TTG

**Privilege**

Inspector

**Command Modes**

Exec  
The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show sgtpu statistics [ ggsn-address ipv4_address | gprs-service gprs_srvc_name  
nsei nse_id | iups-bind-address ipv4_address | iups-service iups_srvc_name |
```

```
recovered-values | rnc-address ipv4_address | sgtp-service sgtp_srvc_name ] [
| { grep grep_options | more } ]
```

#### **ggsn-address** *ipv4\_address*

Displays statistics for the GGSN specified by its IP address in IPv4 dotted-decimal notation.

#### **gprs-service** *gprs\_srvc\_name* **nsei** *nse\_id*

Displays NSEI-based GTPU statistics associated with an existing GPRS service specified as an alphanumeric string of 1 through 63 characters.

**nsei** *nse\_id*: Specifies a GPRS NSEI as an integer from 0 through 65535.

#### **iups-bind-address** *ipv4\_address*

Displays SGSN GPRS Tunnelling Protocol (SGTP) statistics for an Iu GTPU interface specified by its IP address in IPv4 dotted-decimal notation.

#### **iups-service** *iups\_srvc\_name*

Displays statistics for an existing IuPS service specified as an alphanumeric string of 1 through 63 characters.

#### **recovered-values**

Only displays recovered values for key KPI counters that were backed-up.

#### **rnc-address** *ipv4\_address*

Displays statistics for a Radio Network Controller (RNC) identified by its IP address in IPv4 dotted-decimal notation.

#### **sgtp-service** *sgtp\_srvc\_name*

Displays statistics for an existing SGTP service specified as an alphanumeric string of 1 through 63 characters.

#### | { **grep** *grep\_options* | **more** }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display statistics for the SGTPU interface.

### Example

The following command displays GTP-U statistics for the traffic between an SGSN and a connected RNC:

```
show sgtpu statistics rnc-address 123.1.2.3
```

# show sgw-service

Displays configuration settings and/or service statistics for Serving Gateway (S-GW) services on this system.

---

**Product**

S-GW  
SAEGW

---

**Privilege**

Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
show sgw-service { all | name service_name | statistics { all | name  
service_name [ rac rac | tac tac | apn apn_name ] } } [ | { grep grep_options |  
more } ]
```

**all**

Displays configuration information for all S-GW services configured on this system.

**name service\_name**

Displays configuration information for an existing S-GW service *c* specified as an alphanumeric string of 1 through 63 characters.

**statistics { all | name service\_name }**

**all**: Displays statistics for all S-GW services on this system or for a specified service.

**name service\_name**: Displays statistics for an existing S-GW service specified as an alphanumeric string of 1 through 63 characters.

**rac rac**

Specifies the Routing Area Code per 3GPP standards in TS 29.274. This will provide statistics for the SGW service associated with this **rac**.

This entry must be an integer from 0 to 65535.

There is no default setting.

**tac tac**

Specifies the Tracking Area Code per 3GPP standards in TS 29.274. This will provide statistics for the SGW service that is associated with this **tac**.

This entry must be an integer from 0 to 65535.

There is no default setting.

**apn *apn\_name***

Specifies a configured APN name that is associated with the specified SGW service.

This entry must be an alphanumeric string of 1 to 62 characters. This will provide statistics for the SGW service associated with this **apn**.

There is no default setting.

**| { *grep grep\_options* | *more* }**

Indicates the output of the command is to be piped (sent) to the command specified.

A command to send output to must be specified.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section in the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view configuration settings and/or service statistics for S-GW services on this system.

**Example**

The following command displays service statistics for the S-GW service named *sgw1*:

```
show sgw-service statistics name sgw1
```

# show sls-service

Displays information and statistics about SLs interface services configured on this system.

**Product**

MME

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show sls-service { all | name svc_name | peers [ all | esmlc-id esmlc-id ]
| statistics [ name svc_name [ sls | sctp ] ] [ sls | sctp ] [ esmlc-id esmlc-id
] } [ | { grep grep_options | more } ]
```

**all**

Displays information about all SLs interface services configured on this system.

**name *svc\_name***

Displays information about an existing SLs service specified as an alphanumeric string of 1 through 63 characters.

**peers [ all | esmlc-id *esmlc-id* ]**

Displays configuration information of the E-SMLC peers that are connected to the SLs service.

**all**: Displays statistics for all E-SMLC peers.

**esmlc-id *esmlc-id***: Displays statistics for an existing E-SMLC peer specified as an integer value from 0 through 255.

**statistics [ name *svc\_name* [ sls | sctp ] ] [ sls | sctp ] [ esmlc-id *esmlc-id* ]**

Displays all statistics for SLs services configured on this system.

**name *name***: Displays all statistics for an existing SLs service specified as an alphanumeric string of 1 through 63 characters.

**sls**: Filters output to show only SLs interface related statistics.

**sctp**: Filters output to show only SCTP related statistics.

**esmlc-id *esmlc-id***: Displays all statistics for an existing E-SMLC peer specified as an integer value from 0 through 255.

**{ *grep grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display information and statistics about SLs services configured on this system.

**Example**

The following command displays all statistics for an SLs service named *sls1*

```
show sls-service name sls1
```

## show sms statistics

Displays traffic statistics for the Short Message Service (SMS).

**Product**

SGSN

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show sms statistics [ gprs-only | name map_srvc | recovered-values |  
sgsn-only ] [ verbose ] [ | { grep grep_options | more } ]
```

**gprs-only**

Displays only GPRS access type SMS statistics.

**name *map\_srv***

Displays statistics for an existing MAP service specified as an alphanumeric string of 1 through 63 characters.

**recovered-values**

Only displays recovered values for key KPI counters that were backed-up.

**sgsn-only**

Displays only UMTS access type SMS statistics.

**verbose**

Causes the system to displays more detailed level of statistics.

**| { *grep* *grep\_options* | *more* }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display traffic statistics for the SMS services.

**Example**

Use the following command to display SMS statistics for 3G traffic:

```
show sms statistics sgsn-only
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show sndcp statistics

Displays statistics for the packet traffic going through the Subnetwork Dependent Convergence Protocol (SND CP) layer.

**Product**

SGSN

**Privilege**

Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:



```
[local]host_name#
```

---

**Syntax Description**

```
show sndcp statistics [ gprs-service svc_name ] [ verbose ] [ | { grep  
grep_options | more } ]
```

**gprs-service *svc\_name***

Displays statistics for an existing GPRS service specified as an alphanumeric string of 1 through 63 characters.

**verbose**

Displays a more detailed level of statistics.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Use this command to display SNDCP traffic statistics. Include the **gprs-service** keyword to filter the output to statistics for only one GPRS service.

**Example**

Use the following command to display all SNDCP layer traffic statistics:

```
show sndcp statistics verbose
```

Use the following command to display SNDCP layer traffic statistics for the *test1* GPRS service:

```
show sndcp statistics gprs-service test1
```




---

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show snmp

Displays information on the Simple Network Management Protocol (SNMP) servers and interfaces.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator, Operator, Inspector

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show snmp { accesses | communities | notifies | server | transports |
trap { history [ url | varbind | verbose ] | statistics [ verbose | wide
] } [ | { grep grep_options | more } ]
```

**accesses**

Displays SNMP server usage statistics.

**communities**

Displays SNMP community strings.

**notifies**

Displays SNMP event trap and notification statistics.

**server**

Displays SNMP server configuration information.

**transports**

Displays trap destination configuration information.

**trap { history [ url | varbind | verbose ] | statistics [ verbose | wide ] }**

**history**: Displays SNMP event trap history. **trap history** Displays up to 5,000 time-stamped trap records stored in a buffer. The buffer may be cleared by entering the **clear snmp history** command.

**statistics**: Displays SNMP event trap and notification statistics.

**url *pathname***: Redirects output to a file.

**varbind**: Displays varbind-based output which is easier to parse, but harder for an operator to read.

**verbose**: Displays rows for every defined trap, even if never generated.

**wide**: Displays trap statistical data in excess of 80 columns.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Display SNMP information as part of system verification and troubleshooting.

**Example**

The following commands display the usage statistics, community string information, event trap and notification data, server information, and trap destination configuration, respectively.

```
show snmp communities
show snmp transport
```

```
show snmp server
show snmp accesses
show snmp notifies
show snmp trap history
```



**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show software authenticity

Displays information regarding the authenticity of the software.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: [local]host_name#
<b>Syntax Description</b>	<b>show software authenticity { file <i>url</i>[ validate ]   keys   running } [   { grep <i>grep_options</i>   more } ]</b>

### file *url*[ validate ]

Displays authenticity information for a specified file.

*url* specifies the pathname for the file for which authentication information will be displayed as one of the following:

For the ASR 5500:

```
[file:]{/flash | /usb1 | /hd-raid | /sftp}{/directory}/ filename
```

```
tftp://host[:port] [/directory] /filename
```

```
ftp://[username[:password]@]host[:port] [/directory] /filename
```

```
sftp://[username[:password]@]host[:port] [/directory] /filename
```

```
http://[username[:password]@]host[:port] [/directory] /filename
```

*directory* is the directory name.

*filename* is the actual file of interest.

*username* is the user to be authenticated.

*password* is the password to use for authentication.

*host* is the IP address or host name of the server.

*port#* is the logical port number that the communication protocol is to use.

**file *url* [ validate ]**

Displays authenticity information for starfile images on flash or over the network. The **validate** option performs digital signature validation of the image.

**keys**

Displays public StarOS key information for each of the key storage regions (Primary, Backup), as well as Rollover key information.

**running**

Displays information about the chain of trust for all running software images: StarOS, CFE (bootstrap), BIOS/UEFI (Unified Extensible Firmware Interface) and the microloader.

**{ *grep grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Displays information regarding the authenticity of the software.

**Example**

The following commands display authenticity information for currently running BIOS, CFE and StarOS:

```
show software authenticity running
```

# show srp

Displays the Service Redundancy Protocol (SRP) information.

**Product**

All products that support Interchassis Session Recovery (ICSR)

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show srp { audit-statistics [ all | instance number ] [ message-level |
session-level ] | call-loss statistics | checkpoint { info | statistics
[ active | debug-info | standby ] [ verbose ] } | details | info | monitor
[ all | authentication-probe | bfd | bgp | diameter ] | statistics } |
[ grep grep_options | more ]
```

**audit-statistics [ all | instance *number* ] [ message-level | session-level ]**

Displays statistics of external audit.

**all:** Displays information for all Session Managers.

**instance *number*:** Displays information for an instance number of Session Manager specified as an integer from 1 through 4294967295.

**message-level:** Displays message-level statistics.

**session-level:** Displays session-level statistics.

**call-loss statistics**

Displays history of lost calls during switchover.

**checkpoint { info | statistics [ active | standby ] [ verbose ]**

The **info** keyword displays a list of micro-checkpoints by CMD ID, name along with associated status information.

The **statistics** keyword displays checkpointing statistics on session redundancy data (session managers, current call recovery records, etc.).

**active:** Displays information for the active chassis.

**standby:** Displays information for the standby chassis.

**verbose:** Displays cumulative information for all session managers in tabular output.

**details**

Displays detailed information and statistics required by TAC personnel for ICSR/SRP troubleshooting.

**info**

Displays Service Redundancy Protocol information (context, chassis state, peer, connection state, etc.).

**monitor [ all | authentication-probe | bfd | bgp | diameter ]**

Displays SRP monitor information.

**all:** Displays monitor information for all types (authentication-probe, bgp, and diameter).

**authentication-probe:** Displays authentication probe monitor information.

**bfd:** Displays BFD monitor information.

**bgp:** Displays BGP monitor information.

**diameter:** Displays Diameter monitor information.

**statistics**

Displays SRP statistics (hello messages sent, configuration validation, resource messages, switchovers, etc.).

**{ `grep` *grep\_options* | `more` }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

The output of this command may be considered as part of a periodic system auditing program by verifying the Service Redundancy Protocol performance. For more information, refer to the *Interchassis Session Recovery* appendix of the *System Administration Guide* and the *Service Redundancy Protocol Configuration Mode* chapter of this guide.

### Example

The following commands display Service Redundancy Protocol information:

```
show srp audit-statistics
show srp call-loss statistics
show srp checkpoint statistics
show srp info
show srp monitor
show srp statistics
```



### Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show ss7-routing-domain

This command displays the configuration information for the defined Signalling System #7 (SS7) routing domains. Since SS7 routing domains encompass a large number of operational parameters, this command enables you to narrow your displays to specific protocol parameters on a specific link.

### Product

SGSN

### Privilege

Security Administrator, Administrator, Inspector, Operator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show ss7-routing-domain { all | ss7rd_id { m3ua | mtp2 | mtp3 | qsaal |
routes [ adjacent ] | sctp asp { all | instance asp_id } | sscf } }
show ss7-routing-domain ss7rd_id m3ua { statistics { gen | peer-server {
all | id peer-server_id peer-server-process { all | instance psp_instance } }
} | status { address-translation-table | destination-point-code { all |
ss7_dpc } | gen | peer-server peer-server_id [ peer-server-process instance
psp_id | verbose ] }
```

```
show ss7-routing-domain 1 sscf { statistics linkset { all | id linkset_id  
link { all | id link_id } } | status linkset { all | id linkset_id link {  
all | id link_id [ verbose ] } } }
```

### **ss7-routing-domain { all | ss7rd\_id }**

**all:** Displays information for all SS7 routing domains.

*ss7rd\_id:* Displays information for the SS7 routing domain ID specified as an integer from 1 through 12.

### **m3ua**

Displays statistics and status information for the SS7 MTP3 User Adaptation Layer (M3UA) in the specified SS7 routing domain.

### **mtp2**

Displays statistics and status information for the SS7 Message Transfer Part-2 (MTP2) in the specified SS7 routing domain.

### **mtp3**

Displays statistics and status information for the SS7 Message Transfer Part-3 (MTP3) in the specified SS7 routing domain.

### **qsaal**

Displays statistics and status information for the Service Specific Connection-Oriented Protocol (SSCOP) sub-layer of the Quasi Signaling Application Adaptation Layer (QSAAL) in the specified SS7 routing domain.

### **routes [ adjacent ]**

Displays the destination point code (DPC) routing table.

**adjacent:** If this keyword is used with the **routes** keyword, access is provided to the statistics and status information for configured adjacent point codes.

### **sctp asp { all | instance asp\_id }**

Provides access to the status or statistics for the Stream Control Transmission Protocol (SCTP) application server processes (ASP) in the specified SS7 routing domain for all or a specified SCTP ASP instance.

- **all:** Displays the information for all SCTP application server process instances for a specific SS7 routing domain.
- **instance asp\_id:** Displays the information for an SCTP application server process instance specified as an integer from 1 through 4.

### **sscf**

Displays statistics and status information for the Service Specific Coordination Function (SSCF [q.2140]) in the specified SS7 routing domain.

**peer-server [ all | id *peer-server\_id* ]**

Filters the information for the specific protocol in the SS7 routing domain for all or a specific peer server ID.

- **all**: Displays the information for all peer servers for a specific protocol.
- **id *peer-server\_id***: Indicates the specific linkset identifier as an integer from 1 through 49.

**peer-server-process [ all | instance *instance\_id* ]**

Filters the information for the specific protocol in the SS7 routing domain for all or a specific instance of peer-server process.

- **all**: Displays the information for all peer server process instances for a specific protocol.
- **instance *instance\_id***: Specifies a peer server process instance as an integer from 1 through 4.

**destination-point-code [ all | *dest\_point\_code* ]**

Filters the information for the specific protocol in the SS7 routing domain for all or a specific DPC.

- **all**: Displays the information for all DPCs in the SS7 routing domain.
- ***dest\_point\_code***: Specifies a DPC in the SS7 routing domain.

**gen**

Displays general information for the specific protocol in the specified SS7 routing domain.

**verbose**

Enables the display of maximum information for a protocol.

**linkset [ all | id *linkset\_id* ]**

Filters the information for the specific protocol in SS7 routing domain for all or a specific link set.

- **all**: Displays the information for all linkset for a specific protocol.
- **id *linkset\_id***: Specifies a linkset identifier as an integer from 1 through 49.

**link [ all | id *link\_id* ]**

Filters the information for a specified protocol in the SS7 routing domain for all or a specific link set.

- **all**: Displays the information for all links for a specific protocol.
- **id *link\_id***: Specifies a linkset identifier as be an integer from 1 through 16.

**Usage Guidelines**

Use this command to display the SS7 routing domain and different layer protocol information for SGSN service.



**Example**

Displays the information/statistics for all SCTP application server processes of peer server ID 17 and peer server process instance 1 in SS7 routing domain 12:

```
show ss7-routing-domain 12 sctp asp all status peer-server id 17
peer-server-process instance 1
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show ssh

Displays the secure shell (SSH) host or client authentication public key information.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show ssh { client | key } [ type { v1-rsa | v2-rsa | v2-dsa } ]
```

**type { v1-rsa | v2-dsa | v2-rsa }**

Specifies the type of SSH key information to display. If type is not specified, information for all types is displayed.

**v1-rsa:** SSH v1 RSA host key only (obsolete)

**v2-dsa:** SSH v2 DSA host key only

**v2-rsa:** SSH v2 RSA host or client key only

**Usage Guidelines**

Displays the secure shell host or client key information to verify installed keys.

**Example**

The following command displays information for all SSH v1 and SSH v2 host keys:

```
show ssh key
```

The following command shows information for SSH client v2 RSA host keys:

```
show ssh client key type v2-rsa
```

## show ssl cipher-suite

Displays information related to Secure Sockets Layer (SSL) cipher suites since the last restart or **clear** command. A cipher suite contains the cryptographic algorithms supported by the client.

---

### Product

SCM (P-CSCF, A-BG)  
SecGW

---

### Privilege

Security Administrator, Administrator, Inspector, Operator

---

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

### Syntax Description

```
show ssl cipher-suite [ name name ] [ | { grep grep_options | more } ]
```

#### **name** *name*

Displays information related to the SSL cipher suite specified as an alphanumeric string of 1 through 127 characters.

#### | { **grep** *grep\_options* | **more** }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

### Usage Guidelines

Use this command to display information related to SSL cipher suites.

#### Example

The following command displays information for the SSL cipher suite *ssl\_cipher\_suite\_1*:

```
show ssl cipher-suite name ssl_cipher_suite_1
```

## show ssl connection

Displays information pertaining to Secure Sockets Layer (SSL) connections on the Proxy Call Session Control Function (P-CSCF).

---

### Product

SCM (P-CSCF, A-BG)  
SecGW

---

### Privilege

Security Administrator, Administrator, Inspector, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show ssl connection [ list | summary [ service-name name ] ] [ name name ]
[ | { grep grep_options | more } ]
```

**list**

Lists the SSL connections on the P-CSCF.

**summary**

Displays state and statistical information for the SSL connections on the P-CSCF.

**service-name *name***

Lists the SSL connections on the P-CSCF for the specified P-CSCF service, or displays state and statistical information for the SSL connections on the P-CSCF for the specified P-CSCF service.

*name* must be an alphanumeric string of 1 through 63 characters.

**name *name***

Displays state and statistical information for the SSL connection specified as an alphanumeric string of 1 through 127 characters.

**{ **grep** *grep\_options* | **more** }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command in Exec Mode to display information and statistics pertaining to SSL connections.

If the **summary** keyword is not used, detailed information is displayed.

**Example**

The following command displays SSL connection information for the P-CSCF service *pcscf\_tls\_1*:

```
show ssl connection list service-name pcscf_tls_1
```

## show ssl map

Displays information related to configured Secure Sockets Layer (SSL) maps/templates since the last restart or **clear** command.

**Product**

SCM (P-CSCF, A-BG)

SecGW

---

**Privilege**

Security Administrator, Administrator, Inspector, Operator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description**

```
show ssl map [ map-type ssl-subscriber-template ] [ name name ] [ | { grep
grep_options | more } ]
```

**map-type ssl-subscriber-template**

Displays information related to configured SSL maps/templates for the SSL map/template type `ssl-subscriber-template`.

**name *name***

Displays information related to configured SSL maps/templates for the map/template name specified as an alphanumeric string of 1 through 127 characters.

**{ **grep** *grep\_options* | **more** }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Use this command to display information related to configured SSL maps/templates.

**Example**

The following command displays information related to configured SSL maps/templates for the SSL map/template `ssl_template_1`:

```
show ssl map name ssl_template_1
```

## show ssl statistics

Displays statistics for Secure Sockets Layer (SSL) since the last restart or **clear** command.

---

**Product**

SCM (P-CSCF, A-BG)

SecGW

---

**Privilege**

Security Administrator, Administrator, Inspector, Operator

---

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show ssl statistics [ service-name name ] [ | { grep grep_options | more } ]`

**service-name *name***

Displays SSL statistics for the Proxy Call Session Control Function (P-CSCF) service, specified as an alphanumeric string of 1 through 127 characters.

**{ **grep** *grep\_options* | **more** }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines** Use this command to display SSL statistics.

**Example**

The following command displays SSL statistics for all P-CSCF services:

```
show ssl statistics
```

## show subscribers

Displays information for subscriber sessions that are defined by specified keywords. Command keywords are base commands that display distinctive types of data. Filter keywords are a superset of command keywords that modify or filter the output of the base commands.




---

**Important**

Not all filter keywords are available for all command keywords. CLI Help displays available filter keywords based on: the platform type (ASR 5000 or ASR 5500), the products that are licensed to run on the platform, and the preceding command keyword and subsequent filter keywords.

---



---

**Product** All

---

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

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show subscribers [ command_keyword ] [ filter_keywords ] [ | { grep grep_options | more } ]`

**command\_keyword**

The following keywords are base commands that each have a distinct display output. Only one command keyword can be entered on the command line.

**aaa-configuration**

Displays Authentication Authorization and Accounting (AAA) configuration information for subscriber sessions defined by the specified filter keywords. The following filter keywords are valid with this command:

active, active-charging -service, all, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, dormant, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-access-service, hnbgw-only, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-address, l3-tunnel-remote-address, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, nemo-only network-requested, network-type, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, tx-data, username, verbose, grep, more

**access-flows { accounting | dynamic | pre-provisioned | static }**

Shows the ip-flows for the subscribers defined by the specified filter keywords.

- **accounting**: displays the accounting type of access flows for a subscriber.
- **dynamic**: displays the dynamic type of access flows for a subscriber.
- **pre-provisioned**: displays the pre-provisioned type of access flows for a WiMAX subscriber.
- **static**: displays the static type of access flows for a subscriber.

The following filter keywords are valid with this command:

active, active-charging-service, all, apn, asn-peer-address, asngw-service, asnpc-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, dormant, epdg-address, epdg-service, fa, fa-service, flow-type, ggsn-service, gprs-service, gsm-traffic-class, ha, ha-ipsec-only, ha-service, hnbgw-access-service, hnbgw-only, hsgw-service, idle-time, imsi, ip-address, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-address, l3-tunnel-remote-address, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mme-address, mme-service, msid, msisd, network-requested, network-type, pcf, pdg-service, pdif-service, pdsn-service, pdsnclosedrps-service, pgw-address, plmn-type, rulebase, rx-data, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, tpo, tx-data, username, verbose, grep, more

**access-type { lxcdma | ehrpd | lte | undetermined | wcdma | wifi | wired }**

Displays active subscribers using a specific type of UE.

- **lxcdma**: 1XCDMA – Wireless CDMA 1x high speed internet service
- **ehrpdp**: eHRPD – Enhanced High Rate Packet Data
- **evdo**: EvDO – EVolution-Data Optimized
- **lte**: LTE – Long Term Evolution
- **undetermined**
- **wcdma**: WCDMA – Wideband Code Division Multiple Access

- **wifi**: WiFi – Wireless local area network
- **wired**

The following filter keywords are valid with this command:

access-type, bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, domain, ebi, enodeb-address, fa, firewall, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, hnbgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, nat, network-type, profile-id, profile-name, qci, rx-data, slu-state, security-type, session-time-left, sgw-address, smgr-instance, tx-data, ue-type, username, grep, more

### active

Displays active subscribers. When no Filter Keywords are specified, the output is a summary of all active subscribers. When Filter Keywords are specified, the percentage is displayed as graphs in which one is displayed using a high sampling rate, a 10-second interval between samples, and a low sampling rate, a 15-minute interval between samples.

The following filter keywords are valid with this command:

apn, asn-peer-address, asngw-service, asnpc-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-access-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, pcf, pdg-service, pdif-service, pdsn-service, pdsnclosedrp-service, pgw-address, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, session-time-left, sgsn-address, sgsn-service, smgr-instance, sgw-address, sgw-service, tpo, tx-data, username, grep, more

### active-charging-service *acs\_service*

Displays information for subscribers being processed by the active charging service specified as an alphanumeric string of 1 through 15 characters.

The following filter keywords are valid with this command:

active-charging-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, configured-idle-timeout, connected-time, ebi, enodeb-address, epdg-address, epdg-service, fa, firewall, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, idle-time, ims-auth-service, imsi, ip-address, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-address, l3-tunnel-remote-address, long-duration-time-left, mag-service, mipv6ha-service, msid, nat, network-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, session-time-left, sgw-address, smgr-instance, tx-data, username, grep, more

### activity

Displays subscriber link activity percentage. When no Filter Keywords are specified, the output is a summary of all subscriber activity. When Filter Keywords are specified, the link activity percentage is displayed as graphs in which one is displayed using a high sampling rate, a 10-second interval between samples, and a low sampling rate, a 15-minute interval between samples.

The following filter keywords are valid with this command:

active, all, apn, asn-peer-address, asngw-service, asnpc-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, dormant, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service,

firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, henbgw-access-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mme-address, mme-service, msid, msisd, nat, nemo-only, network-requested, pcf, pdg-service, pdif-service, pdsn-service, pdsnclosedrp-service, pgw-address, plmn-type, profile-id, profile-name, qci, rx-data, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tpo, tx-data, username, grep, more

### **all *ip\_address***

Displays all current subscribers who have either active or dormant sessions.

### **apn *apn\_string***

Displays subscribers currently facilitated by the Access Point name (APN) configured on the SGSN or GGSN.

The following filter keywords are valid with this command:

active-charging-service, apn, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, coa-only, configured-idle-timeout, connected-time, dhcp-server, dormant, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-address, l3-tunnel-remote-address, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, msid, nat, nemo-only, network-requested, network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rulename <rule\_name>, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgsn-service, sgw-address, smgr-instance, without-dynamic-rule, without-override-control, tx-data, username, verbose, grep, more

### **asn-peer-address *ip\_address***

Displays information for subscribers on an ASN-GW trusted peer.

*ip\_address* is the IP address of the ASN-GW peer server expressed in IPv4 dotted-decimal notation.

The following filter keywords are valid with this command:

asn-peer-address, asngw-service, bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, connected-time, ebi, enodeb-address, fa, fa-service, firewall, full, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-address, l3-tunnel-remote-address, long-duration-time-left, mipv6ha-service, msid, nat, network-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgw-address, smgr-instance, tx-data, username, grep, more

### **asngw-only *service\_name***

Displays ASN-GW specific context information for the session.

The following filter keywords are valid with this command:

aaa-configuration, access-flows, active, activity, all, asn-peer-address, asngw-service, bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, connected-time, counters, data-rate, dormant, ebi, enodeb-address, fa, fa-service, firewall, full, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-address, l3-tunnel-remote-address, long-duration-time-left, mipv6ha-service, msid, nat, network-type, policy, profile-id, profile-name, qci, rx-data, slu-state, s5-proto,



session-time-left, sgw-address, smgr-instance, subscription, summary, tft, tx-data, username, wfl, grep, more

### **asn-gw-service *service\_name***

Displays counters for subscribers accessing the ASN-GW service.

*service\_name* must be an existing service and be from 1 to 63 alphanumeric characters.

The following filter keywords are valid with this command:

asn-peer-address, asngw-service, bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, connected-time, ebi, enodeb-address, fa, fa-service, firewall, full, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-address, l3-tunnel-remote-address, long-duration-time-left, mipv6ha-service, msid, nat, network-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgw-address, smgr-instance, tx-data, username, grep, more

### **asn-pc-service *service\_name***

Displays counters for subscribers accessing the ASN Paging Controller and Location Registry service.

*service\_name* must be an existing Access Service Network Paging Controller (ASN PC) service and be from 1 to 63 alphanumeric characters.

The following filter keywords are valid with this command:

all, counters all, full, summary, grep, more

### **bandwidth-policy *policy\_name***

Show information for subscribers associated with the specified Active Charging bandwidth policy. Must be followed by the name of an existing bandwidth policy specified as an alphanumeric string of 1 through 63 characters.

The following filter keywords are valid with this command:

access-type, active-charging-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, configured-idle-timeout, connected-time, domain, ebi, enodeb-address, epdg-address, epdg-service, fa, firewall, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, hnbgw-service, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lma-service, long-duration-time-left, mag-service, mipv6ha-service, msid, nat, network-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, security-type, session-time-left, sgw-address, smgr-instance, tx-data, ue-type, username, grep, more

### **bearer-establishment { *direct-tunnel* | *normal* | *pending* }**

Selects Bearer Establishment type defined by the specified filter keywords.

- **direct-tunnel**: Select subscribers having direct tunnel established with the Radio Network Controller (RNC).
- **normal**: Select subscribers having bearer established with SGSN.
- **pending**: Select subscribers for whom bearer is not fully established.

The following filter keywords are valid with this command:

apn, asn-peer-address, asngw-service, asnpc-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, css-delivery-sequence, css-service, dhcp-server, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, henbgw-access-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdg-service, pdif-service, pdsn-service, pdsnclosedrpservice, pgw-address, plmn-type, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tx-data, username, grep, more

### **bng-service *svrc\_name***

Displays current configuration the specified Broadband Network Gateway (BNG) service. The following filter keywords are valid with this command:

active, all, apn, asn-peer-address, asngw-service, asnpc-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, dormant, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, henbgw-access-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, pcf, pdg-service, pdif-service, pdsn-service, pdsnclosedrpservice, pgw-address, plmn-type, profile-id, profile-name, qci, rx-data, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tpo, tx-data, username, grep, more

### **callid *id***

Displays subscriber information for the call ID specified as an 8-byte hexadecimal number.

The following filter keywords are valid with this command:

adc, apn, asn-peer-address, asngw-service, asnpc-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, css-delivery-sequence, css-service, dhcp-server, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, henbgw-access-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdg-service, pdif-service, pdsn-service, pdsnclosedrpservice, pgw-address, plmn-type, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tx-data, username, grep, more

### **card-num *card\_num***

The slot number of the processing card by which the subscriber session is processed. The slot number is an integer from 1 through 7 and 10 through 16 on the ASR 5000, or 1 through 4 and 7 through 10 on the ASR 5500.

The following filter keywords are valid with this command:

apn, asn-peer-address, asngw-service, asnpc-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, cpu-num, css-delivery-sequence, css-service, dhcp-server, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only,

ha-service, hnbgw-access-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisd, nat, nemo-only, network-requested, network-type, pcf, pdg-service, pdif-service, pdsn-service, pdsnclosedrps-service, pgw-address, plmn-type, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tx-data, username, grep, more

### **cbb-policy *policy\_name***

Show information for subscribers associated with the specified Active Charging Content Based Billing (CBB) policy. Must be followed by the name of an existing Active Charging CBB policy specified as an alphanumeric string of 1 through 63 characters.

The following filter keywords are valid with this command:

active, active-charging -service, all, apn, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, coa-only, configured-idle-timeout, connected-time, dhcp-server, dormant, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-only, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-address, l3-tunnel-remote-address, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, msid, nemo-only, network-requested, network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgsn-service, tx-data, username, verbose, grep, more

### **coa-only**

Displays current configuration for all MIP-HA subscribers that registered with a collocated COA only. The following filter keywords are valid with this command:

access-type, active-charging-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, configured-idle-timeout, connected-time, domain, ebi, enodeb-address, epdg-address, epdg-service, fa, firewall, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, hnbgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, nat, network-type, pcc-service, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, smgr-instance, tpo, tx-data, username, grep, more

### **configuration { all | username *name* }**

Displays current configuration for all subscribers or a specified subscriber.

### **configured-idle-timeout [ < | > | greater-than | less-than ] *value***

Shows the idle timeout that is configured for the specified subscriber. A value of 0 (zero) indicates that the subscribers idle timeout is disabled.

- <: Filters output so that only information less than the specified value is displayed.
- >: Filters output so that only information greater than the specified value is displayed.
- **greater-than**: Filters output so that only information greater than the specified value is displayed.
- **less-than**: Filters output so that only information less than the specified value is displayed.

- *value*: Used in conjunction with <, >, greater-than, less-than, If no other filtering options are specified only output matching *value* is displayed. If *value* is not specified all data is displayed. *value* must be an integer from 0 through 4294967295.

### **congestion\_mgmt { not-required | required }**

Shows the current subscribers for which congestion management is **not-required** or **required**. The following filter keywords are valid with this command:

active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, configured-idle-timeout, congestion\_mgmt, connected-time, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-service, hnbgw-access-service, hsgw-service, idle-time, ims-auth-service, imsi, interface-type, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mipv6ha-service, mme-address, mme-service, msid, nat, network-type, pcp, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, saegw-service, session-time-left, sgw-address, sgw-service, smgr-instance, tpo, tx-data, username, wsg-service

### **connected-time [ < | > | greater-than | less-than ] value**

Shows how long the subscriber has been connected.

- <: Filters output so that only information less than the specified value is displayed.
- <=: Filters output so that only information less than the specified value is displayed.
- >: Filters output so that only information greater than the specified value is displayed.
- **greater-than**: Filters output so that only information greater than the specified value is displayed.
- **less-than**: Filters output so that only information less than the specified value is displayed.
- *value*: Used in conjunction with <, >, greater-than, less-than, If no other filtering options are specified only output matching *value* is displayed. If *value* is not specified all data is displayed. *value* must be an integer from 0 through 4294967295.

### **counters**

Shows the counters associated with the subscriber. The following filter keywords are valid with this command:

access-type, active, active-charging-service, all, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, dns-proxy, domain, dormant, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-access-service, hnbgw-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mipv6ha-service, mme-address, mme-service, msid, msisd, nat, nemo-only, network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pdsnclosedrp-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tpo, tx-data, ue-type, username, grep, more

### css-delivery-sequence

**Important**

This is a restricted keyword. In StarOS 9.0 and later, this keyword is obsoleted.

### css-service *csssvc\_name*

**Important**

This is a restricted keyword. In StarOS 9.0 and later releases, this keyword is obsolete.

### data-rate

Displays subscriber throughput data. **This keyword is best used for individual subscriber output.**

The following filter keywords are valid with this command:

access-type, active, active-charging-service, all, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, dormant, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, graph, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hcnbgw-access-service, high, hnbgw-service, hsgw-only, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, low, mag-service, mipv6ha-service, mme-address, mme-service, msid, msisd, network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pdsnclosedrp-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, summary, tpo, tx-data, ue-type, username, verbose, grep, more

### debug-info { callid *id* | msid *id* | username *name* }

Displays internal call troubleshooting information for subscriber sessions defined by the specified keywords.

- **callid *id***: Displays subscriber information for the call specified by *id*. The call ID must be specified as an 8-digit hexadecimal number.
- **msid *id***: Displays information for the mobile user identified by *id*. *id* must be from 7 to 16 digits specified as an IMSI, MIN, or RMI. Wildcard characters \$ and \* are allowed. The \* wildcard matches multiple characters and the \$ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes ( '). For example; '\$'.
- **username *name***: Displays information for connections for the subscriber identified by *name*. The user must have been previously configured. *name* must be a sequence of characters and/or wildcard characters ('\$ and '\*') from 1 to 127 characters. The \* wildcard matches multiple characters and the \$ wildcard matches a single character. If you do not want the wildcard characters interpreted as wildcard enclose them in single quotes ( '). For example; '\$'.

### dhcp-server *ipv4\_address*

Displays subscribers based on a specific DHCP server where their IP address was allocated. Must be followed by IP address of the server, using IPv4 dotted-decimal notation.

The following filter keywords are valid with this command:

apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, msid, msisdn, nat, nemo-only, network-requested, pcf, pdsn-service, pdsnclosedrp-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, session-time-left, sgsn-address, sgsn-service, smgr-instance, tpo, tx-data, username, grep, more

### **domain name**

Displays all subscribers with an Address-of-Record (AoR) from the specified domain. *name* is an alphanumeric string of 1 through 79 characters.

The following filter keywords are valid with this command:

access-type, active-charging-service, all, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, configured-idle-timeout, connected-time, dhcp-server, domain, ebi, enodeb-address, fa, firewall, fw-and-nat, ggsn-service, graph, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, hnbgw-service, hsgw-only, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, network-type, pcc-service, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgw-address, smgr-instance, summary, tpo, tx-data, ue-type, username, grep, more

### **dormant number**

Displays all dormant subscribers, those registered but not transmitting/receiving data.

The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-access-service, hnbgw-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pdsnclosedrp-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tpo, tx-data, ue-type, username, grep, more

### **ebi number**

Displays subscribers based on an EPS bearer identity. *number* specifies the EBI number and must be an integer value from 5 to 15.

The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, ebi, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only,

ha-service, hcnbgw-access-service, hcnbgw-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgw-address, sgw-service, smgr-instance, tx-data, ue-type, username, grep, more

### **enodeb-address *ip\_address***

Displays subscribers based on the eNodeB to which they are attached. *ip\_address* must be a valid IP address of an existing eNodeB specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hcnbgw-access-service, hcnbgw-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgw-address, sgw-service, smgr-instance, tx-data, ue-type, username, grep, more

### **epdg-address *ipv4\_ipv6\_address***

Displays subscribers connected to the specified ePDG peer specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

The following filter keywords are valid with this command:

apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hcnbgw-access-service, idle-time, imei, ims-auth-service, imsi, interface-type, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tpo, tx-data, username, wsg-service, grep, more

### **fa *ipv4\_address***

Displays subscribers for a specified Peer Foreign Agent. Must be followed by the IP address of a Remote FA, in IPv4 dotted-decimal notation.

The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hcnbgw-access-service, hcnbgw-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix,

l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pdsnclosedrpservice, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tpo, tx-data, ue-type, username, grep, more

### **epdg-only**

Displays epdg-specific context information for the session.

The following filter keywords are valid with this command:

all, callid, card-num, configured-idle-timeout, connected-time, counters, data-rate, full, gtp-version, gtpu-bind-address, gtpu-service, idle-time, ip-address, ipv6-prefix, long-duration-time-left, network-type, qci, rx-data, session-time-left, smgr-instance, summary, tft, tx-data, username, grep, more

### **epdg-service *svrc\_name***

Displays subscribers for a specified Evolved Packet Data Gateway service. Must be followed by ePDG service name expressed as an alphanumeric string of 1 through 63 characters.

The following filter keywords are valid with this command:

all, callid, card-num, configured-idle-timeout, connected-time, counters, data-rate, epdg-address, epdg-service, full, gtp-version, gtpu-bind-address, gtpu-service, idle-time, ip-address, ipv6-prefix, long-duration-time-left, network-type, qci, rx-data, session-time-left, smgr-instance, summary, tft, tx-data, username, grep, more

### **fa-only**

Displays FA-specific context information for the session.

The following filter keywords are valid with this command:

aaa-configuration, access-flows, active, activity, all, asn-peer-address, asngw-service, asnpc-service, bearer-establishment, callid, card-num, configured-idle-timeout, connected-time, counters, data-rate, dhcp-server, dormant, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, full, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdif-service, pdsn-service, pgw-address, plmn-type, policy, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgw-address, sgw-service, smgr-instance, subscription, summary, tft, tx-data, username, wfl, grep, more

### **fa-service *svrc\_name***

Displays subscribers for a specified Foreign Agent service. Must be followed by FA service name expressed as an alphanumeric string of 1 through 63 characters.

The following filter keywords are valid with this command:

aaa-configuration, access-flows, active, activity, all, asn-peer-address, asngw-service, asnpc-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configuration, configured-idle-timeout, connected-time, counters, data-rate, debug-info, dhcp-server, dormant, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-only, fa-service, firewall, full, fw-and-nat, ggsn-only, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, henbgw-access-service, idle-time, imei,



ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-only, lac-service, lns, lns-only, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdif-service, pdsn-service, pgw-address, plmn-type, policy, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgw-address, sgw-service, smgr-instance, subscription, summary, tft, tx-data, username, wfl, grep, more

### firewall { not-required | required }

Displays information for subscribers based on whether or not firewall processing is required.

The following filter keywords are valid with this command:

apn, asn-peer-address, asngw-service, asnpc-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, henbgw-access-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv4, ipv6, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdg-service, pdif-service, pdsn-service, pdsnclosedrp-service, pgw-address, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tpo, tx-data, username, grep, more

### fng-only

Displays Femto Network Gateway (FNG) context information for the session.

The following filter keywords are valid with this command:

aaa-configuration, access-flows, active, activity, all, bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, connected-time, counters, data-rate, dormant, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fng-service, full, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, henbgw-access-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, nat, network-type, pdif-service, policy, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgw-address, smgr-instance, subscription, summary, tft, tx-data, username, wfl, grep, more

### fng-service *svrc\_name*

Displays information for subscribers accessing the specified FNG service.

*service\_name* must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

The following filter keywords are valid with this command:

bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, connected-time, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fng-service, full, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, henbgw-access-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, nat, network-type, pdif-service, profile-id, profile-name, qci, rx-data, session-time-left, sgw-address, smgr-instance, subscription, summary, tft, tx-data, username, grep, more

### full

Shows all available subscriber information. The following filter keywords are valid with this command:

access-type, active, active-charging-service, all, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, dormant, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, henbgw-access-service, henbgw-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pdsnclosedrps-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, sl-proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tpo, tx-data, ue-type, username, grep, more

### fw-and-nat policy *fw\_nat\_policy*



#### Important

This option is customer-specific and is only available in StarOS 8.1.

Displays information for subscribers using an existing Firewall-and-NAT policy specified as an alphanumeric string of 1 through 15 characters.

### ggsn-only

Displays only GGSN-specific subscriber context information.

The following filter keywords are valid with this command:

aaa-configuration, access-flows, active, activity, all, apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, counters, data-rate, dhcp-server, dormant, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, full, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-only, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdsn-service, plmn-type, policy, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance, subscription, summary, tft, tx-data, username, wfl, grep, more

### ggsn-service *svc\_name*

Displays only subscribers for a specified GGSN service. Must be followed by the GGSN service name expressed as an alphanumeric string of 1 through 63 characters.

The following filter keywords are valid with this command:

apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, dormant, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username, grep, more

**gsm-traffic-class { background | conversational | interactive }**

Displays subscribers associate with the specified 3GPP QoS traffic class.

The following filter keywords are valid with this keyword:

```
apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout,
connected-time, dhcp-server, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service,
firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address,
gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi,
ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr,
l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left,
mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested,
network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state,
s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username,
grep, more
```

**gprs-only**

This keyword is specific to the SGSN and only displays 2G SGSN subscriber information.

The following filter keywords are valid with this keyword:

```
aaa-configuration, active, active-charging-service, activity, all, apn, callid, card-num,
configured-idle-timeout, connected-time, counters, data-rate, full, ggsn-address,
gprs-service, gsm-traffic-class, idle-time, imsi, msid, msisdn, partial, plmn-type,
profile-name, rx-data, session-time-left, summary, tx-data, wide-format, grep, more
```

**gprs-service *svc\_name***

Enter the name of the configured 2G GPRS service to display subscriber information specific to the named GPRS service for the SGSN.

*svc\_name* must be an alphanumeric string of 1 through 63 characters that identifies a configured GPRS service.

The following filter keywords are valid with this command:

```
apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout,
connected-time, dhcp-server, dormant, ebi, enodeb-address, epdg-address, epdg-service, fa,
fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version,
gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ip-address,
ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr,
l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left,
mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested,
network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state,
s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username,
grep, more
```

**gsm-traffic-class { background | conversational | interactive | streaming }**

Displays information for subscriber traffic that matches the specified 3GPP traffic class.

- **background**: 3GPP QoS background class.
- **conversational**: 3GPP QoS conversational class.
- **interactive**: 3GPP QoS interactive class. Must be followed by a traffic priority.
- **streaming**: 3GPP QoS streaming class.

The following filter keywords are valid with this command:

apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgsn-service, sgw-address, smgr-instance, tx-data, username, grep, more

### **gtp-version { 0 | 1 }**

Displays the specific GTP version number. Must be followed by one of the supported GTP versions (0 or 1).

The following filter keywords are valid with this command:

apn, bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, connected-time, ebi, enodeb-address, epdg-address, epdg-service, fa, firewall, fw-and-nat, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, hcnbgw-access-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mag-service, mipv6ha-service, msid, msisdn, nat, network-type, nri, nsei, pdg-service, pdif-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-service, sgw-address, smgr-instance, tx-data, username, grep, more

### **gtpu-bind-address *ipv4\_address***

Displays the subscribers associated with the specified GTPU service bind address. Must be followed by an IPv4 address in dotted decimal notation.

The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hcnbgw-access-service, hcnbgw-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgw-address, sgw-service, smgr-instance, tx-data, ue-type, username, grep, more

### **gtpu-service *svc\_name***

Displays the subscribers associated with an existing GTPU service specified as an alphanumeric string of 1 through 63 characters.

The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hcnbgw-access-service, hcnbgw-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix,

l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgw-address, sgw-service, smgr-instance, tx-data, ue-type, username, grep, more

### **ha ipv4\_address**

Displays the subscribers associated with the specified Peer Home Agent. Must be followed by the IP address of a Remote HA in IPv4 dotted-decimal notation.

The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-access-service, hnbgw-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-services, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgw-address, sgw-service, smgr-instance, tx-data, ue-type, username, grep, more

### **ha-ipsec-only**

Displays MIPHA subscribers with subscriber IPsec tunnel only.

The following filter keywords are valid with this command:

apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username, grep, more

### **ha-service svc\_name**

Displays the subscribers associated with an existing Home Agent service specified as an alphanumeric string of 1 through 63 characters.

The following filter keywords are valid with this command:

apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state,

s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username, grep, more

### **hcnbgw-access-servicesvc\_name**

Displays specific configured HCNBGW access service information. This must be followed by HCNBGW access service name.

The following filters/keywords are valid with this command:

bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, congestion\_mgmt, connected-time, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fng-service, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, hcnbgw-access-service, hcnbgw-service, idle-time, ims-auth-service, imsi, interface-type, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, nat, network-type, pcp, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, smgr-instance, tx-data, username, grep, more

### **hcnbgw-only**

Displays specific HCNBGW information for the session.

The following filters/keywords are valid with this command:

aaa-configuration, access-flows, active, activity, all, bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, congestion\_mgmt, connected-time, counters, data-rate, dormant, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fng-service, full, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, hcnbgw-access-service, hcnbgw-service, idle-time, ims-auth-service, imsi, interface-type, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, nat, network-type, pcp, policy, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, smgr-instance, subscription, summary, tft, tx-data, username, wfl, grep, more

### **hcnbgw-only**

Displays HCNBGW subscriber session information.

The following filters/keywords are valid with this command:

aaa-configuration, access-flows, access-type, active, active-charging-service, activity, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, configured-idle-timeout, connected-time, counters, data-rate, domain, ebi, enodeb-address, epdg-address, epdg-service, fa, firewall, full, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, hcnbgw-access-service, hcnbgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, nat, network-type, pcc-service, policy, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, smgr-instance, subscription, summary, tpo, tx-data, ue-type, username, wfl, grep, more

### **hcnbgw-service svc\_name**

Displays subscriber information based on the HCNBGW service name.

*svc\_name* must be an existing HCNBGW service expressed as an alphanumeric string of 1 through 63 characters.

The following filters/keywords are valid with this command:

access-type, active-charging-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, configured-idle-timeout, connected-time, domain, ebi, enodeb-address, epdg-address, epdg-service, fa, firewall, full, fw-and-nat, gtp-version,

gtpu-bind-address, gtpu-service, ha, hcnbgw-access-service, hcnbgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, nat, network-type, pcc-service, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, smgr-instance, tpo, tx-data, ue-type, username, grep, more

### **hsgw-only**

Displays HSGW subscriber session information.

The following filters/keywords are valid with this command:

aaa-configuration, access-flows, active, active-charging-only, all, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, configured-idle-timeout, connected-time, counters, data-rate, dormant, ebi, enodeb-address, epdg-address, epdg-service, fa, firewall, full, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mag-service, mipv6ha-service, msid, nat, network-type, pgw-address, policy, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, session-time-left, sgw-address, smgr-instance, subscription, summary, tft, tx-data, username, wfl, grep, more

**hsgw-service** *svc\_name*: Displays subscriber information based on the HSGW service name. *svc\_name* must be an existing HSGW service expressed as an alphanumeric string of 1 through 63 characters.

### **hsgw-service *svc\_name***

Displays subscriber information based on the HSGW service name. *svc\_name* must be an existing HSGW service expressed as an alphanumeric string of 1 through 63 characters.

The following filters/keywords are valid with this command:

active-charging-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, configured-idle-timeout, connected-time, ebi, enodeb-address, epdg-address, epdg-service, fa, firewall, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mag-service, mipv6ha-service, msid, nat, network-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, session-time-left, sgw-address, smgr-instance, tx-data, username, grep, more

### **idle-time**

Displays current configuration for all subscribers within the specified idle-time interval.

- <: Filters output so that only information less than the specified value is displayed.
- <: Filters output so that only information less than the specified value is displayed.
- >: Filters output so that only information greater than the specified value is displayed.
- **greater-than**: Filters output so that only information greater than the specified value is displayed.
- **less-than**: Filters output so that only information less than the specified value is displayed.
- *value*: Used in conjunction with <, >, greater-than, less-than, If no other filtering options are specified only output matching *value* is displayed. If *value* is not specified all data is displayed. *value* must be an integer from 0 through 4294967295.

The following filter keywords are valid with this command:

epdg-address, epdg-service

### **imei *imei\_number***

Displays subscribers having the specified International Mobile Equipment Identity (IMEI/IMEISV) Number. Must be followed by IMEI number.

The following filter keywords are valid with this command:

apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisd, nat, nemo-only, network-requested, network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username, grep, more

### **ims\_auth-service *svc\_name***

Displays subscriber information based on the IMS authentication service name. *svc\_name* must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

The following filters/keywords are valid with this command:

access-type, active-charging-service, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, gprs-service, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec, ha-service, hnbgw-access-service, hnbgw-service, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-up-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisd, nat, nemo-only, network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tpo, tx-data, ue-type, username, grep, more

### **imsi *imsi***

Displays information specific to one subscriber or group of subscribers. Enter 1 to 15 digits to identify a specific subscriber's IMSI (International Mobile Subscriber Identity).

The following filters/keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-access-service, hnbgw-service, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-services, mip-up-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisd, nat, nemo-only, network-requested, network-type, nsapi, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tpo, tx-data, ue-type, username, grep, more



**interface-type { S2aGTP | S2bGTP | S5S8GTP }**

Specifies subscriber type as either **S2a** (eHRPD), **S2b** (ePDG) or **S5/S8** (PMIPv6/GTP).

The following filter keywords are valid with this command:

apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, congestion\_mgmt, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-access-service, idle-time, imei, ims-auth-service, imsi, interface-type, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pcp, pdsn-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username, wsg-service, grep, more

**ip-address *ipv4\_address***

Displays the subscribers associated with the specified IPv4 address. Must be followed by the IP address in IPv4 dotted-decimal notation.

The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-access-service, hnbgw-service, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-up-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, nsapi, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tpo, tx-data, ue-type, username, grep, more

**ip-alloc-method {aaa-assigned | dhcp [ relay-agent | proxy-client ] | dynamic-pool | l2tp-lns-assigned | mip-ha-assigned | ms-provided-static | not-ms-provided-static | static pool }**

Displays the specific IP Allocation Method. Must be followed by one of the IP Allocation Methods:

- **aaa-assigned**: Selects subscribers whose IP addresses were assigned by AAA.
- **dhcp**: Selects subscribers whose IP addresses were assigned by DHCP.
  - **relay-agent**: Selects subscribers whose IP addresses were assigned by the DHCP Relay Agent
  - **proxy-client**: Selects subscribers whose IP addresses were assigned by the DHCP Proxy Client
- **dynamic-pool**: Selects subscribers whose IP addresses were assigned from a dynamic IP address pool.
- **l2tp-lns-assigned**: Selects subscribers whose IP addresses were assigned by the Layer 2 Tunneling Protocol (L2TP) Network Server.
- **mip-ha-assigned**: Selects subscribers whose IP addresses were assigned by the Mobile IP Home Agent.
- **ms-provided-static**: Selects subscribers whose IP addresses were provided by the Mobile Station.

- **not-ms-provided-static**: Selects subscribers whose IP addresses were not provided by the Mobile Station.
- **static-pool**: Selects subscribers whose IP addresses were assigned from a static IP address pool.

The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-access-service, hnbgw-service, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-up-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, nsapi, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, relay-agent, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tpo, tx-data, ue-type, username, grep, more

### **ip-pool *ip\_pool\_name***

Displays subscriber information based on the IP pool name. *ip\_pool\_name* must be an existing IP pool name expressed as an alphanumeric string of 1 through 31 characters.

The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-access-service, hnbgw-service, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-up-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, nsapi, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tpo, tx-data, ue-type, username, grep, more

### **ipcf-only**

Displays Intelligent Policy Control Function (IPCF) subscriber session information.

### **ipsg-only**

Displays IP Services Gateway (IPSG) subscriber session information.

The following filter keywords are valid with this command:

epdg-address, epdg-service

### **ipv6-address *ipv6\_address***

Displays the subscribers associated with the specified IPv6 address. Must be followed by the IP address in IPv8 colon-separated-hexadecimal notation.

The following filter keywords are valid with this command:

apn, asn-peer-address, asngw-service, asnpc-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgw-address, sgw-service, smgr-instance, tx-data, username, grep, more

### **ipv6-prefix *ipv6\_prefix***

Displays the subscribers associated with the specified IPv6 address prefix. Must be followed by an IPv6 address prefix in the format `xx:xx:xx::/len`

The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-service, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-up-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, nsapi, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tpo, tx-data, ue-type, username, grep, more

### **l3-tunnel-local-addr *ipv4\_address***

Displays subscriber information based on the layer 3 tunneling interface. Must be followed by an IP address of the local interface, using IPv4 dotted-decimal notation.

The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-service, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-up-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, nsapi, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tpo, tx-data, ue-type, username, grep, more

### **l3-tunnel-remote-addr *ipv4\_address***

Displays subscriber information based on the layer 3 tunneling interface. Must be followed by an IP address of the remote interface, using IPv4 dotted-decimal notation.

The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-service, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-up-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, nsapi, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tpo, tx-data, ue-type, username, grep, more

### **lac ipv4\_address**

Displays subscriber information based on the Peer L2TP Access Concentrator (LAC). Must be followed by the IP address of a Remote LAC in IPv4 dotted-decimal notation.

The following filter keywords are valid with this command:

apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username, grep, more

### **lac-only**

Displays subscriber information based on the L2TP Access Concentrator (LAC) context information for the session.

### **lac-service svc\_name**

Displays subscriber information based on an existing LAC service name expressed as an alphanumeric string of 1 through 63 characters.

The following filter keywords are valid with this command:

apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, local-tunnel-id, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, remote-tunnel-id, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username, grep, more

### **lma-only**

Displays Local Mobility Anchor (LMA) specific context information for the session.

**lma-service *svc\_name***

Displays subscriber information based on the LMA service name. *svc\_name* must be an existing LMA service expressed as an alphanumeric string of 1 through 63 characters.

**lms *ipv4\_address***

Displays subscriber information based on the L2TP Network Server (LNS). Must be followed by the IP address of an LNS in IPv4 dotted-decimal notation.

The following filter keywords are valid with this command:

```
apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout,
connected-time, dhcp-server, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service,
firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address,
gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi,
ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr,
l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left,
mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested,
network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state,
s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username,
grep, more
```

**lms-only**

Displays LNS specific information only.

**lms-service *svc\_name***

Displays subscriber information based on an existing L2TP Network Server (LNS) service name expressed as an alphanumeric string of 1 through 63 characters.

The following filter keywords are valid with this command:

```
bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, connected-time,
ebi, enodeb-address, epdg-address, epdg-service, fa, firewall, fw-and-nat, gtp-version,
gtpu-bind-address, gtpu-service, ha, idle-time, ims-auth-service, imsi, ip-address,
ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr,
l3-tunnel-remote-addr, lac, lac-service, lns-service, local-tunnel-id,
long-duration-time-left, mipv6ha-service, msid, nat, network-type, profile-id, profile-name,
qci, remote-tunnel-id, rx-data, slu-state, s5-proto, session-time-left, sgw-address,
smgr-instance, tx-data, username, grep, more
```

**long-duration-time-left [ < | > | greater-than | less-than ] *value***

Shows how much time is left for the maximum duration of a specified subscriber session.

- <: Filters output so that only information less than the specified value is displayed.
- >: Filters output so that only information greater than the specified value is displayed.
- **greater-than**: Filters output so that only information greater than the specified value is displayed.
- **less-than**: Filters output so that only information less than the specified value is displayed.
- *value*: Used in conjunction with <, >, greater-than, less-than, If no other filtering options are specified only output matching *value* is displayed. If *value* is not specified all data is displayed. *value* must be an integer from 0 through 4294967295.

**mag-only**

Displays Mobile Access Gateway (MAG) subscriber session information.

**mag-service** *svc\_name*: Displays subscriber information based on the Mobile Access Gateway (MAG) service name. *svc\_name* must be an existing MAG service expressed as an alphanumeric string of 1 through 63 characters.

**mag-service** *svc\_name*

Displays subscriber information based on the Mobile Access Gateway (MAG) service name. *svc\_name* must be an existing MAG service expressed as an alphanumeric string of 1 through 63 characters.

**mip-udp-tunnel-only**

Displays Mobile IP Home Agent (MIP-HA) subscriber information for subscribers that negotiated MIP-UDP tunnels.

The following filter keywords are valid with this command:

```
apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout,
connected-time, dhcp-server, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service,
firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address,
gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi,
ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr,
l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left,
mip-udp-tunnel-only, mipv6ha-service, msid, msisd, nat, nemo-only, network-requested,
network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state,
s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username,
grep, more
```

**mipv6ha-only**

Displays MIP-HA-IPv6 context information for the session.

The following filters/keywords are valid with this command:

```
aaa-configuration, access-flows, access-type, active, active-charging-service, activity,
all, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy,
bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only,
configured-idle-timeout, connected-time, counters, data-rate, dhcp-server, domain, dormant,
ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, full, fw-and-nat,
ggsn-address, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service,
ha, ha-ipsec-only, ha-service, hnbgw-service, hsgw-service, idle-time, imei,
ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix,
l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service,
long-duration-time-left, mag-service, mipv6ha-service, mme-address, mme-service, msid,
nat, network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service,
pgw-address, policy, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto,
security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service,
smgr-instance, subscription, summary, tft, tpo, tx-data, ue-type, username, wfl, grep, more
```

**mipv6ha-service** *svc\_name*

Displays subscriber information based on an existing MIP Home Agent IPv6 service name expressed as an alphanumeric string of 1 through 63 characters.

The following filter keywords are valid with this command:

```
access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service,
bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only,
configured-idle-timeout, connected-time, dhcp-server, domain, ebi, enodeb-address,
```

```
epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service,
gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only,
ha-service, hnbgw-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address,
ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr,
l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service,
long-duration-time-left, mag-service, mip-up-tunnel-only, mipv6ha-service, mme-address,
mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcc-service,
pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id,
profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left,
sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tpo, tx-data, ue-type,
username, grep, more
```

### mme-address

Displays subscriber information based on the Mobility Management Entity (MME) IP address. *ip\_address* must be an existing MME IP address and be entered in IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.

The following filter keywords are valid with this command:

```
bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, connected-time,
ebi, enodeb-address, epdg-address, epdg-service, fa, firewall, fw-and-nat, gtp-version,
gtpu-bind-address, gtpu-service, ha, idle-time, imei, ims-auth-service, imsi, ip-address,
ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr,
l3-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, mme-address, mme-service,
msid, msisdn, nat, network-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto,
session-time-left, sgw-address, smgr-instance, tx-data, username, grep, more
```

### mme-only

Displays MME subscriber session information.

**mme-service** *svc\_name*: Displays subscriber information based on the MME service name. *svc\_name* must be an existing MME service expressed as an alphanumeric string of 1 through 63 characters.

**mme-address** *ip\_address*: Displays subscriber information based on the MME IP address. *ip\_address* must be an existing MME IP address entered in IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.

The following filter keywords are valid with this command:

```
bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, connected-time,
ebi, enodeb-address, epdg-address, epdg-service, fa, firewall, fw-and-nat, gtp-version,
gtpu-bind-address, gtpu-service, ha, idle-time, imei, ims-auth-service, imsi, ip-address,
ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr,
l3-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, mme-address, mme-service,
msid, msisdn, nat, network-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto,
session-time-left, sgw-address, smgr-instance, tx-data, username, grep, more
```

### mseg-only



#### Important

This keyword is not supported in this release.

**mseg-service *mseg\_service\_name***

**Important** This keyword is not supported in this release.

**msid *msid***

For this SGSN-specific keyword, enter the MSID (Mobile Station Identifier) to display information specific to one subscriber's equipment by entering the MSID.

The following filter keywords are valid with this command:

apn, asn-peer-address, asngw-service, asnpc-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgw-address, sgw-service, smgr-instance, tx-data, username, grep, more

**msisdn *msisdn***

For this SGSN-specific keyword, enter the MSISDN (Mobile Station ISDN number - unique SIM phone number) to display information specific to one subscriber's equipment by entering the MSISDN.

The following filter keywords are valid with this command:

apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username, grep, more

**nat { not-required | required }**

Displays information for subscribers based on whether or not Network Address Translation (NAT) processing is required.

The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-up-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, multiple-ips-per-nat-realm, nat, nat-ip, nat-realm, nemo-only,



network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tpo, tx-data, ue-type, usage-time, username, grep, more

### nemo-only

Displays information on MIP-HA subscribers that are mobile routers (Network Mobility).

The following filter keywords are valid with this command:

apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username, grep, more

### network-requested

Selects the currently active subscribers whose sessions were initiated by a GGSN network requested to create a PDP context.

The following filter keywords are valid with this command:

access-type, active-charging-service, apn, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-up-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, nsapi, pcc-service, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, smgr-instance, tpo, tx-data, ue-type, username, grep, more

### network-type { gre | ipip | ipsec | ipv4 | ipv4-pmipv6 | ipv4v6 | ipv4v6-pmipv6 | ipv6 | ipv6-pmipv6 | l2tp | mobile-ip | proxy-mobile-ip }

Selects the currently active subscribers based on network service access type.

- **gre**: Generic Routing Encapsulation
- **ipip**: IP-in-IP
- **ipsec**: IPSec
- **ipv4**: IPv4 only
- **ipv4-pmipv6**: IPv4 and/or Proxy Mobile IPv6 (PMIP)
- **ipv4v6**: IPv4 and/or IPv6
- **ipv4v6-pmipv6**: IPv4, IPv6 and/or Proxy Mobile IPv6
- **ipv6**: IPv6 only
- **ipv6-pmipv6**: IPv6 and/or Proxy Mobile IPv6 (PMIP)

- **l2tp**: Layer 2 Tunneling Protocol
- **mobile-ip**: Mobile IP (MIP)
- **proxy-modile-ip**: Proxy Mobile IPv6 (PMIP)

The following filter keywords are valid with this command:

apn, asn-peer-address, asngw-service, asnpc-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgw-address, sgw-service, smgr-instance, tx-data, username, grep, more

### **pcc-service name**

Displays statistics for users associated with an existing Policy and Charging Control (PCC) service name expressed as an alphanumeric string of 1 through 63 characters.

### **pcf [ < | > | less-than | greater-than ] ipv4\_address [ < | > | less-than | greater-than ] ipv4\_address ]**

Displays information for subscribers connected via the packet control function (PCF) with a specific or range of IP addresses. The address must be specified using IPv4 dotted-decimal notation.

- **<**: Filters output so that only information less than the specified IPv4 address value is displayed.
- **>**: Filters output so that only information greater than the specified IPv4 address value is displayed.
- **less-than**: Filters output so that only information less than the specified IPv4 address value is displayed.
- **greater-than**: Filters output so that only information greater than the specified IPv4 address value is displayed.

Note: It is possible to define a limited range of IP addresses by using the less-than and greater-than options to define minimum and maximum values.

The following filter keywords are valid with this command:

<, apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, less than, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username, grep, more

### **pdg-only**

Displays a summary of PDG subscriber statistics.

The following filters/keywords are valid with this command:

aaa-configuration, access-flows, active, activity, all, apn, bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, connected-time, counters, data-rate, dormant, ebi, enodeb-address, epdg-address, epdg-service, fa, firewall, full, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, nat, network-type, pdg-service, policy, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgw-address, smgr-instance, subscription, summary, tft, tx-data, username, wfl, grep, more

### **pdg-service name**

Displays statistics for users associated with an existing Packet Data Gateway (PDG) service name expressed as an alphanumeric string of 1 through 63 characters.

The following filters/keywords are valid with this command:

bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, connected-time, ebi, enodeb-address, epdg-address, epdg-service, fa, firewall, fng-service, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, nat, network-type, pdg-service, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgw-address, smgr-instance, tx-data, username, grep, more

### **pdif-only**

Displays a summary of Packet Data Interworking Function (PDIF) subscriber statistics.

The following filters/keywords are valid with this command:

aaa-configuration, access-flows, active, activity, all, apn, bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, connected-time, counters, data-rate, dormant, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fng-service, full, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, nat, network-type, pdif-service, policy, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgw-address, smgr-instance, subscription, summary, tft, tx-data, username, wfl, grep, more

### **pdif-service name**

Displays connection statistics for users associated with a specific PDIF service name.

The following filters/keywords are valid with this command:

bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, connected-time, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fng-service, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, nat, network-type, pdif-service, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgw-address, smgr-instance, tx-data, username, grep, more

### **pdsn-only**

Displays a summary of Packet Data Serving Node (PDSN) subscriber statistics.

The following filters/keywords are valid with this command:

aaa-configuration, access-flows, active, activity, all, apn, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout,

connected-time, counters, data-rate, dhcp-server, dormant, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, full, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, msid, nat, nemo-only, network-requested, network-type, pcf, pdsn-service, plmn-type, policy, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgsn-service, sgw-address, smgr-instance, subscription, summary, tft, tpo, tx-data, username, wfl, grep, more

### **pdsn-service name**

Displays statistics for users associated with an existing PDSN service name expressed as an alphanumeric string of 1 through 63 characters.

The following filter keywords are valid with this command:

apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mag-address, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username, grep, more

### **pgw-address ip\_address**

Displays information about the subscribers connected to the specified P-GW.

*ip\_address* must be specified by its IP address using dotted-decimal notation for IPv4 or colon separated notation for IPv6.

The following filters/keywords are valid with this command:

active-charging-service, apn, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, configured-idle-timeout, connected-time, ebi, enodeb-address, epdg-address, epdg-service, fa, firewall fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac-service, lma-service, lns, long-duration-time-left, mag-service, mipv6ha-service, msid, nat, network-type, pgw-address, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, saegw-service, session-time-left, sgw-address, sgw-service, smgr-instance, tx-data, username

### **pgw-only**

Displays PDN-Gateway (P-GW) subscriber session information.

The following filters/keywords are valid with this command:

all, apn, callid, card-num, ebi, epdg-address, full, imsi, interface-type, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, network-type, pgw-service, plmn-type, profile-name, qci, sgw-address, smgr-instance, summary

- **epdg-address ip\_address**: Displays subscriber information based on the ePDG IP address. *ip\_address* must be an existing ePDG IP address.
- **interface-type**: Interface type of subscriber.

**S2aGTP:** Interface type S2a GTP.

**S2bGTP:** Interface type S2b GTP.

**S5S8GTP:** Interface type S5/S8 GTP.

- **pgw-service** *svc\_name*: Displays subscriber information based on the P-GW service name. *svc\_name* must be an existing P-GW service expressed as an alphanumeric string of 1 through 63 characters.
- **qci number**: Displays subscriber session information based on the QoS Class Identifier (QCI) value assigned to the subscriber. *number* must be an integer value from 0 to 9.
- **sgw-address** *ip\_address*: Displays subscriber information based on the S-GW IP address. *ip\_address* must be an existing S-GW IP address.

### **plmn-type [ home | roaming | visiting ]**

Displays subscriber information based on the type of Public Land Mobile Network (PLMN).

- **home**: For GGSN/PGW, shows all the subscribers of charging type HOME.
- **roaming**: For GGSN/PGW, shows all the subscribers of charging type ROAMING.
- **visiting**: For GGSN/PGW, shows all the subscribers of charging type VISITING.

The following filter keywords are valid with this command:

apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username, grep, more

### **policy**

Displays the current policies associated with the subscriber session.

The following filter keywords are valid with this command:

access-type, active-charging-service, all, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, dormant, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-service, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-up-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, nsapi, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tpo, tx-data, ue-type, username, grep, more

**profile-id *id\_number***

Displays subscriber session information based on the profile-id granted for the flow. *id\_number* must be an integer from 0 to 4294967295.

**profile-name *name***

Displays subscriber session information based on an existing policy profile name expressed as an alphanumeric string of 1 through 63 characters.

**qci *number***

Displays subscriber session information based on the QoS Class Identifier (QCI) value assigned to the subscriber. *number* must be an integer value from 0 to 9.

**rulebase *name***

Displays subscriber session information based on the named Active Charging System rulebase. *name* must be an alphanumeric string of 1 through 63 characters.

**rulename *rule\_name***

Displays subscribers associated with the specific charging rule name. The *rule\_name* options are: predefined, static, and dynamic rules..

**rx-data [ < | > | greater-than | less-than ] *value***

The number of bytes received by the specified subscriber.

- <: Filters output so that only information less than the specified value is displayed.
- >: Filters output so that only information greater than the specified value is displayed.
- **greater-than**: Filters output so that only information greater than the specified value is displayed.
- **less-than**: Filters output so that only information less than the specified value is displayed.
- *value*: Used in conjunction with <, >, greater-than, less-than, If no other filtering options are specified only output matching *value* is displayed. If *value* is not specified all data is displayed. *value* must be an integer from 0 through 18446744073709551615.

**s1u-state { active | idle | idle-active }**

Displays session information based on the subscriber's S1-U state. The S1-U interface is the interface from the eNodeB to the S-GW.

- **active**: Displays session information for subscribers with an S1-U state set to active.
- **idle**: Displays session information for subscribers with an S1-U state set to idle.
- **idle-active**: Displays session information for subscribers with an S1-U state set to idle-active.

**s5-proto { gtp | pmip }**

Displays subscriber session information based on the S5 interface protocol used. This interface provides user plane tunneling and tunnel management between S-GW and P-GW. Choose either GPRS Tunneling Protocol (GTP) or Proxy Mobile IPv6 (PMIP).

**saegw-only**

Displays System Architecture Evolution Gateway (SAEGW) subscriber session information.

The following filters/keywords are valid with this command:

```
aaa-configuration, access-flows, active, active-charging-service, activity, all, apn,
bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, co-located,
configured-idle-timeout, connected-time, counters, data-rate, dormant, ebi, enodeb-address,
epdg-address, epdg-service, fa, firewall, full, fw-and-nat, gtp-version, gtpu-bind-address,
gtpu-service, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool,
ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac-service,
lma-service, lns, long-duration-time-left, mipv6ha-service, msid, nat, network-type,
pgw-address, pgw-anchored, plmn-type, policy, profile-id, profile-name, qci, rulebase,
rx-data, slu-state, s5-proto, saegw-service, session-time-left, sgw-address, sgw-anchored,
smgr-instance, subscription, summary, tft, tx-data, username, wfl
```

- **co-located**: Shows only co-located subscribers which have both S-GW and P-GW functions.
- **pgw-anchored**: Shows only PGW-anchored subscribers.
- **saegw-service *svc\_name***: Displays subscriber information based on the SAEGW service name. *svc\_name* must be an existing SAEGW service expressed as an alphanumeric string of 1 through 63 characters.
- **sgw-anchored** : Shows only SGW-anchored subscribers.

**saegw-service *svc\_name***

Displays subscriber information based on the SAEGW service name.

*svc\_name* must be an existing SAEGW service expressed as an alphanumeric string of 1 through 63 characters.

The following filters/keywords are valid with this command:

```
active-charging-service, apn, bandwidth-policy, bearer-establishment, bng-service, callid,
card-num, cbb-policy, configured-idle-timeout, connected-time, ebi, enodeb-address,
epdg-address, epdg-service, fa, firewall, fw-and-nat, gtp-version, gtpu-bind-address,
gtpu-service, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool,
ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac-service,
lma-service, lns, long-duration-time-left, mipv6ha-service, msid, nat, network-type,
pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto,
saegw-service, session-time-left, sgw-address, smgr-instance, tx-data, username
```

**security-type { ipsec | tls }**

Displays subscriber information based on the specified type of security.

- **ipsec**: IPsec
- **tls**: Transport Layer Security

**session-time-left [ < | > | greather-than | less ] *value***

How much session time is left for the specified subscriber.

- **<**: Filters output so that only information less than the specified value is displayed.

- **>**: Filters output so that only information greater than the specified value is displayed.
- **greater-than**: Filters output so that only information greater than the specified value is displayed.
- **less-than**: Filters output so that only information less than the specified value is displayed.
- **value**: Used in conjunction with **<**, **>**, **greater-than**, **less-than**. If no other filtering options are specified only output matching **value** is displayed. If **value** is not specified all data is displayed. **value** must be an integer from 0 through 4294967295.

### **sgsn-address *ipv4\_address***

This SGSN-only keyword displays only subscriber context information for the specified interface. Must be followed by the IP address of the interface, using IPv4 dotted-decimal notation.

The following filter keywords are valid with this command:

```
apn, callid, card-num, connected-time, idle-time, gprs-service, gsm-traffic-class,
gtp-version, imsi, msid, msisdn, nri, nsei, sgsn-service, smgr-instance
```

### **sgsn-only**

This SGSN-only keyword displays only 3G SGSN-specific subscriber context information.

The following filter keywords are valid with this command:

```
aaa-configuration, active, active-charging-service, activity, all, apn, callid, card-num,
configured-idle-timeout, connected-time, counters, data-rate, fa, full, ggsn-address,
gsm-traffic-class, idle-time, imei, imsi, msid, partial, plmn-type, profile-name, rnc,
rx-data, session-time-left, sgsn-service, summary, tx-data, wide-format, grep, more
```

### **sgsn-service *service\_name***

For this SGSN-only keyword, enter the name of the configured 3G SGSN service to display subscriber information specific to the named SGSN service.

The following filter keywords are valid with this command:

```
apn, bearer-establishment, bng-service, callid, card-num, configured-idle-timeout,
connected-time, ebi, enodeb-address, epdg-address, epdg-service, fa, firewall, fw-and-nat,
gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, idle-time,
imei, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix,
l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid,
msisdn, nat, network-type, nri, plmn-type, profile-id, profile-name, qci, rx-data, slu-state,
s5-proto, session-time-left, sgsn-service, sgw-address, smgr-instance, tx-data, username,
grep, more
```

### **sgw-address *ip\_address***

For this MME-only keyword, enter the IP address of the peer S-GW to display information about the subscribers connected to the specified S-GW. *ip\_address* must be specified by its IP address using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

### **sgw-only**

Displays S-GW subscriber session information.

The following filters/keywords are valid with this command:

```
all, full, summary
```



- **sgw-service** *svc\_name*: Displays subscriber information based on an existing S-GW service specified as an alphanumeric string of 1 through 63 characters.
- **pgw-address** *ip\_address*: Displays subscriber information based on an existing P-GW specified by its IP address in IPv4 dotted-decimal notation.

### **sgw-service** *svc\_name*

Displays subscriber information based on an existing S-GW service specified as an alphanumeric string of 1 through 63 characters.

The following filter keywords are valid with this command:

`epdg-address, epdg-service,`

### **smgr-instance** *instance\_id*

Displays subscription information associated with the Session Manager identifier expressed as an integer from 1 through 4294967295.

The following filter keywords are valid with this command:

`epdg-address, epdg-service,`

### **subscription** { *aor address* | *callid id* | *full* }

Displays subscription information for defined subscribers, based on defined parameters.

- **aor** *address*: Clears session(s) by Address of Record.
- **callid** *id*: Specifies a Call Identification Number as an 8-digit hexadecimal number.
- **full**: Displays all available information.

### **summary**

Displays only a summary of the subscriber information. The following filter keywords are valid with this command:

`access-type, active, active-charging-service, activity, all, asn-peer-address, asngw-service, asnpc-service, apn, bandwidth-policy, bearer-establishment, callid, card-num, cbb-policy, configured-idle-timeout, connected-time, dhcp-server, domain, dormant, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-service, hnbgw-service, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-services, mme-address, mme-service, mseg-service, msid, msisd, nat, network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pdsnclosedrp-service, pgw-address, plmn-type, profile-id, qci, rulebase, rulename <rule_name>, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgw-address, sgw-service, smgr-instance, tx-data, ue-type, username, without-dynamic-rule, without-override-control, grep, more`

### **tft**

Displays the current Traffic Flow Template (TFT) associated with the subscriber session.

The following filter keywords are valid with this command:

active, all, apn, asn-peer-address, asngw-service, asnpc-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, dormant, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisd, nat, nemo-only, network-requested, network-type, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgw-address, sgw-service, smgr-instance, tx-data, username, grep, more

### tx-data [ < | > | greater-than | less-than ] value

The number of bytes transmitted by the specified subscriber.

- <: Filters output so that only information less than the specified value is displayed.
- >: Filters output so that only information greater than the specified value is displayed.
- **greater-than**: Filters output so that only information greater than the specified value is displayed.
- **less-than**: Filters output so that only information less than the specified value is displayed.
- *value*: Used in conjunction with <, >, greater-than, less-than, If no other filtering options are specified only output matching *value* is displayed. If *value* is not specified all data is displayed. *value* must be an integer from 0 through 18446744073709551615.

The following filter keywords are valid with this command:

epdg-address, epdg-service,

### ue-type { ims | non-ims }

Displays information for the subscribers based on User Equipment type.

- **ims**: IP Multimedia Subsystem
- **non-ims**: UE other than IMS

The following filter keywords are valid with this command:

access-type, active-charging-service, bandwidth-policy, bearer-establishment, callid, card-num, cbb-policy, configured-idle-timeout, connected-time, domain, ebi, enodeb-address, epdg-address, epdg-service, fa, fa-service, firewall, fw-and-nat, gprs-service, gtp-version, gtpu-bind-address, gtpu-service, ha, hnbgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, msid, nat, network-type, pcc-service, profile-id, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgw-address, smgr-instance, tx-data, ue-type, username, grep, more

### username name

Displays information for connections for the subscriber identified by *name*. The user must have been previously configured. *name* must be a sequence of characters and/or wildcard characters ('\$' and '\*') from 1 to 127 characters. The \* wildcard matches multiple characters and the \$ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (''). For example; '\$'.

The following filter keywords are valid with this command:

epdg-address, epdg-service,

### **wf1**

Displays subscriber information in wide format number 1. Wide format number 1 includes the following information for each listed subscriber session:

- Access Type
- Access Technology
- Call State
- Link Status
- Network Type
- Call ID
- MSID
- Username
- IP Address
- Time-Idle
- Access Peer Address
- Service Address
- Network Peer Address
- Connect Time

The following filter keywords are valid with this command:

epdg-address, epdg-service,

### **without-dynamic-rule**

Displays subscribers without any dynamic rule associated with them.

### **without-override-control**

Displays subscribers without any override control rule associated with them.

### ***filter\_keywords***

The following keywords are filters that modify or filter the output of the Command Keywords. Not all filters are available for all Command Keywords. Multiple Filter Keywords can be entered on a command line.

When multiple Filter Keywords are specified, the output conforms to all of the Filter Keywords specifications.

For example; if you enter the following command:

### **show subscribers counters ip-pool pool1 card-num 1**

Counters for all subscriber sessions that were assigned an IP address from the IP pool named pool1 and also are being processed by the processing card in slot 1 is displayed. Information for all other subscribers is not displayed.

**active**

Only display information for those subscribers who currently have active sessions.

**active-charging-service *acs\_service***

Displays information for subscribers being processed by the active charging service specified as an alphanumeric string of 1 through 15 characters.

**activity**

Displays subscriber link activity percentage.

**all**

If no keywords are specified before **all**, information for all subscribers is displayed. If keywords are specified before **all**, all information is displayed with no further options being allowed.

**apn *name***

Displays subscribers currently facilitated by the access point name (APN) configured on the SGSN or GGSN.

**asngw-only**

Displays counters for subscribers accessing the ASN-GW service only.

**asnpc-only**

Displays counters for subscribers accessing the ASN Paging Controller and Location Registry service only.

**bandwidth-policy *policy\_name***

Displays information for subscribers associated with the specified Active Charging bandwidth policy.

**bearer-establishment { *direct-tunnel* | *normal* | *pending* } *id***

Displays subscriber information for selected bearer establishment type.

**bng-service *svrc\_name***

Displays the current configuration for the specified Broadband Network Gateway (BNG) service.

**callid *id***

Displays subscriber information for the call ID specified as an 8-byte hexadecimal number.

**card-num *card\_num***

The slot number of the processing card by which the subscriber session is processed. The slot number is an integer from 1 through 7 and 10 through 16 on the ASR 5000, or 1 through 4 and 7 through 10 on the ASR 5500.

**cbb-policy *policy\_name***

Displays information for subscribers associated with the specified Active Charging Content Based Billing (CBB) policy.

**ccoa-only**

Displays the subscribers that registered a MIP with CoA directly with the HA.

This option is only valid when a MIPHA session license is enabled.

**configuration { all | username *name* }**

Displays current configuration for all subscribers or a specified subscriber.

**configured-idle-timeout [ < | > | greater-than | less-than ] *value***

Shows the idle timeout that is configured for the specified subscriber. A value of 0 (zero) indicates that the subscribers idle timeout is disabled.

<: Filters output so that only information less than the specified value is displayed.

>: Filters output so that only information greater than the specified value is displayed.

**greater-than**: Filters output so that only information greater than the specified value is displayed.

**less-than**: Filters output so that only information less than the specified value is displayed.

*value*: Used in conjunction with <, >, greater-than, less-than, If no other filtering options are specified only output matching *value* is displayed. If *value* is not specified all data is displayed. *value* must be an integer from 0 through 4294967295.

**connected-time [ < | > | greater-than | less-than ] *value***

Shows how long the subscriber has been connected. <: Filters output so that only information less than the specified value is displayed.

- <: Filters output so that only information less than the specified value is displayed.

- >: Filters output so that only information greater than the specified value is displayed.

- **greater-than**: Filters output so that only information greater than the specified value is displayed.

- **less-than**: Filters output so that only information less than the specified value is displayed.

- *value*: Used in conjunction with <, >, greater-than, less-than, If no other filtering options are specified only output matching *value* is displayed. If *value* is not specified all data is displayed. *value* must be an integer from 0 through 4294967295.

**counters *keyword***

Displays the specified counter for the subscribers.

**cpu-num *number***

Displays information for calls processed through the specified CPU number.

**dhcp-server *address***

Displays subscribers currently accessing the system that have been provided an IP address by the DHCP server specified by its address. GGSN only.

**dns-proxy**

Displays all subscribers associated with a DNS proxy.

**domain *name***

Displays all subscribers with an Address-of-Record (AoR) from the specified domain. *name* is an alphanumeric string of 1 through 79 characters.

**dormant**

Shows information for subscriber sessions that are dormant (not transmitting or receiving data).

**dormant**

Shows information for subscriber sessions that are dormant (not transmitting or receiving data).

**ebi *number***

Displays subscribers based on an EPS bearer identity number.

**enodeb-address *ip\_address***

Displays subscribers based on the eNodeB to which they are attached.

**epdg-address *ip\_address***

Displays information of subscribers connected to the specified ePDG address in IPv4 dotted-decimal notation or IPv6 (::) notation.

**epdg-service *service\_name***

Displays information of subscribers of ePDG service specified as an alphanumeric string of 1 through 63 characters.

**fa *address***

Displays information for subscribers connected to the foreign agent specified by its IP address in IPv4 dotted-decimal notation.

**fa-only**

Only display FA-specific context information.

**fa-service *name***

Displays information for subscribers connected to the named foreign agent (FA) service.

**firewall { not-required | required }**

Displays information for the specified subscribers:

- **not-required**: Subscribers for whom firewall processing is not required.
- **required**: Subscribers for whom firewall processing is required.

**firewall-policy *fw\_policy\_name***

This keyword is obsolete.

**full**

Displays all available information for subscribers.

**fw-and-nat policy *fw\_nat\_policy*****Important**

This option is customer-specific and is only available in StarOS 8.1.

Displays information for subscribers using an existing Firewall-and-NAT policy specified as an alphanumeric string of 1 through 15 characters.

**ggsn-address *ip\_address***

Displays information for subscribers connected to an existing GGSN specified by its IP address in IPv4 dotted-decimal notation. SGSN only

**ggsn-preservation-mode**

Displays information for subscribers connected to the GGSN service with preservation mode enabled. GGSN only.

**ggsn-service *name***

Displays information for subscribers connected to the named GGSN service. This keyword is for GGSN only.

**gprs-only**

Displays only 2G SGSN subscribers content. SGSN only.

**gprs-service *svc\_name***

Displays subscriber information for the named 2G GPRS service. SGSN only.

**gsm-traffic-class { background | conversational | interactive | streaming }**

Displays information for subscriber traffic that matches the specified 3GPP traffic class.

- **background**: 3GPP QoS background class.
- **conversational**: 3GPP QoS conversational class.

- **interactive**: 3GPP QoS interactive class. Must be followed by a traffic priority.
- **streaming**: 3GPP QoS streaming class.

#### **ha address**

Displays information for subscribers connected to the home agent specified by its IP address in IPv4 dotted-decimal notation.

#### **ha-ipsec-only**

Only displays information for subscriber sessions that are using IP-Security (IPSec).

#### **ha-only**

Only displays HA-specific context information.

#### **ha-service name**

Displays information for subscribers connected to the named home agent service.

#### **hnbgw-only**

Displays counters for subscribers accessing the Home evolved NodeB Gateway (HNB-GW) service only.

#### **idle-time [ < | > | greater-than | less-than ] value**

Displays how long the subscriber session has been idle or display subscriber sessions that meet the idle time criteria specified.

- **<**: Filters output so that only information less than the specified value is displayed.
- **>**: Filters output so that only information greater than the specified value is displayed.
- **greater-than**: Filters output so that only information greater than the specified value is displayed.
- **less-than**: Filters output so that only information less than the specified value is displayed.
- **value**: Used in conjunction with <, >, greater-than, less-than. If no other filtering options are specified only output matching *value* is displayed. If *value* is not specified all data is displayed. *value* must be an integer from 0 through 4294967295.

#### **imei imei\_number**

Displays information for subscribers having the specified International Mobile Equipment Identity (IMEI/IMEISV) number.

#### **ims-auth-service service\_name**

Displays information for subscribers for an existing IMS Authorization Service name.

#### **imsi id**

Displays the subscriber with the specified ID. The IMSI (International Mobile Subscriber Identity) ID is a 15-character string which identifies the subscriber's home country and carrier. Wildcard characters \$ and \*



are allowed. The \* wildcard matches multiple characters and the \$ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes ( ' ). For example; '\$'.

### **ip-address [ < | > | greater-than | less-than ] address**

Displays information for subscribers connected to the specified *address*.

- <: Filters output so that only information for subscribers with an IP address lower than the specified address is displayed.
- >: Filters output so that only information for subscribers with an IP address higher than the specified address is displayed.
- **greater-than**: Filters output so that only information for subscribers with an IP address higher than the specified address is displayed.
- **less-than**: Filters output so that only information for subscribers with an IP address lower than the specified address is displayed.
- *address*: The address must be specified using IPv4 dotted-decimal notation. Used in conjunction with <, >, greater-than, less-than. If the IP address is specified without a qualifier, only subscribers with the specified IP address have their information displayed.

### **ip-alloc-method {aaa-assigned | dhcp [ relay-agent | proxy-client ] | dynamic-pool | l2tp-lns-assigned | mip-ha-assigned | ms-provided-static | not-ms-provided-static | static pool }**

Displays the specific IP Allocation Method. Must be followed by one of the IP Allocation Methods:

- **aaa-assigned**: Selects subscribers whose IP addresses were assigned by AAA.
- **dhcp**: Selects subscribers whose IP addresses were assigned by DHCP.
  - **relay-agent**: Selects subscribers whose IP addresses were assigned by the DHCP Relay Agent
  - **proxy-client**: Selects subscribers whose IP addresses were assigned by the DHCP Proxy Client
- **dynamic-pool**: Selects subscribers whose IP addresses were assigned from a dynamic IP address pool.
- **l2tp-lns-assigned**: Selects subscribers whose IP addresses were assigned by the Layer 2 Tunneling Protocol (L2TP) Network Server.
- **mip-ha-assigned**: Selects subscribers whose IP addresses were assigned by the Mobile IP Home Agent.
- **ms-provided-static**: Selects subscribers whose IP addresses were provided by the Mobile Station.
- **not-ms-provided-static**: Selects subscribers whose IP addresses were not provided by the Mobile Station.
- **static-pool**: Selects subscribers whose IP addresses were assigned from a static IP address pool.

### **ip-pool name**

Displays information for subscribers assigned addresses from an existing IP address pool or IP pool group. *name* will be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation based on the call line setup for the specified pool.

**ipv4**

Displays information for subscribers with an IPv4 Firewall enabled/disabled.

**ipv6**

Displays information for subscribers with an IPv6 Firewall enabled/disabled.

**ipv6-address *address***

Displays information for subscribers connected to the specified IPv6 address.

**ipv6-prefix *prefix***

Displays information for subscribers connected to the specified IPv6 address prefix.

**l3-tunnel-local-addr *ip\_address***

A layer 3 tunneling interface specified by its IP address in IPv4 dotted-decimal notation.

**l3-tunnel-remote-addr *ip\_address***

A layer 3 tunneling peer specified by its IP address in IPv4 dotted-decimal notation.

**lac *address***

Displays information for calls to the peer L2TP Access Concentrator (LAC) specified by its IP address.

**lac-only**

Displays LAC specific information only.

**lac-service *name* [ *local-tunnel-id id* | *remote-tunnel-id id* ]**

Displays information for calls associated with the LAC service specified as an alphanumeric string of 1 through 63 characters.

- **local-tunnel-id *id***: Specifies a local tunnel from which to clear calls as an integer from 1 through 65535.
- **remote-tunnel-id *id***: Specifies a remote tunnel from which to clear calls as an integer from 1 through 65535.

**lns *address***

Displays information for calls to the peer L2TP Network Server (LNS) specified by its IP address.

**lns-only**

Displays LNS specific information only.

**lns-service *name* [ *local-tunnel-id id* | *remote-tunnel-id id* ]**

Displays information for calls associated with the LNS service specified as an alphanumeric string of 1 through 63 characters.

- **local-tunnel-id** *id*: Indicates a specific local tunnel from which to clear calls. *id* must be an integer from 1 through 65535.
- **remote-tunnel-id** *id*: Indicates a specific remote tunnel from which to clear calls. *id* must be an integer from 1 through 65535.

**local-tunnel-id** *identifier*

Displays information for a local tunnel identifier specified as an integer from 1 to 65535.

**long-duration-time-left** [ < | > | greater-than | less-than ] *value*

Shows how much time is left for the maximum duration of a specified subscriber session.

- <: Filters output so that only information less than the specified value is displayed.
- >: Filters output so that only information greater than the specified value is displayed.
- **greater-than**: Filters output so that only information greater than the specified value is displayed.
- **less-than**: Filters output so that only information less than the specified value is displayed.
- *value*: Used in conjunction with <, >, greater-than, less-than, If no other filtering options are specified only output matching *value* is displayed. If *value* is not specified all data is displayed. *value* must be an integer from 0 through 4294967295.

**mag-only**

Displays Mobile Access Gateway (MAG) subscriber session information.

**mag-service** *svc\_name*

Displays subscriber information based on the Mobile Access Gateway (MAG) service name. *svc\_name* must be an existing MAG service expressed as an alphanumeric string of 1 through 63 characters.

**mip-udp-tunnel-only**

Displays the subscribers that negotiated MIP-UDP tunneling with the HA.

This option is only valid when MIP NAT Traversal license is enabled.

**mipv6ha-only**

Displays MIPV6HA-specific context information for the session.

**mipv6ha-service** *service\_name*

Displays specific configured MIPV6 Home Agent service. *service\_name* must have been previously defined.

**msid** *id*

Displays information for the mobile user identified by *id*. *id* must be from 7 to 16 hexadecimal digits specified as an IMSI, MIN, or RMI. Wildcard characters \$ and \* are allowed. The \* wildcard matches multiple characters and the \$ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes ( ' ). For example: '\$'.

In case of **enforce imsi-min equivalence** is enabled on the chassis and MIN or IMSI numbers supplied, this filter will show subscribers with a corresponding MSID (MIN or IMSI) whose lower 10 digits matches to lower 10 digits of the supplied MSID.

**show subscribers msid** *ABCD0123456789* or

**show subscribers msid** *0123456789*

will show any subscriber with a MSID that match the lower 10 digits of MSID supplied, for example, 0123456789.

### **msisdn** *msisdn*

Displays information for the mobile user identified by the Mobile Subscriber ISDN Number (MSISDN).

*msisdn* must be 7 to 16 digits; specified as an IMSI, MIN, or RMI.

### **nat** { **not-required** | **required** }

Displays information for the specified subscribers.

- **not-required**: Subscribers for whom Network Address Translation (NAT) processing is not required.
- **required**: Subscribers for whom NAT processing is required.

### **nat-ip** *nat\_ip\_address* ] }

Displays information for the subscribers for whom NAT processing is enabled and are using the specified NAT IP address. *nat\_ip\_address* specifies the NAT IP address and must be in IPv4 dotted-decimal notation. **The nat-ip keyword is only available in StarOS 8.3 and later releases.**

### **nat-realm** *nat\_realm*

Displays information for the subscribers for whom NAT processing is enabled and are using the specified NAT realm. *nat\_realm* specifies the NAT realm name and must be a string from 1 through 63 characters.

### **network-requested**

Display information for currently active subscribers whose sessions were initiated by the GGSN network requested create PDP context procedure.

### **network-type** { **gre** | **ipip** | **ipsec** | **ipv4** | **ipv4-pmipv6** | **ipv4v6** | **ipv4v6-pmipv6** | **ipv6** | **ipv6-pmipv6** | **l2tp** | **mobile-ip** | **proxy-mobile-ip** }

Selects the currently active subscribers based on network service access type.

- **gre**: Generic Routing Encapsulation
- **ipip**: IP-in-IP
- **ipsec**: IPsec
- **ipv4**: IPv4 only
- **ipv4-pmipv6**: IPv4 and/or Proxy Mobile IPv6 (PMIP)
- **ipv4v6**: IPv4 and/or IPv6

- **ipv4v6-pmipv6**: IPv4, IPv6 and/or Proxy Mobile IPv6
- **ipv6**: IPv6 only
- **ipv6-pmipv6**: IPv6 and/or Proxy Mobile IPv6 (PMIP)
- **l2tp**: Layer 2 Tunneling Protocol
- **mobile-ip**: Mobile IP (MIP)
- **proxy-mobile-ip**: Proxy Mobile IPv6 (PMIP)

#### **nri nri\_value**

This SGSN-specific filter uses the configured network resource identifier (NRI) to identify a specific SGSN in a pool to fine-tune the subscriber information to be displayed.

*nri\_value*: enter an integer from 0 through 63

This filter can be used in combination with further refining filters.

#### **nsapi nsap\_id**

Displays session information for the mobile user identified by Network Service Access Point Identifier (NSAPI) between MS and SGSN. NSAPI is also used as part of the tunnel identifier between GPRS Support Nodes (GSNs). The user identity IMSI and the application identifier (NSAPI) are integrated into the Tunnel Identifier (GTPv0) (TID) or Tunnel Endpoint Identifier (GTPv1) (TEID) that uniquely identifies the subscriber's sublink between the GSNs (SGSN and GGSN). The NSAPI is an integer value within the PDP context header.

*nsap\_id* must be an integer from 5 through 15.

#### **partial qos { negotiated | requested }**

This filter is specific to the SGSN.

It limits the display of information to requested or negotiated QoS information for the subscriber.

This filter can be used in combination with further defining filters: active, active-charging-service, all, apn, callid, card-num, configured-idle-timeout, connected-time, ggsn-address, gprs-service, gsm-traffic-class, idle-time, imsi, msid, msisdh, negotiated, plmn-type, requested, rx-data, session-time-left, tx-data

#### **pcc-service name**

Displays statistics for users associated with an existing Policy and Charging Control (PCC) service name expressed as an alphanumeric string of 1 through 63 characters.

#### **pcf [ < | > | less-than | greater-than ] ipv4\_address [ < | > | less-than | greater-than ] ipv4\_address ]**

Displays information for subscribers connected via the packet control function with a specific or range of IP addresses. The address must be specified using IPv4 dotted-decimal notation.

- **<**: Filters output so that only information less than the specified IPv4 address value is displayed.
- **>**: Filters output so that only information greater than the specified IPv4 address value is displayed.
- **less-than**: Filters output so that only information less than the specified IPv4 address value is displayed.

- **greater-than**: Filters output so that only information greater than the specified IPv4 address value is displayed.

Note: It is possible to define a limited range of IP addresses by using the less-than and greater-than options to define minimum and maximum values.

**pdsn-only**

Show PDSN specific information only.

**pdsn-service *name***

Displays information for subscribers connected to the packet data service *name*. The packet data service must have been previously configured.

**pdsnclosedrp-service *service\_name***

Displays information for subscribers connected to the Closed R-P service *service\_name*. The Closed R-P service must have been previously configured.

**plmn-type**

Displays subscriber type (HOME, VISITING, or ROAMING).

This keyword is for the GGSN or the SGSN only.

**policy**

Displays the current policies associated with the subscriber session.

**profile-id *id\_number***

Displays subscriber session information based on the profile-id granted for the flow. *id\_number* must be an integer from 0 to 4294967295.

**profile-name *profile\_name***

Displays the subscribers filtered with PCC profile named *profile\_name* in particular IP-CAN session.

**qci *number***

Displays subscriber session information based on the QoS Class Identifier (QCI) value assigned to the subscriber. *number* must be an integer value from 0 to 9.

**relay-agent**

Selects subscribers whose IP Addresses were assigned by the DHCP Relay Agent.

**remote-tunnel-id *identifier***

Displays information for a remote tunnel identifier specified as an integer from 1 to 65535.

**rnc id *rnc\_id* mcc *mcc\_num* mnc *mnc\_num***

Displays information for subscribers connected to the SGSN via a specific RNC (radio network controller) identified by the RNC ID, the MCC (mobile country code), and the MNC (mobile network code). SGSN only

**rulebase *name***

Selects subscribers associated with the specified Active Charging rulebase.

**rx-data [ < | > | greater-than | less-than ] *value***

The number of bytes received by the specified subscriber.

- <: Filters output so that only information less than the specified value is displayed.
- >: Filters output so that only information greater than the specified value is displayed.
- **greater-than**: Filters output so that only information greater than the specified value is displayed.
- **less-than**: Filters output so that only information less than the specified value is displayed.
- *value*: Used in conjunction with <, >, greater-than, less-than, If no other filtering options are specified only output matching *value* is displayed. If *value* is not specified all data is displayed. *value* must be an integer from 0 through 18446744073709551615.

**saegw-only**

Displays System Architecture Evolution Gateway (SAEGW) subscriber session information only.

**saegw-service *svc\_name***

Displays subscriber information based on the SAEGW service name.

*svc\_name* must be an existing SAEGW service expressed as an alphanumeric string of 1 through 63 characters.

**security-type { ipsec | tls }**

Displays subscriber information based on the specified type of security.

- **ipsec**: IPSec
- **tls**: Transport Layer Security

**session-time-left [ < | > | greater-than | less ] *value***

How much session time is left for the specified subscriber.

- <: Filters output so that only information less than the specified value is displayed.
- >: Filters output so that only information greater than the specified value is displayed.
- **greater-than**: Filters output so that only information greater than the specified value is displayed.
- **less-than**: Filters output so that only information less than the specified value is displayed.
- *value*: Used in conjunction with <, >, greater-than, less-than, If no other filtering options are specified only output matching *value* is displayed. If *value* is not specified all data is displayed. *value* must be an integer from 0 through 4294967295.

**smgr-instance *number***

Specific sessmgr instance. *number* must be in the range of 1 to 4294967295.

**sgsn-address *address***

Shows information for subscribers whose PDP contexts are currently being facilitated by the SGSN specified by address. This command is for GGSN only.

**sgsn-service *svrc\_name***

Shows subscriber information for a specified 3G SGSN service. *svrc\_name* must be an alphanumeric string of 1 through 63 characters that identifies a configured SGSN service.

This command is for SGSN only.

**subscription { aor *address* | callid *id* | full }**

Displays subscription information for defined subscribers, based on defined parameters.

- **aor *address***: Clears session(s) by Address of Record.
- **callid *id***: Specifies a Call Identification Number as an 8-digit hexadecimal number.
- **full**: Displays all available information.

**tft**

Displays the current Traffic Flow Template (TFT) associated with the subscriber session.

**tpo { not-required | required }****Important**


---

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

---

Displays information for specified subscribers.

**tx-data [ < | > | greater-than | less-than ] *value***

The number of bytes transmitted by the specified subscriber.

- **<**: Filters output so that only information less than the specified value is displayed.
- **>**: Filters output so that only information greater than the specified value is displayed.
- **greater-than**: Filters output so that only information greater than the specified value is displayed.
- **less-than**: Filters output so that only information less than the specified value is displayed.
- **value**: Used in conjunction with <, >, greater-than, less-than, If no other filtering options are specified only output matching *value* is displayed. If *value* is not specified all data is displayed. *value* must be an integer from 0 through 18446744073709551615.



**ue-type { ims | non-ims }**

Displays information for the subscribers based on User Equipment type.

- **ims**: IP Multimedia Subsystem
- **non-ims**: UE other than IMS

**username *name***

Displays information for connections for the subscriber identified by *name*. The user must have been previously configured. *name* must be a sequence of characters and/or wildcard characters ('\$ and '\*') from 1 to 127 characters. The \* wildcard matches multiple characters and the \$ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes ( '). For example; '\$'.

**verbose**

Display detailed information.

**wide-format**

Display detailed information in a wider screen format.

**{ *grep grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Use this command to view information about subscriber sessions.

The output of this command may be considered for part of a periodic system auditing program by verifying active and dormant subscribers.

The Command Keywords may be used standalone to display detailed information or you may use one or more of the various Filter Keywords to reduce the amount of information displayed.



---

**Caution**

Executing this command may negatively impact performance if multiple instances are executed while the system is under heavy load and simultaneously facilitating multiple CLI sessions.

---

**Example**

The following command displays information for all subscriber sessions:

```
show subscribers all
```

The following command displays information for all ggsn-only subscriber sessions:

```
show subscribers ggsn-only all
```

The following command displays information for all subscriber sessions in wide format 1:

```
show subscribers wfl all
show subscribers aaa-configuration
show subscribers counters username ispluser1
```

The following command displays information for subscriber in GGSN service:

```
show subscribers ggsn-only all
show subscribers ggsn-only full
```

The following command displays information for all subscriber with SGSN session having partial QoS requests:

```
show subscribers sgsn-only partial qos requested
```

The following command displays information for all subscriber with MME session connected to MME service having IP address as *10.1.1.1*:

```
show subscribers mme-only mme-address 10.1.1.1
```




---

**Important** Output descriptions for commands are available in the *Statistics and Counters Reference*.

---

## show subscribers samog-only

Displays SaMOG specific context information for the session.

---

**Product** SaMOG

---

**Privilege** Inspector

---

**Syntax Description** `show subscribers samog-only [ [ all ] [ callid call_id ] [ card-num card_num ] [ connected-time [ < | > | greater-than | less-than ] connected_time ] [ full ] [ idle-time [ < | > | greater-than | less-than ] idle_time ] [ ip-address [ < | > | greater-than | less-than ] ipv4_adress ] [ ipv6-prefix ipv6_prefix ] [ network-type { gre | ipip | ipsec | ipv4 | ipv4-pmipv6 | ipv4v6 | ipv4v6-pmipv6 | ipv6 | ipv6-pmipv6 | l2tp | mobile-ip | proxy-mobile-ip } ] [ session-time-left [ < | > | greater-than | less-than ] session_time_left ] [ smgr-instance smgr_instance ] [ summary ] [ username user_name ] [ | { grep grep_options | more } ] ]`

**idle-time [ < | > | greater-than | less-than ] *idle\_time***

Displays how long the subscriber has been idle.

> and **greater-than** Specifies greater than. This must be followed by *idle\_time*, an integer ranging from 0 and 4294967295.

< and **less-than** Specifies less than. This must be followed by *idle\_time*, an integer ranging from 0 and 4294967295.

**ipv6-prefix *ipv6\_prefix***

Displays the subscribers associated with the specified IPv6 address prefix. Must be followed by an IPv6 address prefix in the format `xx:xx:xx::/len`

**{ *grep grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on using the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

## show subscribers wsg-service

Displays information for specific configured WSG service. This command must be followed by the WSG service name.

<b>Product</b>	SecGW (WSG)
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<b>show subscribers wsg-service</b> <i>service_name</i> [   { <b>grep</b> <i>grep_options</i>   more } ]  <b><i>service_name</i></b> Specifies the name of the WSG service as an alphanumeric string of 1 through 63 characters.
<b>Usage Guidelines</b>	Use this command to displays information about selected WSG calls and services.

**Example**

The following command displays counter information for wsg-service wsg01:

```
show subscribers wsg-service wsg01 arg1
```

## show super-charger

Lists subscribers with valid super-charger configuration. When super-charger is enabled for a subscriber, the SGSN handles 2G or 3G connections controlled by an operator policy and changes hand-off and location update procedures to reduce signaling traffic management (3GPP, TS.23.116).

<b>Product</b>	SGSN
<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show super-charger { imsi imsi | all }
```

**imsi**

Defines a specific subscriber's international mobile subscriber identity (IMSI) number.

**imsi** is a string of up to 15 digits that includes the MCC (mobile country code), the MNC (mobile network code) and the MSIN (mobile station identification number),

**all**

Instructs the SGSN to display super charger subscription information for all subscribers.

**Usage Guidelines**

Use this command to determine if a single subscriber, identified by the IMSI, has a super charger configuration. Also, this command can display the list of all subscribers with a super charger configuration. If a subscriber has super charger as part of the configuration, subscriber data is backed up (using the IMSI Manager) after the subscriber detaches and the purge timer expires.

**Example**

The following command displays the super charger configuration information for the subscriber identified by the IMSI 90121882144672.

```
show super-charger imsi 90121882144672
```

## show supplementary-service statistics

Displays the statistics for Supplementary Service Information.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show supplementary-service statistics
```

**Usage Guidelines**

Use this command to display the Supplementary Service Information.

**Example**

The following command displays the Supplementary Service Information:

**show supplementary-service statistics**

## show support collection

Displays information about when and where the Support Data Collector (SDC) stores its Support Data Record (SDR) files.

**Product** All

**Privilege** All

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description** **show support collection [ definitions ] [ | { grep *grep\_options* | more } ]**

### definitions

Displays the list of default support record section definitions. This is the list of all valid record section definitions. The display also indicates whether the record section is enabled or disabled by default.

### { grep *grep\_options* | more }

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on using the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Use this command to display the status of SDR collection, collection times, SDR file names and sizes, as well as the date/time the files were written. If SDR collection has occurred this command displays the pathname where the files have been stored.

With the **definitions** option this command lists existing record sections and their associated CLI commands.

For additional information, refer to the descriptions of the **support collection** and **support record** commands in the *Global Configuration Mode (L - S) Commands* chapter. Also see the *System Administration Guide*.

### Example

The following command displays the SDR collection information.

```
show support collection
```

# show support details

Displays a comprehensive list of system information that is useful for troubleshooting purposes. In most cases, the output of this command is requested by the Technical Assistance Center (TAC). A single instance of the output of this command is known as an SSD.



## Important

To improve output performance when executing the **show cli history** command, this command displays the **config** command but not the individual CLI commands within the config file.

## Product

All

## Privilege

All

## Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

## Syntax Description

```
show support details [ force ] [ to file url ] [ compress ] [ icsr ] [
no-bulkstats ] [ vpn-npu ]
[ -noconfirm ] [ | { grep grep_options | more } ]
```

### force

Overrides an currently running **show support details** command.



## Important

To avoid a possible file collision with the output of a currently running SSD, use a different target URL file (*force\_url*) for the forced SSD.

### to file url

Specifies the location where a .tar file with the support detail information should be created. *url* may refer to a local or a remote file and must be entered using the following format:

For the ASR 5000:

```
[ file: ] { /flash | /pcmcial | /hd } [ /directory ] /file_name [ compress ]
```

```
tftp:// { host [ :port# ] } [ /directory ] /file_name
```

```
[ ftp: | sftp: ] // [ username[:password] @ ] { host } [ :port# ] [ /directory
] /file_name
```

For the ASR 5500:

```
[ file: ] { /flash | /usb1 | /hd } [ /directory ] /file_name [ compress ]
```

```
tftp:// { host [ :port# ] } [ /directory ] /file_name
```

```
[ ftp: | sftp: ] // [ username[:password] @ ] { host } [ :port# ] [ /directory
] /file_name
```

**Important**

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

*directory* is the directory name.

*filename* is the actual file of interest.

*username* is the user to be authenticated.

*password* is the password to use for authentication.

*host* is the IP address or host name of the server.

*port#* is the logical port number that the communication protocol is to use.

If the filename is not specified with a .tar extension, it is automatically appended to the filename when the file is created and a message is generated.

The .tar file includes:

- **support\_summary** - An ASCII text file that contains the support detail information.
- **information.minicores.tar** - A tar file that contains any minicores files found on the system. Minicores files contain memory core dumps that are captured during some events. These core dumps provide specific memory locations and other information about the event. This information is useful to the technical support team in identifying where and when an event occurred along with its probable cause.

**icsr**

Captures only ICSR-specific information needed for debugging. This keyword reduces the **show support details** (SSD) capture time when debugging ICSR timing issues between the Active and Standby chassis, facilitating quicker resolution of the problem.

See the *Statistics and Counters Reference* for a list of the **show** commands output in the mini SSD for this keyword.

**no-bulkstats**

When the SSD archive is being created in the temporary storage, the bulk statistics samples might occupy a large amount of the storage space. As a result, the SSD archive creation might fail. During such scenarios, use this keyword to exclude the bulkstats samples from the SSD archive.

Also see the **bulkstats ssd-samples** command under the *Global Configuration Mode* chapter for information on enabling bulkstats sample collection in the SSD archive.

**compress**

Generates a compressed .tar.gz file for the output of the command.

**vpn-npu**

Captures only VPN and NPU-specific information needed for debugging. This keyword reduces the SSD capture time and facilitates quicker resolution of the problem. This keyword can be used for any of the other options supported by the **show support details** command.

**-noconfirm**

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

**| { grep *grep\_options* | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on using the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to obtain extensive system information for use in troubleshooting. This command does the work of multiple separate commands, which saves time and ensures that all of the information needed is collected and displayed in the same order every time.

In addition to the information provided, the **show support details** command includes information that is not otherwise accessible to users but that is helpful in the swift resolution of issues.

**Example**

The following command displays the system information on your console.

```
show support details
```

The following command displays the information on your console and also writes it to the local device (pcmcial in this case) and includes the mini core dumps, using the filename *r-p\_problem.tar*:

```
show support details to file /pcmcial/r-p_problem.tar
```

The following command displays the information on your console and also writes it to /flash, placing the file in the **ssd** directory and includes the mini core dumps, using the filename *re\_problem.tar*:

```
show support details to file /flash/ssd/re_problem.tar
```

## show support record

Displays the output of one or more Support Data Records (SDRs) previously saved by the Support Data Collector (SDC). SDRs are displayed in the order of lowest record-id to highest record-id.

---

**Product** All

---

**Privilege** All

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show support record** *record-id* [ **to** *record-id* ] [ **section** *section\_name* ] [ | { **grep** *grep\_options* | **more** } ]



**record-id**

Specifies a record-id as an integer from 0 through 65536.

Each SDR is identified by a time index called the record-id. For example, the most recent record is always record-id 0 (filename = sdr.0.gz). The next older record is record-id 1 (filename = sdr.1.gz), and so on.

When a new record is collected it is given a record-id of 0. The previously most recent record is renamed to record-id 1, and so on. The display includes the record-id along with the collection time-stamp.

**to record-id**

Specifies a the end point of a range of record-ids as an integer from 0 through 65536.

**section section\_name**

Specifies the name of an existing record section as an alphanumeric string of 1 through 64 characters.

**{ grep grep\_options | more }**

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on using the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display the output of one or more SDRs. This information is a useful troubleshooting tool when data is compared chronologically across several SDRs. For additional information refer to the *System Administration Guide*.

**Example**

The following command displays the SDRs from 2 through 4:

```
show support record 2 to 4
```

## show system ssh key status

Displays the fingerprint of the current internal SSH key in use, the source of where the key was found, and the SSH status of all online VMs.

**Product**

VPC-DI

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show system ssh key status [ | { grep grep_options | more } ]
```

**| { grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

#### Usage Guidelines

This command displays information about the SSH keys used for internal communication between all component VMs in a VPC-DI system, such as for remote command execution and file transfers.

## show system uptime

Displays the amount of time the system has been operational since its last down time (maintenance or otherwise).

#### Product

All

#### Privilege

Security Administrator, Administrator, Operator, Inspector

#### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

#### Syntax Description

**show system uptime [ | { grep *grep\_options* | more } ]**

#### uptime

Displays system up time in days (D), hours (H) and minutes (M).

**| { grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

#### Usage Guidelines

Display the system up time to check for the possibility of anomalous behavior related to shorter or longer up times.

#### Example

The following command displays basic system basic information and up time.

```
show system uptime
```

## show sx peers

Displays the Sx peer monitor related parameters.

---

**Product** CUPS

---

**Privilege** All

---

**Command Modes** Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** **show sx peers { full address *peer-ip-address* | wide }**

**full address *peer\_ip\_address***

Displays the monitor related information for the specified Sx peer (for example, VPN context name, group name, and state).

*peer\_ip\_address* is the IP address of the Sx peer.

**wide**

Displays “Monitor State” with the default state being “U” for UP, “D” for Down, and “N” for Not Applicable.

---

**Usage Guidelines** Use this command to display the information about the Sx peer devices and the peer connections.

**Example**

The following command displays the details on peer connections:

```
show sx peers wide
```

■ show sx peers



## CHAPTER 24

# Exec Mode show Commands (T-Z)

The Exec Mode is the initial entry point into the command line interface system. Exec mode **show** commands are useful in troubleshooting and basic system monitoring.

### Command Modes

This chapter includes the commands **show tacacs** through **show version**.

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```



### Important

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

- [show tacacs](#), on page 1207
- [show task](#), on page 1209
- [show tcap statistics](#), on page 1215
- [show temperature](#), on page 1216
- [show terminal](#), on page 1217
- [show threshold](#), on page 1217
- [show transaction-rate](#), on page 1218
- [show url-blacklisting database](#), on page 1219
- [show version](#), on page 1220
- [show wsg-application](#), on page 1222
- [show wsg-lookup](#), on page 1223
- [show wsg-service](#), on page 1223
- [show x2gw-service](#), on page 1224

## show tacacs

Displays information about all active Terminal Access Controller Access-Control System Plus (TACACS+) sessions.

### Product

All

<b>Privilege</b>	Security Administrator, Administrator, Operator, Inspector
<b>Command Modes</b>	Exec The following prompt is displayed in the Exec mode: <code>[local]host_name#</code>
<b>Syntax Description</b>	<b>show tacacs</b> [ <b>client</b>   <b>priv-lvl</b>   <b>session</b> { <b>all</b>   <b>id</b> <i>session_id</i>   <b>idle</b>   <b>statistics</b> }   <b>summary</b> ] [   { <b>grep</b> <i>grep_options</i>   <b>more</b> } ]

### show tacacs

This command provides the following TACACS+ information:

- Individual active session number with the following additional session-specific information:
  - login user name
  - login tty
  - time of login
  - login server priority
  - current session state
  - current privilege level
  - remote client application (if applicable)
  - remote client ip address (if applicable)
  - last server reply status
- Total number of TACACS+ sessions

### [ client | priv-lvl | session | summary ]

Optional filters are available for the output of the **show tacacs** command:

- **client** – Display information about the TACACS+ client.
- **priv-lvl** – Display TACACS+ priv-level authorization attributes for StarOS administrative levels. Only supported in StarOS Release 17.3 and higher.
- **session** – Display information about the TACACS+ sessions.
  - **all** – Displays all TACACS+ sessions with session id, idle threshold, idle time, and application type.
  - **id** *session\_id* – Session ID to be displayed. *session\_id* must be an integer from 1 to 128.
  - **idle** – Lists all idle TACACS+ sessions in the order of most idle sessions.
  - **statistics** – Display statistics about the TACACS+ sessions.
- **summary** – Display summary information about the TACACS+ sessions.

### [ { grep *grep\_options* | more } ]

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view detailed session information for all active TACACS+ sessions.

**Important**

This command is available on version 11.0 and later systems.

**Example**

```
show tacacs
```

# show task

Displays information about system tasks.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show task { info | memory | resources | table } [ card card_num ] [ facility
facility { all | instance id } ] [ process process_name all ] [ max ] [ | {
grep grep_options | more } ]
```

**{ info | memory | resources | table }**

Specifies the type of information to be displayed and scope of tasks to include in output.

**info**: Displays detailed task information.

**memory**: Displays detailed task memory usage information.

**resources**: Displays resource allocation and usage information for all tasks.

**table**: Displays identification information in tabular format for all tasks.

**Note**

In Release 21.1, the Active Health Monitor (AHM) functionality is added to the Resource Manager (RMMGR) to aid in the monitoring of specific processes and proactively collect required debug information at runtime without manual intervention.

When a process enters the “warn” or “over” state for a memory limit, CPU limit, or both, the RMMGR triggers a logging mechanism that proactively collects the memory heap/CPU profiler information, writes it into a file and stores it locally.

The files that are stored locally on the CPU of each individual processing card are then transferred to HD-RAID in the preconfigured directory location.

**card *card\_num***

Default: all powered on cards.

Specifies a single card for which task information is to be displayed where *card\_num* must be an integer from 1 to 48 for the ASR 5000 and 1 to 20 for the ASR 5500.

**facility *facility*{ all | instance *id* max }**

Default: all facilities.

Specifies the list of facilities for which task information may be displayed. A specific instance of the facility may be displayed as specified by ID or all instances may be displayed. The value of *id* must be an integer from 0 to 10000000. *facility* must be one of:

- **a1lmgr**: A11 Interface Manager facility
- **aaamgr**: AAA Manager Facility
- **aaaproxy**: AAA Proxy manager Facility
- **acsctrl**: Active Charging Service (ACS) Controller Facility [Release 11.0 and earlier versions only]
- **acsmgr**: Active Charging Service (ACS) Manager Facility
- **afctrl**: Fabric Manager [ASR 5500 only]
- **afmgr**: Fabric Manager [ASR 5500 only]
- **alcapmgr**: ALCAP Manager
- **asnwmgr**: ASN Gateway Manager
- **asnpcrmgr**: ASN Paging/Location-Registry (ASN-PC) Manager
- **bfd**: Bidirectional Forwarding Detection
- **bgp**: Border Gateway Protocol (BGP) Facility
- **bngmgr**: BNG Manager
- **bulkstat**: Bulk Statistics Manager Facility
- **callhome**: Call Home Controller
- **cdrmod**: Charging Detail Record Module
- **cli**: Command Line Interface Facility
- **connproxy**: Proxy for connections from same card or chassis
- **cspectrl**: Card Slot Port controller Facility
- **cssctrl**: Content Service Steering Controller
- **dcardctrl**: IPsec Daughter-card Controller Logging Facility
- **dcardmgr**: IPsec Daughter-card Manager Logging Facility
- **dgmbmgr**: Diameter Gmb Application Manager
- **dhmgr**: Distributed Host Manager



- **diamproxy**: Diameter Proxy
- **drvctrl**: Driver Controller Facility
- **egtpegmgr**: EGTP Egress Demux Manager
- **egtpinmgr**: EGTP Ingress Demux Manager
- **evlogd**: Event Log Daemon Facility
- **famgr**: Foreign Agent Manager Facility
- **gtpcmgr**: GTP-C Protocol Logging facility (GGSN product only)
- **gtpumgr**: GTP-U Demux Manager
- **h248prt**: H.248 Protocol Task [Release 11.0 and earlier versions only]
- **hamgr**: Home Agent Manager Facility
- **hatcpu**: High Availability Task CPU Facility
- **hatsystem**: High Availability Task Facility
- **hdctrl**: HD Controller
- **henbgwdemux**: Home eNodeB Gateway demux manager




---

**hpat** In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

- **henbgwmgr**: Home eNodeB Gateway Manager




---

**hpat** In Release 20, 21.0 and 21.1, HeNBGW is not supported. This keyword must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

---

- **hnbmgr**: HNBGW HNB Manager




---

**hpat** In Release 20 and later, HNBGW is not supported. This keyword must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

---

- **hwctrl**: Hardware Monitor Controller
- **hwmgr**: Hardware Monitor Manager
- **imsimgr**: SGSN IMSI Manager
- **ipsecctrl**: IP Security Controller Facility

- **ipsecmgr**: IP Security Manager Facility
- **ipsgmgr**: IP Services Gateway Facility
- **kvctrl**: KV Controller
- **kvmgr**: KV Manager
- **l2tpdemux**: L2TP Demultiplexor (LNS) Facility
- **l2tpmgr**: L2TP Manager Facility
- **lagmgr**: Link Aggregation Group (LAG) Manager
- **linkmgr**: SGSN/SS7 Link Manager
- **magmgr**: Mobile Access Gateway Manager
- **megadiammgr**: MegaDiameter Manager
- **mmedemux**: MME Demux Manager logging facility
- **mmemgr**: MME Manager logging facility
- **mmgr**: SGSN/SS7 Master Manager
- **mpls\_sig**: Multiprotocol Label Switching
- **mpctest**: Migration Performance Test on Packet Accelerator Card
- **netwstrg**: Network Storage Manager [Release 11.0 and earlier versions only]
- **npuctrl**: Network Processor Unit Control Facility
- **npudrv**: Network Processor Unit Driver Facility [ASR 5500 only]
- **npumgr**: Network Processor Unit Manager Facility
- **npusim**: Network Processor Unit Simulator [ASR 5500 only]
- **nputst**: Network Processor Unit Tester
- **nsctrl**: Charging Service Controller [Release 11.0 and earlier versions only]
- **nsmgr**: Charging Service Process Manager [Release 11.0 and earlier versions only]
- **orbns**: Object Request Broker Notification Server Facility
- **orbs**: Object Request Broker System Facility
- **ospf**: Open Shortest Path First Facility
- **ospfv3**: Open Shortest Path First (OSPFv3)
- **pdgmgr**: PDG Manager
- **phsgwmgr**: PHS Gateway manager
- **phspcmgr**: PHS Paging Controller manager
- **rct**: Recovery Control Task Facility
- **rdt**: Redirect Task Facility

- **rip**: Routing Information Protocol Facility
- **rmctrl**: Resource Manager Controller Facility
- **rmmgr**: Resource Manager Facility
- **sct**: Shared Configuration Task Facility
- **sessctrl**: Session Controller Facility
- **sessmgr**: Session Manager Facility
- **sesstrc**: Session Trace Collection task
- **sft**: Switch Fabric Monitoring Task
- **sgtpcmgr**: SGSN GTPC Manager
- **sipcdprt**: SIP Call Distributor Task [Release 11.0 and earlier versions only]
- **sitmain**: System Initialization Task Main Facility
- **sitparent**: Card based system initialization facility that applies to the MIO card.
- **snmp**: SNMP Protocol Facility
- **srd**: Static Rating Database
- **testctrl**: Test Controller
- **testmgr**: Test Manager
- **threshold**: Threshold Server Facility
- **vpnctrl**: Virtual Private Network Controller Facility
- **vpnmg**: VPN Manager Facility
- **zebos**: ZEBOS™ OSPF Message Facility

**all**: Displays information for all instances of the specified facility.

**instance *id***: Displays information for the facility instance that is specified as an integer from 0 to 1000000.

#### **process *process\_name* all**

Display information for all instances of the specified process. must be one of the following process names:

- **ftpd**: File Transfer Protocol Daemon
- **inetd**: Internet Superserver Daemon
- **nsproc**: NetSpira Packet Processor
- **ntpd**: Network Time Protocol Daemon
- **orbsnd**: Object Request Broker Notification Server
- **ping**: Ping
- **pvm**: NetSpira Messenger Daemon

- **pvmgs**: NetSpira Messenger Daemon
- **rlogin**: Remote Login
- **sftp-server**: Secure File Transfer Protocol Server
- **sitreap**: System Initialization Task Cleanup Process
- **sn\_resolve**: DNS Resolver Process
- **ssh**: Secure Shell
- **sshd**: Secure Shell Daemon
- **telnet**: Telnet
- **telnetd**: Telnet daemon
- **tftpd**: Trivial File Transfer Protocol Daemon
- **traceroute**: Traceroute

**max**

Default: current usage levels are displayed.

Displays the maximum usage levels for tasks as opposed to the current usage levels.

**max** is valid only along with the **resources** keyword.

**{ grep grep\_options | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Displays task information as part of a system troubleshooting for unexpected behavior.

**Important**

This command is not supported on all platforms.



**Note** The following conditions may cause Shared Configuration Task (SCT) CPU spikes:

- Frequent CLI session initiation that includes both failed and successful session may cause SCT CPU spike.

It is therefore recommended to use an alternate to CLI, such as bulkstats if there is a requirement to view the statistics. Also, avoid exiting CLI sessions and using scripts that initiate CLI sessions.

- “show” commands like “show configuration”.

It is recommended to use the monitoring commands sparingly and only on need-basis.

- Configuration monitoring can drive high CPU usage and also spike the SCT CPU. Note that higher the configuration, higher the CPU usage.

It is recommended to monitor the configuration only when required.

- SDR configuration and periodicity. Periodic data collection adds load to the SCT and to the entire CPU. Therefore, ensure that the SDR is optimally configured. Use the CLI “show configuration collection definition” to check which CLI collections are enabled, review the configuration, and configure only required items.

### Example

The following commands provide some examples of the combinations of options that may be used to display task information.

```
show task info facility hatspc all
show task info facility hatspc instance 456
show task resources facility zebos all
show task table facility ospf
show task table card 8 facility cli all
show task table card 5 facility cli all
show task resources facility rip all max
```

## show tcap statistics

This command displays the collected traffic statistics that have passed through the SS7 Transaction Capabilities Application Part (TCAP) layer.

### Product

SGSN

### Privilege

Security Administrator, Administrator, Operator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show tcap statistics [ camel-service [ all | name camel_srvc ] | map-service
[ all | name map_srvc ] ] [ | { grep grep_options | more } ]
```

**camel-service** [ all | name *camel\_srvc* ]

Displays TCAP statistics for either all Customized Applications for Mobile networks Enhanced Logic (CAMEL) services or only for the named CAMEL service.

**map-service** [ all | name *mapl\_srvc* ]

Displays TCAP statistics for either all Mobile Application Part (MAP) services or only for the named MAP service.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to display the collected TCAP statistics for MAP or CAMEL services.

**Example**

The following command displays the collected statistics for a MAP service named *MAP-Tewk*.

```
show tcap statistics map-service name MAP-Tewk
```

## show temperature

Displays the current temperature on all installed cards. Also displays the temperature of upper and lower fan trays. Temperature readings are acquired from sensors located on these components.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show temperature [ verbose] [ | { grep grep_options | more } ]
```

**| { grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**verbose**

Indicates that the output is to contain detailed information.

**Usage Guidelines**

Verify current temperature of components in chassis.

**Example**

```
show temperature
show temperature verbose
```

## show terminal

Displays the current terminal settings for number of lines in length and number of characters in width.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show terminal [ | { grep grep_options | more } ]
```

```
|{ grep grep_options | more }
```

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to verify current terminal settings in case the output displayed appears to have line breaks/wraps in unexpected places.

**Example**

```
show terminal
```

## show threshold

Displays thresholding information for the system.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`**Syntax Description****show threshold [ default ]****[ default ]**

Used to display the system's thresholding default values.

**Usage Guidelines**

Use this command to display information on threshold value configuration and activity.

**Example**

The following command displays configuration information pertaining to threshold values configured on the system:

**show threshold****Important**Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show transaction-rate

Displays transaction-rate (per sec) for given services.

**Product**

ePDG

PGW

**Privilege**

Security Administrator, Administrator, Inspector, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`**Syntax Description****show transaction-rate { epdg-service | pgw-service | saegw-service [ all | name *svrc\_name* ] } [ | { **grep** *grep\_options* | more } ]****epdg-service**

Displays transaction-rate (per sec) for all or given epdg services.

**pgw-service**

Displays transaction-rate (per sec) for all or given pgw services.



**saegw-service**

Displays transaction-rate (per sec) for all or given SAE-GW services.

**all**

Displays consolidated transaction-rate (per sec) for all epdg / pgw services configured on this system.

**name *svrc\_name***

Displays node level transaction-rate (per sec) for given epdg / pgw service as an alphanumeric string of 1 through 63 characters.

**[ { *grep grep\_options* | *more* } ]**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Syntax Description**

Use this command to display the transaction-rate (per sec) for given services configured on this system.

**Example**

The following command displays the transaction-rate (per sec) for given epdg service by name *epserv1* configured on this system:

```
transaction-rate epdg-service name epserv1
```

## show url-blacklisting database

Displays URL Blacklisting static database configurations.

**Product**

CF

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show url-blacklisting database [ all | url url | facility acsmgr { all | instance instance } ] [ | { grep grep_options | more } ]
```

**all**

Displays configurations of all URL Blacklisting databases present in the default or override directory.

**facility acsmgr { all | instance *instance* }**

Displays configurations of URL Blacklisting database configuration per facility/ACSMgr instance.

**all:** Displays URL Blacklisting database configuration of all ACSMgrs.

**instance *instance*:** Displays URL Blacklisting database configuration for the instance number of the database specified as an integer from 1 through 10000000.

**url *url***

Displays configurations of the URL Blacklisting database specified in the database's URL expressed as an alphanumeric string of 1 through 512 characters.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

Use this command to view configurations associated with in-memory and on-flash Blacklisting database. The **show url-blacklisting database** command displays the active database that is loaded, and is the one set by either the default or override CLI commands.

**Example**

The following command displays configurations of all the databases present in default or override directory, indicating one as Active and rest as Not Loaded:

```
show url-blacklisting database all
```

The following command displays configurations of the */flash/bl/optblk.bin* database:

```
show url-blacklisting database url /flash/bl/optblk.bin
```

The following command displays database configuration for the ACSMgr instance *1*:

```
show url-blacklisting database facility acsmgr instance 1
```

**Important**

Output descriptions for commands are available in the *Statistics and Counters Reference*.

## show version

Displays the version information for the current system image or for a remote image.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show version [ url ] [ all | verbose ] [ | { grep grep_options | more } ]
```

#### *url*

Specifies the location of a configuration file for which to display version information. The *url* may refer to a local or a remote file and must be entered in the following format:

For the ASR 5000:

```
[ file: ] { /flash | /pcmcia1 | /hd } [ /directory ] /file_name
tftp:// { host [ :port# ] } [ /directory ] /file_name
[ http: | ftp: | sftp: ] // [ username [ :password ] @ ] { host } [ :port# ] [
  /directory ] /file_name
```

For the ASR 5500:

```
[ file: ] { /flash | /usb1 | /hd } [ /directory ] /file_name
tftp:// { host [ :port# ] } [ /directory ] /file_name
[ http: | ftp: | sftp: ] // [ username [ :password ] @ ] { host } [ :port# ] [
  /directory ] /file_name
```

For VPC:

```
[ file: ] { /flash | /usb1 | /usb2 /cdrom1 } [ /directory ] /file_name
tftp:// { host [ :port# ] } [ /directory ] /file_name
[ http: | ftp: | sftp: ] // [ username [ :password ] @ ] { host } [ :port# ] [
  /directory ] /file_name
```



### Important

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

*directory* is the directory name.

*filename* is the actual file of interest.

*username* is the user to be authenticated.

*password* is the password to use for authentication.

*host* is the IP address or host name of the server.

*port#* is the logical port number that the communication protocol is to use.

#### **all** | **verbose**

**all**: displays all image information.

**verbose**: displays detailed information.

The **verbose** keyword may not be used in conjunction with a URL specification.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage Guidelines

Display the version information to verify the image versions loaded in preparation for maintenance, upgrades, etc.

You can display additional release build information by running the Exec mode **show build** command.

### Example

The following commands display the version information with the basic level of output and the detailed level, respectively.

```
show version
show version verbose
```

## show wsg-application

Displays wsg-application information.

### Product

SecGW (WSG)

### Privilege

Security Administrator, Administrator, Operator

### Command Modes

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

### Syntax Description

```
show wsg-application ( all | name | application_name [ counter ] [ | {
grep grep_options | more } ] | statistics [ all ] [ name ] [ | { grep grep
options | more } ] ] }
```

#### all

Displays information for all configured application

#### name *application\_name*

Displays specific application. Must be followed by application name which is a string of size 1 through 63.

#### counter

Displays information for all configured application.

**statistics**

Displays information for all configured application.

**[ { grep *grep options* | more } ]**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent. For details on the usage of the grep and more commands, refer to the Regulating a Command's Output section of the Command Line Interface Overview chapter.

**Usage Guidelines**

Use this command to display wsg-application information.

**Example**

The following example displays information for all configured application:

```
show wsg-application statistics
```

## show wsg-lookup

Displays the current priority settings of subnet components for site-to-site tunnels in WSG services.

**Product**

SecGW (WSG)

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show wsg-lookup
```

**Usage Guidelines**

Use this command to display current WSG lookup priority settings,

**Examples**

```
show wsg-lookup
```

## show wsg-service

Displays information about WSG service calls and configured services.

**Product**

SecGW (WSG)

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax Description**

```
show wsg-service ( all | name | srvc_name | statistics [ name srvc_name |
peer-address ip_address ] [ | { grep grep_options | more } ]
```

**all**

Displays information for all configured services.

**name *srvc\_name***

Displays information for the specified service name.

**| statistics [ name *srvc\_name* | peer-address *ip\_address***

Displays information collected for the WSG service since the last VPC-VSM reload or clear command

You can display information for all WSG services (default), for named service or for a specific peer IP address. The peer *ip\_address* can be specified in IPv4 dotted decimal or IPv5 colon-separated hexadecimal notation.

**| { grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage Guidelines**

This command displays information about all or a specified WSG service.

**Example**

The following command displays information about all WSG services:

```
show wsg-service all
```

## show x2gw-service

**Important**

In Release 20, 21.0 and 21.1, HeNBGW is not supported. This command must not be used for HeNBGW in these releases. For more information, contact your Cisco account representative.

This command is used to display the X2GW service related information.

**Product**

HeNBGW

**Privilege**

Security Administrator, Administrator, Operator

**Command Modes**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

---

**Syntax Description** `show x2gw-service { all | enb-association [ all ] | statistics [ sctp | x2ap ] } [ | { grep grep_options | more } ]`

**all**

Displays all the X2GW services.

**enb-association**

Displays the information about (H)ENB associations.

**statistics**

Displays the X2GW service statistics.

**{ grep *grep\_options* | more }**

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage Guidelines**

Use this command to display the X2GW service related information.

**Example**

The following command displays the X2GW service statistics.

```
show x2gw-service statistics
```

■ `show x2gw-service`





## CHAPTER 25

# FA Service Configuration Mode Commands

The Foreign Agent Service Configuration Mode is used to create and manage the Foreign Agent (FA) services associated with the current context.

### Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

**configure** > **context** *context\_name* > **fa-service** *service\_name*

Entering the above command sequence results in the following prompt:

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



### Important

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

- [advertise](#), on page 1228
- [authentication aaa](#), on page 1230
- [authentication mn-aaa](#), on page 1231
- [authentication mn-ha](#), on page 1232
- [bind](#), on page 1233
- [challenge-window](#), on page 1234
- [default subscriber](#), on page 1235
- [dynamic-ha-assignment](#), on page 1236
- [dynamic-mip-key-update](#), on page 1237
- [encapsulation allow gre](#), on page 1238
- [end](#), on page 1238
- [exit](#), on page 1238
- [fa-ha-spi](#), on page 1239
- [gre](#), on page 1241
- [ha-monitor](#), on page 1243
- [idle-timeout-mode](#), on page 1245
- [ignore-mip-key-data](#), on page 1245
- [ignore-stale-challenge](#), on page 1246
- [ip local-port](#), on page 1247
- [isakmp](#), on page 1248
- [limit-reg-lifetime](#), on page 1249

- [max-challenge-len](#), on page 1250
- [mn-aaa-removal-indication](#), on page 1251
- [multiple-reg](#), on page 1252
- [optimize tunnel-reassembly](#), on page 1253
- [private-address allow-no-reverse-tunnel](#), on page 1253
- [proxy-mip](#), on page 1254
- [reg-timeout](#), on page 1256
- [reverse-tunnel](#), on page 1257
- [revocation](#), on page 1258
- [threshold reg-reply-error](#), on page 1259

## advertise

Configures agent advertisement parameters within the FA service.

### Product

PDSN  
GGSN  
ASN-GW

### Privilege

Security Administrator, Administrator

### Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

**configure** > **context** *context\_name* > **fa-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

### Syntax Description

```
advertise {adv-delay seconds | adv-lifetime time | adv-interval { seconds | msec num } | num-adv-sent number | prefix-length-extn | reg-lifetime reg_time }
no advertise { prefix-length-extn | reg-lifetime }
default advertise adv-delay
```

**no**

Disables prefix-length-extn.

**no advertise reg-lifetime**

Specifies that there is no limit to the registration lifetime that the FA service will allow in any Registration Request message from the mobile node.

**default advertise adv-delay**

Sets the initial delay for the unsolicited advertisement to the default value of 1000 ms.

**advertise adv-delay *seconds***

Default: 1000

Sets the initial delay for the unsolicited advertisement.

*seconds* is the advertisement delay in milliseconds and must be an integer from 10 through 5000.



---

**Important**

This command is available for WiMAX CMIP calls only.

---

**adv-lifetime *time***

Default: 9000

Specifies the FA agent advertisement lifetime.

The agent advertisement lifetime is the amount of time that an FA agent advertisement remains valid in the absence of further advertisements.

*time* is measured in seconds and can be configured to an integer from 1 through 65535.

**adv-interval { *seconds* | msec *num* }**

Default: 5 seconds

Specifies the amount of time between agent advertisements.

*seconds* is the time in seconds and can be an integer from 1 through 1800.

**msec *num***: Configures agent advertisement Interval in milliseconds. *num* can be an integer from 100 through 1800000.

**num-adv-sent *number***

Default: 5

Specifies the number of unanswered agent advertisements that the FA service sends upon PPP establishment before rejecting the session.

*number* can be an integer from 1 through 65535.

**prefix-length-extn**

Default: Disabled

When enabled, the FA includes the FA-service address in the Router Address field of the Agent Advertisement and appends a Prefix Length Extension in Agent Advertisements with a prefix length of 32.

**reg-lifetime *reg\_time***

Default: 600

Specifies the longest registration lifetime that the FA service will allow in any Registration Request message from the mobile node.

*reg\_time* is measured in seconds and can be configured to an integer from 1 through 65534.

---

**Usage Guidelines**

Use to tailor FA advertisements to meet your network needs and/or conditions.

**Example**

The following command configures the FA advertisement interval at 10 seconds, the advertise lifetime to 20000 seconds, and the maximum number of unanswered advertisements that will be set to 3.

```
advertise adv-interval 10 adv-lifetime 20000 num-adv-sent 3
```

## authentication aaa

This configuration enables or disables the authentication parameters for the FA service to override dynamic keys from AAA with static keys to support MIP registration with an HA that does not support dynamic keys.

**Product**

FA  
ASN-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ no | default ] authentication aaa-distributed-mip-keys override
```

**no**

Disable the override of dynamic keys from AAA.

**default**

By default the override behavior is disabled and the system uses dynamic keys from AAA after successful EAP authentication. If EAP authentication fails, the system uses static keys by default.

**Usage Guidelines**

Specify how the system will perform authentication of registration request messages. By default dynamic MN-HA and FA-HA keys from AAA after successful EAP authentication used by a PMIP client in WiMAX calls for MIP registration with HA. This configuration in FA service overrides the dynamic keys from AAA with static keys to support MIP registration with an HA that does not support dynamic keys.

**Example**

The following command configures the FA service to override use of AAA MIP keys and force the use of statically configured FA-HA SPI/key for WiMAX calls.

```
authentication aaa-distributed-mip-keys override
```

# authentication mn-aaa

Specifies how the system handles authentication for mobile node re-registrations.

---

## Product

PDSN  
ASN-GW  
GGSN

---

## Privilege

Security Administrator, Administrator

---

## Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

**configure** > **context** *context\_name* > **fa-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

---

## Syntax Description

```
authentication mn-aaa { always | ignore-after-handoff | init-reg |  
init-reg-except-handoff | renew-and-dereg-noauth | renew-reg-noauth } [  
optimize-retries ]
```

### **always**

Specifies that the FA service performs authentication each time a mobile node registers. This is the default setting.

### **ignore-after-handoff**

MN-AAA authentication is not done at the FA for a handoff Access Gateway (AGW).

### **init-reg**

MN-AAA and MN-FAC extensions are required only in initialization RRQ.

### **init-reg-except-handoff**

MN-AAA and MN-FAC extensions are not required in initialization RRQ after inter-Access Gateway (AGW) handoff.

### **renew-and-dereg-noauth**

Specifies that the FA service does not perform authentication for mobile node re-registration or deregistration authorization requests. Initial registration is handled normally.

### **renew-reg-noauth**

Specifies that the FA service does not perform authentication for mobile node re-registrations. Initial registration and de-registration are handled normally.

**optimize-retries**

Optimizes the number of Authentication retries sent to the AAA server.

When an authentication request is pending for a MIP call at the AGW, if a retry RRQ is received from the mobile node, the AGW discards the old RRQ and keeps the most recent RRQ. Subsequently when the authentication succeeds, the AGW forwards the most recent RRQ to the HA. If the authentication fails, the AGW replies to the MN using the most recent RRQ.

**Usage Guidelines**

Use this command to determine how the FA service handles mobile node re-registrations.

The system is shipped from the factory with the mobile AAA authentication set to always.

**Example**

The following command configures the FA service to perform mobile node authentication for every re-registration:

```
authentication mn-aaa always
```

The following command specifies that the FA service does not perform authentication for mobile node re-registrations:

```
authentication mn-aaa renew-reg-noauth
```

## authentication mn-ha

Configures whether the FA service looks for a Mobile Network-Home Agent (MN-HA) authentication extension in the RRP (registration reply).

**Product**

PDSN  
ASN-GW  
GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
authentication mn-ha { allow-noauth | always }
```

**allow-noauth**

Allows a reply that does not contain the auth extension.

**always**

A reply should always contain the auth extension to be accepted.

This is the default setting.

### Usage Guidelines

Use this command to determine whether or not the FA service requires the MN-HA auth extension in the RRP.

The system is shipped from the factory with this set to always.

### Example

The following command configures the FA service to require a reply to contain the authentication extension to be accepted.:

```
authentication mn-ha always
```

## bind

Binds the FA service to a logical IP interface serving as the Pi interface and specifies the maximum number of subscribers that can access this service over the interface.

### Product

PDSN  
ASN-GW  
GGSN  
PDIF

### Privilege

Security Administrator, Administrator

### Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

### Syntax Description

```
bind address address [ max-subscribers count ]
no bind address
```

#### **address**

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

#### **max-subscribers max#**

Default: 500000

Specifies the maximum number of subscribers that can access this service on this interface.

*count* can be configured to an integer from 0 through 500000.

**Important**

The maximum number of subscribers supported is dependant on the license key installed and the number of active packet processing cards installed in the system. Refer to the license key command for additional information.

**Usage Guidelines**

Associate or tie the FA service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an Pi interface. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.

When configuring the **max-subscribers** option, be sure to consider the following:

- The total number of interfaces you will configure for use as Pi interfaces
- The maximum number of subscriber sessions that all of these interfaces may handle during peak busy hours
- The average bandwidth for each of the sessions
- The type of physical port (10/100Base-T or 1000Base-Tx) that these interfaces will be bound to

Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.

Use the **no bind address** command to delete a previously configured binding.

**Example**

The following command would bind the logical IP interface with the address of *192.168.3.1* to the FA service and specifies that a maximum of *600* simultaneous subscriber sessions can be facilitated by the interface/service at any given time.

```
bind address 192.168.3.1 max-subscribers 600
```

The following command disables a binding that was previously configured:

```
no bind address
```

## challenge-window

Defines the number of recently sent challenge values that are considered valid by the FA.

**Product**

PDSN  
ASN-GW  
GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > FA Service Configuration



**configure > context** *context\_name* > **fa-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

---

### Syntax Description

**challenge-window** *number*

***number***

Default: 2

The number of recently sent challenge values that are considered valid. *number* must be an integer from 1 through 5.

---

### Usage Guidelines

Use this command to set the number of recently sent challenge values that are considered valid by the FA.

### Example

Set the challenge window to 3:

```
challenge-window 3
```

## default subscriber

Specifies the name of a subscriber profile configured within the same context as the FA service from which to base the handling of all other subscriber sessions handled by the FA service.

---

### Product

PDSN

ASN-GW

GGSN

PDIF

---

### Privilege

Security Administrator, Administrator

---

### Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

**configure > context** *context\_name* > **fa-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

---

### Syntax Description

[ **no** ] **default subscriber** *profile\_name*

***profile\_name***

Specifies the name of the configured subscriber profile. *profile\_name* is an alphanumeric string of 1 through 63 characters that is case sensitive.

---

### Usage Guidelines

Each subscriber profile specifies "rules" such as permissions, PPP settings, and timeout values.

By default, the FA service will use the information configured for the subscriber named `default` within the same context. This command allows for multiple FA services within the same context to apply different "rules" to sessions they process. Each set of rules can be configured under a different subscriber name which is pointed to by this command.

Use the **no default subscriber** *profile\_name* command to delete the configured default subscriber.

### Example

To configure the FA service to apply the rules configured for a subscriber named *user1* to every other subscriber session it processes, enter the following command:

```
default subscriber user1
```

## dynamic-ha-assignment

This command configures various dynamic HA assignment parameters.

<b>Product</b>	HA
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > Global Configuration > Context Configuration > FA Service Configuration <b>configure</b> > <b>context</b> <i>context_name</i> > <b>fa-service</b> <i>service_name</i> Entering the above command sequence results in the following prompt: <code>[context_name]host_name(config-fa-service)#</code>
<b>Syntax Description</b>	<b>[ default   no ] dynamic-ha-assignment [ aaa-override mn-supplied-ha-addr   allow-failover ]</b>  <b>default</b> Feature is disabled by default.  <b>no</b> Removes the feature and returns it to the default setting of disabled.  <b>aaa-override mn-supplied-ha-addr</b> Enables the system to override the mobile node supplied HA IP address with the AAA provided HA address.  <b>allow-failover</b> Enables/disables a failover retry for dynamic HA assignment from the AAA server.
<b>Usage Guidelines</b>	Use this command to override the mobile node supplied HA IP address with the AAA supplied HA address. Use this command to enable or disable the failover feature that allows the system to receive and use a newer HA address from the AAA server in cases where the original HA address is not responding.

A AAA server may assign different HA addresses each time a retransmitted MIP RRQ is authenticated during the MIP session setup. When this configuration is enabled, if the FA gets a new HA address from AAA during setup, it discards the previous HA address and start using the new address. This allows the FA session to connect to an available HA during setup.

### Example

The following command enables the failover feature that allows the system to receive and use a newer HA address from the AAA server:

```
dynamic-ha-assignment allow-failover
```

## dynamic-mip-key-update

When enabled, the FA service processes MIP\_Key\_Update\_Request from the AAA server and allows dynamic MIP key updates (DMUs).

Default: Disabled

---

### Product

PDSN  
ASN-GW  
GGSN

---

### Privilege

Security Administrator, Administrator

---

### Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

---

### Syntax Description

```
[ no ] dynamic-mip-key-update
```

**no**

The FA service rejects MIP\_Key\_Update\_Request from the AAA server, not allowing dynamic MIP key updating to occur and terminates the call.

---

### Usage Guidelines

Use this command to enable or disable the DMU feature in the FA service.

### Example

To enable DMU and allow dynamic updates of MIP keys, enter the following command:

```
dynamic-mip-key-update
```

## encapsulation allow gre

Enables or disables the use of generic routing encapsulation (GRE) when establishing a Mobile IP (MIP) session. When enabled, if requested by a Mobile Node (MN), the FA requests the HA to use GRE encapsulation when establishing the MIP session. When disabled, the FA does not set the GRE bit in Agent Advertisements to the MN.

Default: GRE is enabled.

<b>Product</b>	PDSN ASN-GW GGSN
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > Global Configuration > Context Configuration > FA Service Configuration <b>configure</b> > <b>context</b> <i>context_name</i> > <b>fa-service</b> <i>service_name</i> Entering the above command sequence results in the following prompt: <pre>[context_name]host_name(config-fa-service)#</pre>
<b>Syntax Description</b>	[ no ] <b>encapsulation allow gre</b>
<b>Usage Guidelines</b>	Use to disable or re-enable the use of GRE encapsulation for MIP sessions.

### Example

To re-enable GRE encapsulation for MIP sessions, enter the following command:

```
encapsulation allow gre
```

## end

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

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Syntax Description</b>	<b>end</b>
<b>Usage Guidelines</b>	Use this command to return to the Exec mode.

## exit

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

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Syntax Description</b>	<b>exit</b>
<b>Usage Guidelines</b>	Use this command to return to the parent configuration mode.

## fa-ha-spi

Configures the security parameter index (SPI) between the FA service and the HA.

<b>Product</b>	PDSN ASN-GW GGSN PDIF
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > Global Configuration > Context Configuration > FA Service Configuration <b>configure &gt; context</b> <i>context_name</i> > <b>fa-service</b> <i>service_name</i> Entering the above command sequence results in the following prompt: [ <i>context_name</i> ]host_name(config-fa-service)#
<b>Syntax Description</b>	<p><b>fa-ha-spi remote-address</b> { <i>ha_ip_address</i>   <i>ip_addr_mask_combo</i> } <b>spi-number</b> <i>number</i>  { <b>encrypted secret</b> <i>enc_secret</i>   <i>secret</i> } [ <b>description string</b>    <b>hash-algorithm</b> { <b>hmac-md5</b>   <b>md5</b>   <b>rfc2002-md5</b> }   <b>monitor-ha</b>    <b>replay-protection</b> { <b>timestamp</b>   <b>nonce</b> }   <b>timestamp-tolerance</b> <i>tolerance</i> ]  <b>no fa-ha-spi remote-address</b> { <i>ha_ip_address</i>   <i>ip_addr_mask_combo</i> } <b>spi-number</b>  <i>number</i></p> <p><b>remote-address</b> { <i>ha_ip_address</i>   <i>ip_addr_mask_combo</i> }</p> <p><i>ha_ip_address</i>: Specifies the IP address of the HA in IPv4 dotted-decimal notation.</p> <p><i>ip_addr_mask_combo</i>: Specifies the IP address of the HA including network mask bits. <i>ip_addr_mask_combo</i> must be specified IPv4 dotted-decimal notation with CIDR subnet mask bits (x.x.x.x/xx).</p> <p><b>spi-number</b> <i>number</i></p> <p>Specifies the Security Parameter Index (SPI) which indicates a security context between the FA and the HA in accordance with RFC 2002.</p> <p><i>number</i> can be configured to an integer from 256 through 4294967295.</p> <p><b>encrypted secret</b> <i>enc_secret</i>   <b>secret</b> <i>secret</i></p> <p>Configures the shared-secret between the FA service and the HA. The secret can be either encrypted or non-encrypted.</p>

- **encrypted secret** *enc\_secret* : Specifies the encrypted shared key (*enc\_secret*) between the FA service and the HA. *enc\_secret* must be an alphanumeric string of 1 through 254 characters that is case sensitive.

**Important**

The **encrypted** keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **secret** keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.

- **secret** *secret*: Specifies the shared key (*secret*) between the FA service and the HA. *secret* must be an alphanumeric string of 1 through 127 characters that is case sensitive.

**description string**

This is a description for the SPI. *string* must be an alphanumeric string of 1 through 31 characters.

**hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }**

Default: hmac-md5

Specifies the hash-algorithm used between the FA service and the HA.

- **hmac-md5**: Configures the hash-algorithm to implement HMAC-MD5 per RFC 2002bis.
- **md5**: Configures the hash-algorithm to implement MD5 per RFC 1321.
- **rfc2002-md5**: Configures the hash-algorithm to implement keyed-MD5 per RFC 2002.

**monitor-ha**

Default: disabled

Enables the HA monitor feature for this HA address.

To set the behavior of the HA monitor feature, refer to the **ha-monitor** command in this chapter. To disable this command (if enabled) for this HA address, re-enter the entire **fa-ha-spi** command without the **monitor-ha** keyword.

**replay-protection { timestamp | nonce }**

Default: timestamp

Specifies the replay-protection scheme that should be implemented by the FA service for this SPI.

- **nonce**: Configures replay protection to be implemented using NONCE per RFC 2002. Nonce is an arbitrary number used only once to sign a cryptographic communication.
- **timestamp**: Configures replay protection to be implemented using timestamps per RFC 2002.

**Important**

This keyword should only be used in conjunction with Proxy Mobile IP support.

**timestamp-tolerance *tolerance***

Default: 60

Specifies the allowable difference (tolerance) in timestamps that is acceptable. If the difference is exceeded, then the session will be rejected. If this is set to 0, then timestamp tolerance checking is disabled at the receiving end.

*tolerance* is measured in seconds and can be configured to an integer value from 0 through 65535.

**Important**

This keyword should only be used in conjunction with Proxy Mobile IP support.

+

More than one of the above keywords can be entered within a single command.

**Usage Guidelines**

An SPI is a security mechanism configured and shared by the FA service and the HA. Please refer to RFC 2002 for additional information.

Though it is possible for FAs and HAs to communicate without SPIs being configured, the use of them is recommended for security purposes. It is also recommended that a "default" SPI with a remote address of 0.0.0.0/0 be configured on both the HA and FA to prevent hackers from spoofing addresses.

**Important**

The SPI configuration on the HA must match the SPI configuration for the FA service on the system in order for the two devices to communicate properly.

A maximum of 2,048 SPIs can be configured per FA service.

Use the **no** version of this command to delete a previously configured SPI.

**Example**

The following command configures the FA service to use an SPI of 512 when communicating with an HA with the IP address 192.168.0.2. The key that would be shared between the HA and the FA service is q397F65. When communicating with this HA, the FA service will also be configured to use the *rfc2002-md5* hash-algorithm.

```
fa-ha-spi remote-address 192.168.0.2 spi-number 512 secret q397F65
hash-algorithm rfc2002-md5
```

The following command deletes the configured SPI of 400 for an HA with an IP address of 172.100.3.200:

```
no fa-ha-spi remote-address 172.100.3.200 spi-number 400
```

**gre**

Configures Generic Routing Encapsulation (GRE) parameters.

<b>Product</b>	PDSN ASN-GW GGSN
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > Global Configuration > Context Configuration > FA Service Configuration <b>configure</b> > <b>context</b> <i>context_name</i> > <b>fa-service</b> <i>service_name</i> Entering the above command sequence results in the following prompt: <pre>[context_name]host_name(config-fa-service)#</pre>
<b>Syntax Description</b>	<pre><b>gre</b> { <b>checksum</b>   <b>checksum-verify</b>   <b>reorder-timeout</b> <i>timeout</i>   <b>sequence-mode</b>   { <b>none</b>   <b>reorder</b> }   <b>sequence-numbers</b> } <b>no gre</b> { <b>checksum</b>   <b>checksum-verify</b>   <b>sequence-numbers</b> }</pre> <p><b>no</b> Disables the specified functionality.</p> <p><b>checksum</b> Default: disabled Enables the introduction of the checksum field in outgoing GRE packets.</p> <p><b>checksum-verify</b> Default: disabled Enables verification of the GRE checksum (if present) in incoming GRE packets.</p> <p><b>reorder-timeout</b> <i>timeout</i> Default: 100 Configures maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets. <i>timeout</i> must be an integer from 0 through 5000.</p> <p><b>sequence-mode</b> { <b>none</b>   <b>reorder</b> } Default: none Configures how incoming out-of-sequence GRE packets should be handled. <b>none</b>: Disables reordering of incoming out-of-sequence GRE packets. <b>reorder</b>: Enables reordering of incoming out-of-sequence GRE packets.</p> <p><b>sequence-numbers</b> Default: Disabled. Enables insertion or removal of GRE sequence numbers in GRE packets.</p>



**Usage Guidelines**

Use this command to configure how the FA service handles GRE packets.

**Example**

To set maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets to 500 milliseconds, enter the following command:

```
gre reorder-timeout 500
```

To enable the reordering of incoming out of sequence GRE packets, enter the following command:

```
gre sequence-mode reorder
```

## ha-monitor

Configures the behavior of the HA monitor feature.

**Product**

PDSN  
ASN-GW  
FA  
HA

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ default ] ha-monitor [ interval sec | max-inactivity-time sec | num-retry num ]  
no ha-monitor
```

**default**

Restores the system default setting(s) for the command/keyword(s). This command is disabled by default.

**no**

Disables the HA monitoring feature for this FA service.

**interval *sec***

Default: 30

Configures the time interval before the next monitoring request message is sent to the HA.

*sec* must be an integer from 1 through 36000.

**max-inactivity-time sec**

Default: 60

Specifies the maximum amount of time the system will wait without receiving MIP control traffic from a HA before the HA monitoring mechanism is triggered.

*sec* must be an integer from 30 through 600.

**num-retry num**

Default: 5

Configures the number of time the system will attempt to send HA monitor requests before determining the HA is down and a trap is initiated.

*num* must be an integer from 0 through 10.

**Usage Guidelines**

Use this command to set parameters for the HA monitor feature. This feature allows the AGW/FA to monitor HAs with which it has MIP sessions. The monitoring feature is triggered when the AGW/FA does not receive any MIP traffic from a HA for a configured amount of time (**max-inactivity-time**). The AGW/FA starts sending special MIP RRQ monitor messages and waits for RRP monitor message responses from the HA. The RRQ monitor messages are addressed to the HA service address. The source address of the monitor-request messages is the FA service's IP address.

The actions taken during monitoring are comprised of the following:

- If no monitor response is received during the interval time (**interval**), the AGW retransmits the monitor message a configured number of times (**num-retry**).
- If no response is received after retransmitting for the number configured in **num-retry**, the HA is considered down. The AGW/FA sends a trap (HAUnreachable) to the management station. Monitoring of this HA is stopped until a MIP control message is received from the particular HA and when the AGW/FA sends a trap (HAreachable) to the management station and starts monitoring the HA again.
- When an HA receives the RRQ from an FA, it verifies the message and identifies it as a monitor message based on a special reserved NAI (in the message) and a Monitor HA CVSE in the RRQ. The HA responds with an RRP with Reply code 0x00 (accepted) and includes the Monitor HA CVSE. When the FA receives the RRP from the HA, it updates the activity for the peer HA to maintain the "up" state.

**Important**

This command only sets the behavior of the HA monitor feature. To enable the HA monitor feature for each HA address, refer to the **fa-ha-spi** command in this chapter. Up to 256 HAs can be monitored per system.

**Example**

The following commands set the HA monitor message interval to 45 seconds, the HA inactivity time to 60 seconds, and the number of HA monitor retries to 6:

```
ha-monitor interval 45
ha-monitor max-inactivity-time 60
ha-monitor num-retry 6
```

## idle-timeout-mode

Controls whether Mobile IP data and control packets or only Mobile IP data resets the session idle timer.

---

**Product**

PDSN  
ASN-GW  
GGSN  
PDIF

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > Global Configuration > Context Configuration > FA Service Configuration

**configure** > **context** *context\_name* > **fa-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description**

**idle-timeout-mode** { **aggressive** | **normal** }

**aggressive**

Only Mobile IP data resets the session idle timer.

**normal**

Both Mobile IP data and control packets reset the session idle timer.

---

**Usage Guidelines**

Use this command to control how the session idle timer is reset.

**Example**

The following command specifies that only Mobile IP data can reset the session idle timer:

```
idle-timeout-mode aggressive
```

## ignore-mip-key-data

When this command is enabled, if the Dynamic Mobile IP Key Update (DMU) is not enabled and the mobile node (MN) sends a MIP\_Key\_Data CVSE, the FA ignores the MIP\_Key\_Data extension and the call is continued like a regular Mobile IP (MIP) call.

---

**Product**

PDSN  
GGSN

---

**Privilege**

Security Administrator, Administrator

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

**configure** > **context** *context\_name* > **fa-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description** [ no ] **ignore-mip-key-data**

**no**

Disable ignoring of MIP key data.

**Usage Guidelines** When DMU is not enabled, use this command to ignore MIP key data sent by the MN and allow the call to continue normally.

#### Example

To enable the FA to ignore MIP key data sent by the MN, enter the following command:

```
ignore-mip-key-data
```

## ignore-stale-challenge

Enables the system to accept RRQs with previously used challenges. This feature is disabled by default.

**Product** PDSN  
GGSN

**Privilege** Security Administrator, Administrator

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

**configure** > **context** *context\_name* > **fa-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description** [ no ] **ignore-stale-challenge**

**no**

Disables this feature. If an RRQ is received with a previously used challenge and there are RRQs pending on the same session, accept the RRQ if it has a new Identification in the retransmitted RRQ. All other RRQs received with previously used challenge are rejected with the Stale Challenge (106) error code.

**Usage Guidelines** Use this command to allow the FA to accept stale challenges regardless of the ID field or if other RRQs are pending.

**Example**

To enable this functionality in the FA service, enter the following command;

```
ignore-stale-challenge
```

To disable this functionality, enter the following command;

```
no ignore-stale-challenge
```

## ip local-port

Configures the local User Datagram Protocol (UDP) port for the Pi interfaces' IP socket on which to listen for Mobile IP Registration messages.

**Product**

PDSN

ASN-GW

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
ip local-port port#
```

***port#***

Specifies the UDP port number.

*port#* can be an integer from 1 through 65535.

**Usage Guidelines**

Specify the UDP port that should be used for communications between the FA service and the HA.

The system defaults to using local port 434.

**Example**

The following command specifies a UDP port of 3950 for FA-to-HA communication on the Pi interface:

```
ip local-port 3950
```

# isakmp

Configures support for IPSec within the FA-service.

---

## Product

PDSN  
ASN-GW  
GGSN

---

## Privilege

Security Administrator, Administrator

---

## Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

**configure** > **context** *context\_name* > **fa-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

---

## Syntax Description

```
isakmp {peer-ha ha_address { crypto map map_name [ [ encrypted ] secret secret ] } | default { crypto map map_name [ [ encrypted ] secret secret ] } }  
no isakmp { peer-ha peer_ip_address | default }
```

### no

Deletes the reference to the crypto map for the specified HA, or deletes the reference for the default crypto map.

**peer-ha** *ha\_address*{ **crypto map** *map\_name* [ [ **encrypted** ] **secret** *preshared\_secret* ] }

Configures a crypto map for a peer HA.

- *ha\_address*: The IP address of the HA with which the FA service will establish an IPSec SA. The address must be expressed in IPv4 dotted-decimal format.
- **crypto map** *map\_name*: The name of a crypto map configured in the same context that defines the IPSec tunnel properties. *map\_name* is the name of the crypto map expressed as an alphanumeric string of 1 through 127 characters.
- **encrypted**: This keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **secret** keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.
- **secret** *secret*: The pre-shared secret that will be used during the IKE negotiation. *preshared\_secret* is the secret expressed as an alphanumeric string of 1 through 127 characters.

**default** { **crypto map** *map\_name* [ [ **encrypted** ] **secret** *secret* ] }

Specifies the default crypto map to use when there is no matching crypto map configured for an HA address.

- **crypto map** *map\_name*: The name of a crypto map configured in the same context that defines the IPSec tunnel properties. *map\_name* is the name of the crypto map expressed as an alphanumeric string of 1 through 127 characters.

- **encrypted**: This keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **secret** keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.
- **secret** *secret*: The pre-shared secret that will be used during the IKE negotiation. *preshared\_secret* is the secret expressed as an alphanumeric string of 1 through 127 characters.

### Usage Guidelines

Use this command to configure the FA-service's per-HA IPSec parameters. These dictate how the FA service is to establish an IPSec SA with the specified HA.



#### Important

For maximum security, the above command should be executed for every possible HA with which the FA service communicates.

A default crypto map can also be configured using the default keyword. The default crypto map is used in the event that the AAA server returns an HA address that is not configured as an isakmp peer-ha.



#### Important

For maximum security, the default crypto map should be configured in addition to peer-ha crypto maps instead of being used to provide IPSec SAs to all HAs.

Note that once an IPSec tunnel is established between the FA and HA for a particular subscriber, all new Mobile IP sessions using the same FA and HA are passed over the tunnel regardless of whether or not IPSec is supported for the new subscriber sessions. Data for existing Mobile IP sessions is unaffected.

### Example

The following command creates a reference for an HA with the IP address *10.2.3.4* to a crypto map named *map1*:

```
isakmp peer-ha 10.2.3.4 crypto map map1
```

The following command deletes the crypto map reference for the HA with the IP address *10.2.3.4*.

```
no isakmp peer-ha 10.2.3.4
```

## limit-reg-lifetime

Enable the current default behavior of limiting the Mobile IP (MIP) lifetime to be smaller than the Idle, Absolute, or Long Duration timeouts. When disabled, this command allows a MIP lifetime that is longer than the Idle, Absolute or Long Duration timeouts.

### Product

PDSN  
ASN-GW  
GGSN  
PDIF

<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > Global Configuration > Context Configuration > FA Service Configuration <b>configure &gt; context</b> <i>context_name</i> > <b>fa-service</b> <i>service_name</i> Entering the above command sequence results in the following prompt: <pre>[context_name]host_name(config-fa-service)#</pre>
<b>Syntax Description</b>	<b>[ no   default ] limit-reg-lifetime</b>  <b>no</b> Allows a MIP lifetime that is longer than the Idle, Absolute or Long Duration timeouts.  <b>default</b> Enables the default behavior of limiting the MIP lifetime to be smaller than the Idle, Absolute, or Long Duration timeouts.
<b>Usage Guidelines</b>	Use the no keyword with this command to allow a MIP lifetime that is longer than the Idle, Absolute or Long Duration timeouts.  Use the base command or the keyword to reset the FA service to the default behavior of limiting the MIP lifetime to be smaller than the Idle, Absolute, or Long Duration timeouts.  <b>Example</b> Configure the FA service to allow a MIP lifetime that is longer than the Idle, Absolute or Long Duration timeouts by entering the following command: <b>no limit-reg-lifetime</b>  Configure the FA service to the default behavior of limiting the MIP lifetime to be smaller than the Idle, Absolute, or Long Duration timeouts by entering either of the following commands: <b>default limit-reg-lifetime</b> <b>limit-reg-lifetime</b>

## max-challenge-len

For mobile subscribers, the FA generates a random number and sends it to the mobile node as part of the mobile authentication extension (Mobile-Foreign Authentication extension) as described in RFC 3012. This command sets the maximum length of the FA challenge in bytes.

<b>Product</b>	PDSN ASN-GW GGSN
<b>Privilege</b>	Security Administrator, Administrator



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

**configure > context** *context\_name* > **fa-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description** **max-challenge-len** *length*

**length**

Default: 16

The maximum length, in bytes, of the FA challenge. This value must be an integer from 4 through 32.

**Usage Guidelines** Change the maximum allowed length of the randomly generated FA challenge its default of 16.

#### Example

Use the following command to change the maximum length of the FA challenge to 18 bytes:

```
max-challenge-len 18
```

## mn-aaa-removal-indication

Enables the FA to remove the Mobile Network-Final Assembly Code (MN-FAC) and MN-AAA extensions from RRQs. This is disabled by default.

**Product** PDSN

ASN-GW

GGSN

**Privilege** Security Administrator, Administrator

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

**configure > context** *context\_name* > **fa-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description** [ **no** ] **mn-aaa-removal-indication**

**no**

Disable the removal of the MN-FAC and MN-AAA extensions from RRQs.

**Usage Guidelines** Enable this feature if there is no need to authenticate the subscriber at HA using MN-AAA extension.

**Example**

The following command enables the FA service to remove MN-FAC and MN-AAA extensions from RRQs:

```
mn-aaa-removal-indication
```

# multiple-reg

Specifies the number of simultaneous Mobile IP sessions that will be supported for over a single PPP session.

**Product**

PDSN  
ASN-GW  
GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
multiple-reg number
```

***number***

*number* can be configured to an integer from 1 through 3.

**Usage Guidelines**

Use to support multiple registrations per subscriber.

The system defaults to a setting of "1" for multiple simultaneous MIP sessions.

**Important**

The system will only support multiple Mobile IP sessions per subscriber if the subscriber's mobile node has a static IP address. The system will only allow a single Mobile IP session for mobile nodes that receive a dynamically assigned IP address. In addition, because only a single Mobile IP or proxy-Mobile IP session is supported for IP PDP contexts, this parameter must remain at its default configuration.

**Example**

The following command configures the number of supported simultaneous registrations for subscribers using this FA service to 3.

```
multiple-reg 3
```

# optimize tunnel-reassembly

Configures FA to HA optimization for tunnel reassembly.

---

**Product**

PDSN  
ASN-GW  
GGSN

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > Global Configuration > Context Configuration > FA Service Configuration

**configure** > **context** *context\_name* > **fa-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description**

[ **no** ] **optimize tunnel-reassembly**

---

**Usage Guidelines**

Enabling this functionality fragments large packets prior to encapsulation for easier processing. Tunnel reassembly optimization is disabled by default.


**Important**

You should not use this command without first consulting Cisco Systems Technical Support. This command applies to very specific scenarios where packet reassembly is not supported at the far end of the tunnel. There are cases where the destination network may either discard the data, or be unable to reassemble the packets.


**Important**

This functionality works best when the FA service is communicating with an HA service running in a system. However, an FA service running in the system communicating with an HA from a different manufacturer will operate correctly even if this parameter is enabled.

Use the **no** version of this command to disable tunnel optimization if it was previously enabled.

---

**Example**

The following command enables tunnel reassembly optimization:

```
optimize tunnel-reassembly
```

# private-address allow-no-reverse-tunnel

This command enables the FA to allow calls with private addresses and no reverse tunneling.

---

**Product**

PDSN

ASN-GW

GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec &gt; Global Configuration &gt; Context Configuration &gt; FA Service Configuration

**configure** > **context** *context\_name* > **fa-service** *service\_name*

Entering the above command sequence results in the following prompt:

*[context\_name]*host\_name(config-fa-service)#**Syntax Description****[ no ] private-address allow-no-reverse-tunnel****no**

Disables the functionality. This is the default setting.

**Usage Guidelines**

Use this command to let the FA allow sessions with private addresses that do not have the reverse tunnel bit set.

**Example**

To enable sessions with private addresses and no reverse tunneling, enter the following command:

**private-address allow-no-reverse-tunnel**

## proxy-mip

Configures parameters pertaining to Proxy Mobile IP support.

**Product**

PDSN

ASN-GW

GGSN

PDIF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec &gt; Global Configuration &gt; Context Configuration &gt; FA Service Configuration

**configure** > **context** *context\_name* > **fa-service** *service\_name*

Entering the above command sequence results in the following prompt:

*[context\_name]*host\_name(config-fa-service)#**Syntax Description****proxy-mip** { **allow** | **ha-failover** [ **max-attempts** *max\_attempts* | **num-attempts-before-switching** *num\_attempts* | **timeout seconds** ] | **max-retransmissions** *number* | **renew-percent-time** *renew-time* | **retransmission-timeout** *time* }

```
no proxy-mip {allow | ha-failover }
default proxy-mip { allow | ha-failover | max-retransmissions |
renew-percent-time | retransmission-timeout }
```

**no**

Disables FA service support for Proxy Mobile IP or HA failover for Proxy Mobile IP.

**default**

Restores the specified option to the default setting as described below.

**allow**

Default: Disabled

Enables FA service support for Proxy Mobile IP.

```
ha-failover [max-attempts max_attempts | num-attempts-before-switching num_attempts | timeout seconds
]
```

Default: Disabled

Enables HA failover for the Proxy Mobile IP feature.

- **max-attempts** *max\_attempts* - Configures the maximum number of retransmissions of Proxy MIP control messages. *max\_attempts* must be an integer from 1 through 10. Default is 4
- **num-attempts-before-switching** *num\_attempts* - Configures the total number of RRQ attempts (including retransmissions) before failing over to the alternate HA. *num\_attempts* must be an integer from 1 through 5. Default is 2.
- **timeout** *seconds* - Configures the retransmission timeout (in seconds) of Proxy MIP control messages when failover happens. *seconds* must be an integer from 1 through 50. Default is 2

**max-retransmissions** *number*

Default: 5

Configures the maximum number re-try attempts that the FA service is allowed to make when sending Proxy Mobile IP Registration Requests to the HA.

*number* is the maximum number of retries and can be configured to an integer from 1 through 4294967295.

**renew-percent-time** *renew-time*

Default: 75

Configures the amount of time that must pass prior to the FA sending a Proxy Mobile IP Registration Renewal Request.

*renew-time* is entered as a percentage of the advertisement registration lifetime configured for the FA service. (Refer to the **advertise** command in this chapter). *renew-time* can be configured to an integer from 1 through 100.

The following equation can be used to calculate *renew-time*:

$$\text{renew-time} = (\text{duration} / \text{lifetime}) * 100$$

*duration* = The desired amount of time that can pass prior to the FA sending a Proxy Mobile IP Registration Renewal Request

*lifetime* = The advertisement registration lifetime configured for the FA service.

*duration* / *lifetime*

#### **retransmission-timeout *time***

Default: 3

Configures the maximum amount of time allowed by the FA for a response from the HA before re-sending a Proxy Mobile IP Registration Request message.

*time* is measured in seconds and can be configured to an integer from 1 through 100.

#### **Usage Guidelines**

The **proxy-mip** command and its keywords configure the FA services support for Proxy Mobile IP.

When enabled through the session license and feature use key, the system supports Proxy Mobile IP to provide a mobility solution for subscribers with mobile nodes (MNs) capable of supporting only Simple IP.

In addition to the parameters configured via this command, the HA-FA SPI(s) must also be modified to support Proxy Mobile IP. Refer to the **fa-ha-spi** command for more information.

#### **Example**

The following command configures the FA service to wait up to 5 seconds for an HA to respond prior to re-sending an a Mobile IP Registration Request message:

```
proxy-mip retransmission-timeout 5
```

If the advertisement registration lifetime configured for the FA service is 900 seconds and you want the system to send a Proxy Mobile IP Registration Renewal Request message after 500 seconds, then the following command must be executed:

```
proxy-mip renew-percent-time 50
```

Note that 50 = (450 / 900) 100.

## reg-timeout

Configures the FA registration reply timeout.

#### **Product**

PDSN

ASN-GW

GGSN

PDIF

#### **Privilege**

Security Administrator, Administrator

#### **Command Modes**

Exec > Global Configuration > Context Configuration > FA Service Configuration

**configure** > **context** *context\_name* > **fa-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description**

**reg-timeout** *time*

**time**

Default: 45

time is measured in seconds and can be configured to an integer from 1 through 65535.

---

**Usage Guidelines**

Configure the amount of time that the FA service will wait for a Registration Reply from an HA before the call is rejected with a reply code of 78H (registration Timeout).

**Example**

The following command configures a registration timeout of 10.

```
reg-timeout 10
```

## reverse-tunnel

Enables the use of reverse tunneling for a Mobile IP (MIP) sessions when requested by the mobile node (MN).

---

**Product**

PDSN

ASN-GW

GGSN

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > Global Configuration > Context Configuration > FA Service Configuration

**configure** > **context** *context\_name* > **fa-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description**

[ **no** ] **reverse-tunnel**

**no**

Indicates the reverse tunnel option is to be disabled. When omitted, the reverse tunnel option is enabled.

---

**Usage Guidelines**

Reverse tunneling involves tunneling datagrams originated by the MN to the HA via the FA service.

When an MN arrives at a foreign network, it listens for agent advertisements and selects an FA that supports reverse tunnels. The MN requests this service when it registers through the selected FA. At this time, the MN may also specify a delivery technique such as Direct or the Encapsulating Delivery Style.

The advantages of using reverse-tunneling:

- All datagrams from the mobile node seem to originate from its home network
- The FA can keep track of the HA that the mobile node is registered to and tunnel all datagrams from the mobile node to its HA

Use the **no** option of this command to disable reverse tunneling. If reverse tunneling is disabled, and the mobile node does not request it, then triangular routing is used.

The system defaults to reverse tunnel enabled.



### Important

If reverse tunneling is disabled on the system and an MN requests it, the call will be rejected with a reply code of 74H (reverse-tunneling unavailable).

### Example

The following command disables reverse-tunneling support for the FA service:

```
no reverse-tunnel
```

## revocation

Enables the MIP revocation feature and configures revocation parameters.

### Product

PDSN  
ASN-GW  
GGSN  
PDIF

### Privilege

Security Administrator, Administrator

### Command Modes

Exec > Global Configuration > Context Configuration > FA Service Configuration

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

Entering the above command sequence results in the following prompt:

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

### Syntax Description

```
revocation { enable | max-retransmission number | negotiate-i-bit |
retransmission-timeout secs | trigger internal-failure }
no revocation enable | trigger internal-failure | negotiate-i-bit
```

### no

Completely disables registration revocation on the FA.

Disables sending revocation messages to the HA when a session is affected by an internal task failure.



**enable**

Enables the MIP registration revocation feature on the FA. When enabled, if revocation is negotiated with an HA, and a MIP binding is terminated, the FA can send a Revocation message to the HA. This feature is disabled by default.

**max-retransmission *number***

Default: 3

Specifies the maximum number of retransmissions of a Revocation message before the revocation fails. *number* must be an integer from 0 through 10.

**negotiate-i-bit**

Default: disabled

Enables the FA to negotiate the i-bit via PRQ/RRP messages and processes the i-bit revocation messages.

**retransmission-timeout *secs***

Default: 3

Specifies the number of seconds to wait for a Revocation Acknowledgement from the HA before retransmitting the Revocation message. *secs* must be an integer from 1 through 10.

**trigger internal-failure**

Default: disabled

Enable sending a revocation message to the HA for all sessions that are affected by an internal task failure.

---

**Usage Guidelines**

Use this command to enable or disable the MIP revocation feature on the FA or to change settings for this feature. Both the HA and the FA must have Registration Revocation enabled and FA/HA authorization must be in use for Registration Revocation to be negotiated successfully.

**Example**

The following command enables Registration Revocation on the FA:

```
revocation enable
```

The following command sets the maximum number of retries for a Revocation message to 6:

```
revocation max-retransmission 6
```

The following command sets the timeout between retransmissions to 10:

```
revocation retransmission-timeout 10
```

## threshold reg-reply-error

Set an alarm or alert based on the number of registration reply errors per FA service.

---

**Product**

PDSN

ASN-GW  
GGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > FA Service Configuration

**configure** > **context** *context\_name* > **fa-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

**threshold reg-reply-error** *high\_thresh* [ **clear** *low\_thresh* ]  
**no threshold reg-reply-error**

**no**

Deletes the alert or alarm.

**high\_thresh**

Default: 0

The high threshold number of registration reply errors that must be met or exceeded within the polling interval to generate an alert or alarm. *high\_thresh* can be an integer from 0 through 100000.

**Important**

You must enter a value between 1 and 100000 to trigger an alert/alarm.

**clear low\_thresh**

Default:0

The low threshold number of registration reply errors that must be met or exceeded within the polling interval to clear an alert or alarm. *low\_thresh* can be an integer from 0 through 100000.

**Important**

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

**Important**

You must enter a value between 1 and 100000 to trigger an alert/alarm.

**Usage Guidelines**

Use this command to set an alert or an alarm when the number of registration reply errors is equal to or greater than a specified number of calls per second.

Alerts or alarms are triggered for the number of registration reply errors on the following rules:

- **Enter condition:** Actual number of registration reply errors > High Threshold
- **Clear condition:** Actual number of registration reply errors £ Low Threshold

**Example**

The following command configures a registration reply error threshold of *1000* and a low threshold of *500* for a system using the Alarm thresholding model:

```
threshold reg-reply-error 1000 clear 500
```

■ **threshold reg-reply-error**



## CHAPTER 26

# FNG Service Configuration Mode Commands

### Command Modes

The FNG Service Configuration Mode is used to configure the properties required for the Femto Network Gateway (FNG) to interface with the Femto Access Points (FAPs) in the network.

Exec > Global Configuration > Context Configuration > FNG Service Configuration

**configure** > **context** *context\_name* > **fng-service** *service\_name*

Entering the above command sequence results in the following prompt:

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



### Important

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

- [aaa aggregation, on page 1263](#)
- [aaa authentication, on page 1264](#)
- [bind, on page 1265](#)
- [default, on page 1266](#)
- [duplicate-session-detection, on page 1267](#)
- [end, on page 1268](#)
- [exit, on page 1268](#)
- [ip source-violation, on page 1269](#)
- [setup-timeout, on page 1270](#)

## aaa aggregation

Sets the system attributes for A12 aggregation for the FNG service.

### Product

FNG

### Privilege

Security Administrator, Administrator

### Command Modes

Exec > Global Configuration > Context Configuration > FNG Service Configuration

**configure** > **context** *context\_name* > **fng-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

### Syntax Description

```
aaa aggregation { interface type a12 | destination address ipv4_address |
a12-group { context name [ aaa-group name ] | aaa-group name [ context name ]
} }
no aaa aggregation interface type a12
no a12 destination address ipv4_address
no aaa aggregation a12-group { context name [ aaa-group name ] | aaa-group
name [ context name ] }
```

#### aaa aggregation interface type a12

Enables A12 aggregation functionality for the FNG service.

#### aaa aggregation interface a12 destination address ipv4\_address

Adds a destination address for an AN-AAA server for A12 aggregation. A maximum of ten destination addresses can be configured.

#### aaa aggregation a12-group { context name [ aaa-group name ] | aaa-group [ context name ] }

Defines the AAA context and AAA group to be used for A12 aggregation.

If the context name and AAA group are not specified, the FNG defaults to the FNG service context and the default AAA group in that context. If the AAA group is specified but the context is not specified, the FNG uses the FNG service context and the AAA group in that context. If the AAA group is not specified and the context is specified, the FNG uses the default AAA group in that context.

#### no aaa aggregation interface type a12

Disables A12 aggregation functionality for the FNG service.

#### no aaa aggregation a12-destination address ipv4\_address

Deletes the specified destination address for an AN-AAA server.

#### no aaa aggregation a12-group { context name [ aaa-group name ] | aaa-group [ context name ] }

Deletes the specified AAA context and AAA group to be used for A12 aggregation.

### Usage Guidelines

Sets the system attributes for AAA aggregation in the FNG service.

#### Example

The following command enables the A12 functionality for the FNG service:

```
aggregation interface type a12
```

## aaa authentication

Specifies the AAA group to use for FAP authentication.

<b>Product</b>	FNG
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > Global Configuration > Context Configuration > FNG Service Configuration <b>configure &gt; context</b> <i>context_name</i> > <b>fng-service</b> <i>service_name</i> Entering the above command sequence results in the following prompt: [ <i>context_name</i> ]host_name(config-fng-service)#
<b>Syntax Description</b>	<b>aaa authentication { context-name</b> <i>name</i> <b>aaa-group</b> <i>name</i>   <b>context-name</b> <i>name</i> <b>aaa-group</b> <i>name</i> <b>}</b> <b>no aaa authentication</b>  <b>no aaa authentication</b> Removes any existing authentication configuration.  <b>context-name</b> <i>name</i> <b>aaa-group</b> <i>name</i> Specifies the context name and the AAA group name configured in the context for FAP authentication. <b>context-name</b> <i>name</i> : Specifies the context where the AAA server group is defined as an alphanumeric string of 1 through 79 characters. <b>aaa-group</b> <i>name</i> : Specifies the name of the AAA group to be used for authentication as an alphanumeric string of 1 through 63 characters.
<b>Usage Guidelines</b>	Use this command to specify that during IPSec session establishment using IKEv2 setup, the FNG will use Radius AAA for FAP authentication.

**Example**

Use the following to configure device authentication for an AAA group named *aaa-10* in the FNG context named *fng1*:

```
aaa authentication context-name fng1 aaa-group aaa-10
```

## bind

Binds the FNG service IP address to a crypto template and specifies the maximum number of sessions the FNG service supports.

<b>Product</b>	FNG
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > Global Configuration > Context Configuration > FNG Service Configuration <b>configure &gt; context</b> <i>context_name</i> > <b>fng-service</b> <i>service_name</i> Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
bind address ipv4_address { crypto-template string }[ max-sessions number ]  
no bind
```

**no bind**

Removes a previously configured binding.

**address ipv4\_address**

Specifies the IPv4 address of the FNG service.

**crypto-template string**

Specifies the name of the crypto template to be bound to the FNG service.

*string* is any value from 0 - 127 alpha and/or numeric characters.

**max-sessions number**

Specifies the maximum number of sessions to be supported by the FNG service as an integer from 0 through 1000000. Default: 1000000

If the max-sessions value is changed on an existing system, the new value takes effect immediately if it is higher than the current value. If the new value is lower than the current value, existing sessions remain established, but no new sessions are permitted until usage falls below the newly-configured value.

**Usage Guidelines**

Binds the IP address used as the connection point for establishing the IKEv2 sessions to a crypto template. It can also define the maximum number of sessions the FNG can support.

**Example**

The following command binds an FNG service with an IP address of *10.2.3.4* to the crypto template named *T1* and sets the maximum number of sessions to *500000*:

```
bind address 10.2.3.4 crypto-template T1 max-sessions 500000
```

# default

Sets or restores the default condition for the selected parameter.

**Product**

FNG

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > FNG Service Configuration

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

Entering the above command sequence results in the following prompt:

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



**Syntax Description**

```
default { { aaa attribute 3gpp2-service-option } |  
duplicate-session-detection | ip source-violation { drop-limit | period  
} | setup-timeout | subscriber name }
```

**aaa attribute 3gpp2-service-option**

Sets or restores the default value of 4095.

**duplicate-session-detection**

Sets or restores the default option for duplicate session detection to be fapid-based.

**ip source-violation ( drop-limit | period )**

Sets or restores the IP source violation detection defaults, as follows:

**drop-limit:** Sets or restores the maximum number of IP source violations within the detection period before dropping the call to the default value of 10.

**period:** Sets or restores the detection period for IP source violations to the default value of 120 seconds.

**setup-timeout**

Sets or restores the maximum time allowed for session setup to the default value of 60 seconds.

**subscriber *name***

Sets or restores the name of the default subscriber.

*name* is a string of 1-127 characters.

**username mac-address-stripping**

The default behavior is to disable stripping the MAC address from the username.

**Usage Guidelines**

Configures the default settings for a given parameter.

**Example**

Use the following command to set the maximum time allowed for session setup to the default value of 60 seconds:

```
default setup-timeout
```

## duplicate-session-detection

Configures the FNG to detect duplicate call sessions based on Femtocell Access Point (FAP) ID and to clear old call information.

This feature is disabled by default.

**Product**

FNG

**end**


---

**Privilege** Security Administrator, Administrator

---

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

**configure > context** *context\_name* > **fng-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description** **duplicate-session-detection { fapid-based }**  
**no duplicate-session-detection**  
**default duplicate-session-detection**

#### **fapid-based**

Sets the FNG to detect duplicate call sessions based on the FAP ID.

#### **no duplicate-session-detection**

Disables duplicate session detection.

#### **default duplicate-session-detection**

Sets or restores the default option for duplicate session detection to be fapid-based.

---

**Usage Guidelines** By default, duplicate session detection is disabled. Use this command to enable this feature. It applies only to calls established after the feature has been enabled.

The following command enables duplicate session detection based on FAP ID:

```
duplicate-session-detection fapid-based
```

## **end**

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

---

**Product** All

---

**Privilege** Security Administrator, Administrator

---

**Syntax Description** **end**


---

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

## **exit**

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

---

**Product** All

---

**Privilege** Security Administrator, Administrator

---

**Syntax Description**    `exit`

---

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

## ip source-violation

Sets the parameters for IP source validation. Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session.

---

**Product**    FNG

---

**Privilege**    Security Administrator, Administrator

---

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

**configure > context** *context\_name* > **fng-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description**    **ip source-violation** { **clear-on-valid-packet** | **drop-limit** *num* | **period** *secs* }  
**no ip source-violation clear-on-valid-packet**

### **clear-on-valid-packet**

Configures the service to reset the drop-limit counters upon receipt of a properly addressed packet. Default: disabled

### **drop-limit** *num*

Sets the maximum number of allowed IP source violations within the detection period before dropping a call as an integer from 1 through 1000000. Default: 10

### **period** *secs*

Sets the detection period (in seconds) for IP source violations as an integer from 1 through 1000000. Default: 120

---

**Usage Guidelines**    This function allows the operator to configure the network to prevent problems such as when a user gets handed back and forth between two gateways a number of times during a handoff scenario.

When a subscriber packet is received with a source IP address violation, the system increments the IP source violation drop-limit counter and starts the timer for the IP source violation period. Every subsequent packet received with a bad source address during the IP source violation period causes the drop-limit counter to increment.

For example, if the drop-limit is set to 10, after 10 source violations, the call is dropped. The detection period timer continues to count throughout this process.

**Example**

The following command sets the drop limit to *15* and leaves the other values at their default values:

```
ip source-violation drop-limit 15
```

## setup-timeout

Specifies the maximum time allowed to set up a session in seconds.

**Product**

FNG

**Privilege**

Security-Administrator, Administrator

**Command Modes**

Exec > Global Configuration > Context Configuration > FNG Service Configuration

**configure** > **context** *context\_name* > **fng-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
setup-timeout integer  
default setup-timeout
```

**setup-timeout** *integer*

Sets the session setup timer (in seconds) as an integer from 2 through 300. Default: 60

**default**

Sets or restores the default session setup timer value to 60 seconds.

**Usage Guidelines**

The FNG clears both the user session and tunnels if a call does not initiate successfully before the session setup timer expires.

**Example**

The following command sets the session setup timeout value to the default value of 60 seconds:

```
default setup-timeout
```



# CHAPTER 27

## FTP Configuration Mode Commands

The FTP Configuration Mode is used to manage the FTP server options for the current context.

### Command Modes

Exec > Global Configuration > Context Configuration > FTP Configuration

**configure > context** *context\_name* > **server ftpd**

Entering the above command sequence results in the following prompt:

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



### Important

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



### Caution

For maximum system security, you should not enable FTP functionality. SFTP is the recommended file transfer protocol. In release 20.0 and higher Trusted StarOS builds, FTP is not supported.

- [end, on page 1271](#)
- [exit, on page 1272](#)
- [max servers, on page 1272](#)
- [timeout, on page 1273](#)

## end

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

### Product

All

### Privilege

Security Administrator, Administrator

### Syntax Description

**end**

### Usage Guidelines

Use this command to return to the Exec mode.

# exit

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

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Syntax Description</b>	<b>exit</b>
<b>Usage Guidelines</b>	Use this command to return to the parent configuration mode.

# max servers

Configures the maximum number of FTP servers that can be started within any 60 second interval. If this limit is reached, the system waits two minutes before trying to start any more servers.

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > Global Configuration > Context Configuration > FTP Configuration <b>configure &gt; context <i>context_name</i> &gt; server ftpd</b>
<b>Syntax Description</b>	Entering the above command sequence results in the following prompt: [local]host_name(config-ftpd)# <b>max servers <i>count</i></b>

## ***count***

Default: 40

Specifies the maximum number of servers that can be spawned in any 60-second interval. *count* must be an integer from 1 through 100.

**Usage Guidelines** Set the number of servers to tune the system response as a heavily loaded system may need more servers to support the incoming requests.

The converse would be true as well in that a system can benefit by reducing the number of servers such that FTP services do not cause excessive system impact to other services.

## **Example**

```
max servers 50
```

# timeout

Configures the client idle timeout before an FTP session is automatically closed.

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > Global Configuration > Context Configuration > FTP Configuration

**configure > context *context\_name* > server ftpd**

Entering the above command sequence results in the following prompt:

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

---

**Syntax Description**

**timeout** *seconds*

***seconds***

Default: 900

Specifies the number of seconds of inactivity before an FTP session is automatically closed. *seconds* must be an integer from 10 through 86400.

---

**Usage Guidelines**

Adjust the session timeout to fine tune the system. FTP session resources can be released sooner to support additional requests by adjusting the timeout to a smaller value.

**Example**

```
timeout 300
```

**timeout**





## CHAPTER 28

# Firewall-and-NAT Action Configuration Mode Commands

### Command Modes

The Firewall-and-NAT Action Configuration Mode enables configuring Stateful Firewall (FW) and Network Address Translation (NAT) actions.

Exec > ACS Configuration > Firewall-and-NAT Action Configuration

**active-charging service** *service\_name* > **fw-and-nat action** *action\_name*

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-fw-and-nat-action) #
```



### Important

This configuration mode is only available in release 11.0 and later releases. This configuration mode must be used to configure Action-based Stateful Firewall and NAT features.



### Important

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

- [end, on page 1275](#)
- [exit, on page 1276](#)
- [flow check-point, on page 1276](#)

## end

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

### Product

All

### Privilege

Security Administrator, Administrator

### Syntax Description

**end**

### Usage Guidelines

Use this command to return to the Exec mode.

## exit

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

---

**Product**

All

---

**Privilege**

Security Administrator, Administrator

---

**Syntax Description**

**exit**

---

**Usage Guidelines**

Use this command to return to the parent configuration mode.

## flow check-point

This command checkpoints all the flows matching the Firewall-and NAT action.

---

**Product**

NAT

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Action Configuration

**active-charging service** *service\_name* > **fw-and-nat action** *action\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-action)#
```

---

**Syntax Description**

```
flow check-point [ data-usage data_usage [ and | or ] | time-duration duration
[ and | or ] ]
{ default | no } flow check-point
```

**default**

Configures the default Firewall action.

**no**

Deletes the Firewall action configuration.

**data-usage** *data\_usage*

Specifies the data usage in bytes.

*data\_usage* must be an integer from 1 through 4294967295.

The maximum limit for data-usage is 4 GB.

**time-duration** *duration*

Specifies the time duration in seconds.

*duration* must be an integer from 1 through 86400.

The maximum limit for time-duration is 24 hours.

#### **and | or**

This option allows to configure only **data-usage** or **time-duration**, or a combination of **data-usage** and **time-duration**.

---

#### **Usage Guidelines**

Use this command to enable/disable the check-pointing of NATed flows and control the type of flows that need to be check pointed based on specified criteria. Check pointing is done only for TCP and UDP flows.

#### **Example**

The following command checkpoints flows with data-usage set to 5000 bytes and time duration set to 300 seconds:

```
flow check-point data-usage 5000 and time-duration 300
```

flow check-point



## CHAPTER 29

# Firewall-and-NAT Policy Configuration Mode Commands

### Command Modes

The Firewall-and-NAT Policy Configuration Mode enables configuring Stateful Firewall (FW) and Network Address Translation (NAT) policies.

Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

**active-charging service** *service\_name* > **fw-and-nat policy** *policy\_name*

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-fw-and-nat-policy) #
```



### Important

This configuration mode is only available in 8.1, 9.0, and later releases. This configuration mode must be used to configure Policy-based Stateful Firewall and NAT features.



### Important

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

- [access-rule](#), on page 1280
- [end](#), on page 1284
- [exit](#), on page 1284
- [firewall dos-protection](#), on page 1284
- [firewall flooding](#), on page 1288
- [firewall icmp-checksum-error](#), on page 1290
- [firewall icmp-destination-unreachable-message-threshold](#), on page 1291
- [firewall icmp-echo-id-zero](#), on page 1292
- [firewall icmp-fsm](#), on page 1293
- [firewall ip-reassembly-failure](#), on page 1293
- [firewall malformed-packets](#), on page 1294
- [firewall max-ip-packet-size](#), on page 1295
- [firewall mime-flood](#), on page 1296
- [firewall policy](#), on page 1297
- [firewall tcp-checksum-error](#), on page 1299

- [firewall tcp-first-packet-non-syn](#), on page 1300
- [firewall tcp-fsm](#), on page 1300
- [firewall tcp-idle-timeout-action](#), on page 1301
- [firewall tcp-options-error](#), on page 1302
- [firewall tcp-partial-connection-timeout](#), on page 1303
- [firewall tcp-reset-message-threshold](#), on page 1304
- [firewall tcp-syn-flood-intercept](#), on page 1305
- [firewall tcp-syn-with-ecn-cwr](#), on page 1306
- [firewall udp-checksum-error](#), on page 1307
- [firewall validate-ip-options](#), on page 1308
- [nat binding-record](#), on page 1309
- [nat check-point-info](#), on page 1310
- [nat icnr-flow-recovery](#), on page 1311
- [nat max-chunk-per-realm](#), on page 1312
- [nat pkts-drop](#), on page 1313
- [nat policy](#), on page 1314
- [nat private-ip-flow-timeout](#), on page 1315
- [nat suppress-aaa-update](#), on page 1316

## access-rule

This command creates and configures an access rule.

### Product

PSF  
NAT  
SaMOG

### Privilege

Security Administrator, Administrator

### Command Modes

Exec > ACS Configuration > Firewall-and-NAT Policy Configuration  
**active-charging service** *service\_name* > **fw-and-nat policy** *policy\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

### Syntax Description

```
access-rule { no-ruledef-matches { downlink | uplink } action { deny [
charging-action charging_action ] | permit [ bypass-nat | nat-realm nat_realm [
fw-and-nat-action name ] ] } | priority priority { [ dynamic-only |
static-and-dynamic ] access-ruledef ruledef_name { deny [ charging-action
charging_action ] | permit [ [ bypass-nat | nat-realm nat_realm [
fw-and-nat-action name ] ] | trigger open-port { port_number | range start_port
to end_port } direction { both | reverse | same } ] } } }
default access-rule no-ruledef-matches { downlink | uplink } action
no access-rule priority priority
```

**default**

Configures the default setting.

Default: Uplink direction: **permit**; Downlink direction: **deny**

**no**

Removes the access rule specified by the priority.

**no-ruledef-matches**

Configures action on packets with no ruledef match.

**downlink**

Specifies to act on downlink packets with no ruledef match.

**uplink**

Specifies to act on uplink packets with no ruledef match.

**action**

Specifies action to take on downlink/uplink packets with no ruledef match.

**deny**

Specifies to deny packets.

**permit**

Specifies to permit packets and allow the creation of data flows.

**charging-action *charging\_action***

Specifies the charging action. Optionally, a charging action can be configured for deny action. If a packet matches the deny rule, action is taken as configured in the charging action. If a charging action is specified, the content-ID and billing-action configured in the charging action are used. Also, the flow may be terminated (instead of just discarding the packet), if so configured in the specified charging action.

*charging\_action* must be an alphanumeric string of 1 through 63 characters.

**bypass-nat****Important**

---

In 9.0 and later releases, this keyword is NAT license dependent.

---

Specifies to bypass NAT.

**nat-realm *nat\_realm***

**Important** In 9.0 and later releases, this keyword is NAT license dependent.

Specifies the NAT realm to be used to perform NAT on subscriber packets matching the access ruledef. If the NAT realm is not specified, NAT will be bypassed. That is, NAT will not be performed on subscriber packets that are matching a ruledef with no NAT realm name configured in it.

*nat\_realm* must be an alphanumeric string of 1 through 31 characters.

**priority *priority***

Specifies priority of an access ruledef in the Firewall-and-NAT policy.

*priority* must be an integer from 1 through 65535 that is unique for each access ruledef in the Firewall-and-NAT policy.

**[ *dynamic-only* | *static-and-dynamic* ] access-ruledef *ruledef\_name***

Specifies the access ruledef name. Optionally, the ruledef type can also be specified.

- **dynamic-only**: Dynamic Ruledef—Predefined ruledef that can be enabled/disabled by the policy server, and is disabled by default.
- **static-and-dynamic**: Static and Dynamic Ruledef—Predefined ruledef that can be enabled/disabled by the policy server, and is enabled by default.
- **access-ruledef *ruledef\_name***: Specifies the access ruledef name. *ruledef\_name* must be an alphanumeric string of 1 through 63 characters.

**trigger open-port { *port\_number* | range *start\_port* to *end\_port* } direction { *both* | *reverse* | *same* }**

**Important** In 9.0 and later releases, this keyword is Stateful Firewall license dependent.

Optionally a port trigger can be specified to be used for this rule to limit the range of auxiliary data connections (a single or range of port numbers) for protocols having control and data connections (like FTP). The trigger port will be the destination port of an association which matches a rule.

- ***port\_number***: Specifies the auxiliary port number to open for traffic, and must be an integer from 1 through 65535.
- **range *start\_port* to *end\_port***: Specifies the range of port numbers to open for subscriber traffic.
  - *start\_port* must be an integer from 1 through 65535.
  - *end\_port* must be an integer from 1 through 65535, and must be greater than *start\_port*.
- **direction { *both* | *reverse* | *same* }**: Specifies the direction from which the auxiliary connection is initiated. This direction can be same as the direction of control connection, or the reverse of the control connection direction, or in both directions.
  - *both*: Provides the trigger to open port for traffic in either direction of the control connection.



- *reverse*: Provides the trigger to open port for traffic in the reverse direction of the control connection (from where the connection is initiated).
- *same*: Provides the trigger to open port for traffic in the same direction of the control connection (from where the connection is initiated).

### Usage Guidelines

Use this command to add access ruledefs to the Firewall-and-NAT policy and configure the priority and actions for rule matching.

The policy specifies the rules to be applied on calls. The ruledefs in the policy have priorities, based on which priority matching is done.

For Stateful Firewall, the port trigger configuration is optional, and can be configured only if a rule action is permit. When a rule is matched and the rule action is permit, if the trigger is configured, the appropriate check is made. The trigger port will be the destination port of an association that matches the rule. Multiple triggers can be defined for the same port number to permit multiple auxiliary ports for subscriber traffic.

When a rule is matched and if the rule action is deny, the action taken depends on what is configured in the specified charging action. If the flow exists, flow statistics are updated and action is taken as configured in the charging action:

- If the billing action is configured as Event Data Record (EDR) enabled, an EDR is generated.
- If the content ID is configured, UDR information is updated.
- If the flow action is configured as "terminate-flow", the flow is terminated instead of just discarding the packet.

If the billing action, content ID, and flow action are not configured, no action is taken on the dropped packets.



### Important

For Stateful Firewall, only the terminate-flow action is applicable if configured in the specified charging action.

Allowing/dropping of packets is determined in the following sequence:

- Check is done to see if the packet matches any pinholes. If yes, no rule matching is done and the packet is allowed.
- Access ruledef matching is done. If a rule matches, the packet is allowed or dropped as per the **access-rule priority** configuration.
- If no access ruledef matches, the packet is allowed or dropped as per the **access-rule no-ruledef-matches** configuration.

For a packet dropped due to access ruledef match or no match (first packet of a flow), the charging action applied is the one configured in the **access-rule priority** or the **access-rule no-ruledef-matches** command respectively.

For action on packets dropped due to any error condition after data session is created, the charging action must be configured in the **flow any-error charging-action** command in the ACS Rulebase Configuration Mode.

The GGSN can dynamically activate or deactivate dynamic ruledefs for a subscriber based on the rule name received from a policy server. At rule match, if a rule in the policy is a dynamic rule, and if the rule is enabled

**end**

for the particular subscriber, rule matching is done for the rule. If the rule is disabled for the particular subscriber, rule matching is not done for the rule.

### Example

For Stateful Firewall, the following command assigns a priority of *10* to the access ruledef *test\_rule*, adds it to the policy, and permits port trigger to be used for the rule to open ports in the range of *1000* to *2000* in either direction of the control connection:

```
access-rule priority 1 access-ruledef test_rule permit trigger open-port
range 1000 to 2000 direction both
```

## end

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

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Syntax Description</b>	<b>end</b>
<b>Usage Guidelines</b>	Use this command to return to the Exec mode.

## exit

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

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Syntax Description</b>	<b>exit</b>
<b>Usage Guidelines</b>	Use this command to return to the parent configuration mode.

## firewall dos-protection

This command configures Stateful Firewall protection for subscribers from Denial-of-Service (DoS) attacks.



### Important

In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

<b>Product</b>	PSF
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	<p>Exec &gt; ACS Configuration &gt; Firewall-and-NAT Policy Configuration</p> <p><b>active-charging service</b> <i>service_name</i> &gt; <b>fw-and-nat policy</b> <i>policy_name</i></p> <p>Entering the above command sequence results in the following prompt:</p> <pre>[local]host_name(config-fw-and-nat-policy)#</pre>
<b>Syntax Description</b>	<pre>[ no ] firewall dos-protection { all   flooding { icmp   tcp-syn   udp }   ftp-bounce   ip-sweep { icmp   tcp-syn   udp }   ip-unaligned-timestamp   ipv6-dst-options [ invalid-options   unknown-options ]   ipv6-extension-hdrs [ limit <i>extension_limit</i> ]   ipv6-frag-hdr nested-fragmentation   ipv6-hop-by-hop [ invalid-options   jumbo-payload   router-alert   unknown-options ]   mime-flood   port-scan   source-router   tcp-window-containment   teardrop   winnuke } default firewall dos-protection</pre> <p><b>no</b></p> <p>Disables Stateful Firewall protection for subscribers against the specified Denial of Service (DoS) attack(s).</p> <p><b>default</b></p> <p>Disables Stateful Firewall protection for subscribers against all DoS attacks.</p> <p><b>all</b></p> <p>Enables Stateful Firewall protection for subscribers against all DoS attacks supported by the Stateful Firewall service.</p> <p>The IPv6 extension headers will be enabled only if the <b>firewall validate-ip-options</b> command is enabled in the Firewall-and-NAT policy configuration.</p> <p><b>flooding { icmp   tcp-syn   udp }</b></p> <p>Enables protection against the specified flooding attack:</p> <ul style="list-style-type: none"> <li>• <b>icmp</b>: Enables protection against ICMP Flood attack.</li> <li>• <b>tcp-syn</b>: Enables protection against TCP Syn Flood attack.</li> <li>• <b>udp</b>: Enables protection against UDP Flood attack.</li> </ul> <p><b>ftp-bounce</b></p> <p>Enables protection against FTP Bounce attacks.</p> <p><b>ip-sweep { icmp   tcp-syn   udp }</b></p> <p>Enables protection against IP Sweep attacks in the downlink direction.</p> <ul style="list-style-type: none"> <li>• <b>icmp</b>: Enables protection against ICMP IP Sweep attack.</li> </ul>

- **tcp-syn**: Enables protection against TCP Syn IP Sweep attack.
- **udp**: Enables protection against UDP IP Sweep attack.

IP Sweep attacks are also detected in the uplink direction. The **firewall dos-protection ip-sweep** command must be configured in the ACS Configuration mode. The configuration values for packet limit and sampling interval are common for both uplink and downlink.

### **ip-unaligned-timestamp**

Enables protection against IP Unaligned Timestamp attacks.

### **ipv6-dst-options [ invalid-options | unknown-options ]**

Drops IPv6 packets containing the IPv6 destination options header.

The following options are specified in the Destination Options extension header:

- The Tunnel Encapsulation Limit (option type: 0x04) is a destination option defined in RFC 2473.
- The Home Address option (option type: 0xC9) is part of Mobile IP processing defined in RFC 3775. This option is only valid as a Destination Option.
- The NSAP Address option (option type: 0xC3) is assigned as a Destination Option by RFC 1888 and deprecated (reclassified as historic) by RFC 4048.
- **invalid-options**: Drops IPv6 packets containing invalid IPv6 destination options.

The following values are invalid in a Destination Options extension header option type field. Packets with these options in a Destination Options header will be dropped.

- Value 0xC2, Jumbo Payload
- Value 0x05, Router Alert
- Value 0x06, Quick start
- Value 0x07, CALIPSO

- **unknown-options**: Drops IPv6 packets containing unknown IPv6 destination options.

### **ipv6-extension-hdrs [ limit *extension\_limit* ]**

Default: 8

Limits the number of IPv6 extension headers in an IPv6 packet. An IPv6 packet can contain zero or more extension headers.

Firewall will not fully parse packets with unknown extension headers as the extension header format is unspecified. Under such cases, the transport protocol will be considered as **unknown**. Packets with invalid length field in the extension headers and packets with next header 0x01 (ICMPv4) will be dropped. IPv6 uses ICMPv6 of type 0x3A.

*extension\_limit* must be an integer from 0 through 4294967295.

**ipv6-frag-hdr nested-fragmentation**

Drops IPv6 packets containing nested fragmentation (reassembled packets containing a fragment header).

IPv6 fragmentation is done only by the source node. An IPv6 fragment packet must have only one fragment header. Firewall will drop packets with more than one fragment header. The Reassembled packet containing a fragment header will be dropped by Firewall. As per RFC 2460, the fragment length (except for last fragment) must be a multiple of 8 octets. If not, such fragments are dropped.

**ipv6-hop-by-hop [ invalid-options | jumbo-payload | router-alert | unknown-options ]**

Drops IPv6 packets containing the hop-by-hop extension header.

The Hop-by-Hop Options extension header, if present, must be the first header to follow the IPv6 main header. This is indicated by a value of 0x00 in the next header field in the main header. The length must be expressed as a multiple of 8 octets (excluding the first 8 octets). If not, such packets will be dropped.

- **invalid-options:** Drops IPv6 packets containing invalid IPv6 hop-by-hop options.

The following values are invalid in a Hop-by-Hop extension header option type field. Packets with these options in a hop-by-hop header will be dropped.

- Value 0x04, Tunnel Encapsulation limit
- Value 0xC9, Home Address Destination option
- Value 0xC3, NSAP Address option

The options are present in TLV (Type Length Value) format. If the length specified is invalid, then such packets will be dropped.

- **jumbo-payload:** Drops IPv6 packets with jumbo payload hop-by-hop options.

The Jumbo Payload option (RFC 2675) has the option type value 0xC2 and is only valid as a Hop-by-Hop option. This option allows the creation of very large IP packets (packets larger than 65K bytes). If this option is allowed, the following validity checks will be done.

- The IP payload length must be 0x00 when the Jumbo Payload option is present.
- The Jumbo Payload option must be used only when the length is greater than 65,535; the two most significant bytes of the Jumbo length cannot be 0x00.
- The Jumbo Payload option cannot be used in conjunction with a Fragmentation extension header.

If any of the above checks fail, then the IPv6 packet will be dropped. The Option Type field must have  $4n+2$  alignment.

- **router-alert:** Drops IPv6 packets with router alert hop-by-hop options.

The Router Alert (RFC 2711) option is used to signal the routers that a closer inspection of the packet is warranted. Denial of service (DoS) attacks can occur if an attacker sends large number of packets with this option. Only one option of this type must be present, regardless of value, per Hop-by-Hop header with  $2n + 0$  alignment.

- **unknown-options:** Drops IPv6 packets containing unknown IPv6 hop-by-hop options.

**mime-flood**

Enables protection against HTTP Multiple Internet Mail Extension (MIME) header flooding attacks.

**port-scan**

Enables protection against Port Scan attacks.

**tcp-window-containment**

Enables protection against TCP sequence number out-of-range attacks.

**source-router**

Enables protection against IPv4/IPv6 Source Route IP Option attacks.

This command can be used to filter IPv4/IPv6 packets containing Routing header of Type 0 (source routing). In this release, only type 0 filtering is supported.

**teardrop**

Enables protection against IPv4/IPv6 Teardrop attacks.

**winnuke**

Enables protection against WIN-NUKE attacks.

**Usage Guidelines**

Use this command to enable Stateful Firewall protection from different types of DoS attacks. This command can be used multiple times for different DoS attacks.

**Important**

DoS attacks are detected only in the downlink direction.

**Example**

The following command enables protection from all supported DoS attacks:

```
firewall dos-protection all
```

## firewall flooding

This command configures Stateful Firewall protection from Packet Flooding attacks.

**Important**

In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

**Product**

PSF

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec &gt; ACS Configuration &gt; Firewall-and-NAT Policy Configuration

**active-charging service** *service\_name* > **fw-and-nat policy** *policy\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

---

**Syntax Description**

```
firewall flooding { protocol { icmp | tcp-syn | udp } packet limit packets  
| sampling-interval interval }  
default firewall flooding { protocol { icmp | tcp-syn | udp } packet limit  
| sampling-interval }
```

**default**

Configures the default setting for the specified configuration.

**protocol { icmp | tcp-syn | udp }**

Specifies the transport protocol:

- **icmp**: Configuration for ICMP protocol.
- **tcp-syn**: Configuration for TCP-SYN packet limit.
- **udp**: Configuration for UDP protocol.

**packet limit** *packets*

Specifies the maximum number of specified packets a subscriber can receive during a sampling interval.

*packets* must be an integer from 1 through 4294967295.

Default: 1000 packets per sampling interval for all protocols.

**sampling-interval** *interval*

Specifies the flooding sampling interval, in seconds.

*interval* must be an integer from 1 through 60.

Default: 1 second

The maximum sampling-interval configurable is 60 seconds.

---

**Usage Guidelines**

Use this command to configure the maximum number of ICMP, TCP-SYN, / UDP packets allowed to prevent the packet flooding attacks to the host.

**Example**

The following command ensures a subscriber will not receive more than 1000 ICMP packets per sampling interval:

```
firewall flooding protocol icmp packet limit 1000
```

The following command ensures a subscriber will not receive more than *1000* UDP packets per sampling interval on different 5-tuples. That is, if an attacker is sending lot of UDP packets on different ports or using different spoofed IP addresses, those packets will be limited to 1000 packets per sampling interval. This way only "suspected" malicious packets are limited and not "legitimate" packets.

```
firewall flooding protocol udp packet limit 1000
```

The following command ensures a subscriber will not receive more than *1000* TCP-Syn packets per sampling interval:

```
firewall flooding protocol tcp-syn packet limit 1000
```

The following command specifies a flooding sampling interval of *1* second:

```
firewall flooding sampling-interval 1
```

## firewall icmp-checksum-error

This command configures Stateful Firewall action on packets with ICMP/ICMPv6 Checksum errors.

---

### Product

PSF

---

### Privilege

Security Administrator, Administrator

---

### Command Modes

Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

**active-charging service** *service\_name* > **fw-and-nat policy** *policy\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

---

### Syntax Description

```
firewall icmp-checksum-error { drop | permit }
default firewall icmp-checksum-error
```

#### default

Configures the default setting.

Default: **drop**

#### drop

Drops packets with ICMP/ICMPv6 Checksum errors.

#### permit

Permits packets with ICMP/ICMPv6 Checksum errors.

---

### Usage Guidelines

Use this command to configure Stateful Firewall action on packets with ICMP/ICMPv6 Checksum errors. This command also applies to ICMP/ICMPv6 packets with Inner IP Checksum error.

For NAT-only calls, packets with ICMP/ICMPv6 errors are dropped, and other packets are allowed.



**Example**

The following command configures Stateful Firewall to drop packets with ICMP/ICMPv6 Checksum errors:

```
firewall icmp-checksum-error drop
```

## firewall icmp-destination-unreachable-message-threshold

This command configures a threshold on the number of ICMP/ICMPv6 error messages sent by the subscriber for a particular data flow.

**Important**

In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

**Product**

PSF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

**active-charging service** *service\_name* > **fw-and-nat policy** *policy\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax Description**

```
firewall icmp-destination-unreachable-message-threshold messages  
then-block-server  
{ default | no } firewall icmp-destination-unreachable-message-threshold
```

**default**

Configures the default setting.

Default: No limit

**no**

Removes the previous configuration.

**messages**

Specifies the threshold on the number of ICMP/ICMPv6 error messages sent by the subscriber for a particular data flow. *messages* must be an integer from 1 through 100.

**Usage Guidelines**

Use this command to configure a threshold on the number of ICMP/ICMPv6 error messages sent by the subscriber for a particular data flow. After the threshold is reached, it is assumed that the server is not reacting properly to the error messages, and further downlink traffic to the subscriber on the unwanted flow is blocked.

Some servers that run QChat ignore the ICMP/ICMPv6 error messages (Destination Port Unreachable and Host Unreachable) from the mobiles. So the mobiles continue to receive unwanted UDP traffic from the QChat servers, and their batteries get exhausted quickly.

### Example

The following command configures a threshold of 10 ICMP/ICMPv6 error messages:

```
firewall icmp-destination-unreachable-message-threshold 10
then-block-server
```

## firewall icmp-echo-id-zero

This command configures Stateful Firewall action on echo packets with ICMP/ICMPv6 ID zero.

### Product

PSF

### Privilege

Security Administrator, Administrator

### Command Modes

Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

**active-charging service** *service\_name* > **fw-and-nat policy** *policy\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

### Syntax Description

```
firewall icmp-echo-id-zero { drop | permit }
default firewall icmp-echo-id-zero
```

#### default

Configures the default setting.

Default: **permit**

#### drop

Drops packets with ICMP/ICMPv6 ID zero.

#### permit

Permits packets with ICMP/ICMPv6 ID zero.

### Usage Guidelines

Use this command to configure Stateful Firewall action on echo packets with ICMP/ICMPv6 ID zero.

### Example

The following command configures Stateful Firewall to drop packets with ICMP/ICMPv6 ID zero:

```
firewall icmp-echo-id-zero drop
```

## firewall icmp-fsm

This command enables/disables Stateful Firewall's ICMP/ICMPv6 Finite State Machine (FSM).

**Product** PSF

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > ACS Configuration > Firewall-and-NAT Policy Configuration  
**active-charging service** *service\_name* > **fw-and-nat policy** *policy\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax Description** [ **default** | **no** ] **firewall icmp-fsm**

### default

Configures the default setting.

Default: Enabled. Same as **firewall icmp-fsm**.

### no

Disables Stateful Firewall ICMP/ICMPv6 FSM checks.

### Usage Guidelines

Use this command to enable/disable Stateful Firewall ICMP/ICMPv6 FSM checks. When Stateful Firewall and ICMP/ICMPv6 FSM are enabled, ICMP/ICMPv6 reply messages for which there is no saved ICMP/ICMPv6 request message are discarded. ICMP/ICMPv6 error messages (i.e., messages containing an embedded message) for which there is no saved flow for the embedded message are discarded.

### Example

The following command disables Stateful Firewall's ICMP/ICMPv6 FSM checks:

```
no firewall icmp-fsm
```

## firewall ip-reassembly-failure

This command configures Stateful Firewall action on IPv4/IPv6 packets involved in IP Reassembly Failure scenarios.

**Product** PSF

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > ACS Configuration > Firewall-and-NAT Policy Configuration  
**active-charging service** *service\_name* > **fw-and-nat policy** *policy\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

---

**Syntax Description**

```
firewall ip-reassembly-failure { drop | permit }
default firewall ip-reassembly-failure
```

**default**

Configures the default setting.

Default: **permit**

**drop**

Drops IPv4/IPv6 packets involved in IP reassembly failure scenarios.

**permit**

Permits IPv4/IPv6 packets involved in IP reassembly failure scenarios.

---

**Usage Guidelines**

Use this command to configure Stateful Firewall action on IPv4/IPv6 packets involved in IP reassembly failure scenarios such as missing fragments, overlapping offset, etc.

For NAT-only calls, packets involved in IP reassembly failure scenarios are dropped.

**Example**

The following command specifies to drop IPv4/IPv6 packets involved in IP reassembly failure scenarios:

```
firewall ip-reassembly-failure drop
```

## firewall malformed-packets

This command configures Stateful Firewall action on malformed packets. In release 12.0, this command supports ICMPv6 and IPv6 packets.

---

**Product**

PSF

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

```
active-charging service service_name > fw-and-nat policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

---

**Syntax Description**

```
firewall malformed-packets { drop | permit }
default firewall malformed-packets
```

**default**

Configures the default setting.

Default: **permit**

**drop**

Drops malformed packets.

**permit**

Permits malformed packets.

**Usage Guidelines**

Use this command to configure Stateful Firewall action on malformed packets.

For NAT-only calls, malformed packets are always permitted.

**Example**

The following command specifies Stateful Firewall to drop malformed packets:

```
firewall malformed-packets drop
```

## firewall max-ip-packet-size

This command configures the maximum IPv4/IPv6 packet size (after IP reassembly) allowed over Stateful Firewall.

**Important**

In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

**Product**

PSF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

```
active-charging service service_name > fw-and-nat policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax Description**

```
firewall max-ip-packet-size packet_size protocol { icmp | non-icmp }
default firewall max-ip-packet-size protocol { icmp | non-icmp }
```

**default**

Configures the default setting.

Default: 65535 bytes (for both ICMP/ICMPv6 and non-ICMP/ICMPv6)

### ***packet\_size***

Specifies the maximum packet size allowed by firewall. Any IPv6 packet with payload size greater than the configured value will be dropped.

*packet\_size* must be an integer from 30000 through 65535.

### **protocol { icmp | non-icmp }**

Specifies the transport protocol:

- **icmp**: Configuration for ICMP/ICMPv6 protocol.
- **non-icmp**: Configuration for protocols other than ICMP/ICMPv6.

### **Usage Guidelines**

Use this command to configure the maximum IPv4/IPv6 packet size allowed for ICMP/ICMPv6 and non-ICMP/ICMPv6 packets to prevent packet flooding attacks to the host. Packets exceeding the configured size will be dropped for "Jolt" and "Ping-Of-Death" attacks.

### **Example**

The following command allows a maximum packet size of *60000* for ICMP/ICMPv6 protocol:

```
firewall max-ip-packet-size 60000 protocol icmp
```

## firewall mime-flood

This command configures Stateful Firewall protection from MIME Flood attacks.



### **Important**

In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

### **Product**

PSF

### **Privilege**

Security Administrator, Administrator

### **Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Policy Configuration  
**active-charging service** *service\_name* > **fw-and-nat policy** *policy\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

### **Syntax Description**

```
firewall mime-flood { http-headers-limit max_limit |  
max-http-header-field-size max_size }
```

```
default firewall mime-flood { http-headers-limit |
max-http-header-field-size }
```

### default

Configures the default setting for the specified parameter.

### http-headers-limit *max\_limit*

Specifies the maximum number of headers allowed in an HTTP packet. If the number of HTTP headers in a page received is more than the specified limit, the request will be denied.

*max\_limit* must be an integer from 1 through 256.

Default: 16

### max-http-header-field-size *max\_size*

Specifies the maximum header field size allowed in the HTTP header, in bytes. If the size of HTTP header in the received page is more than the specified number of bytes, the request will be denied.

*max\_size* must be an integer from 1 through 8192.

Default: 4096 bytes

## Usage Guidelines

Use this command to configure the maximum number of headers allowed in an HTTP packet, and the maximum header field size allowed in the HTTP header to prevent MIME flooding attacks.

This command is only effective if Stateful Firewall DoS protection for MIME flood attacks has been enabled using the **firewall dos-protection mime-flood** command, and the **route** command has been configured to send HTTP packets to the HTTP analyzer.

### Example

The following command sets the maximum number of headers allowed in an HTTP packet to *100*:

```
firewall mime-flood http-headers-limit 100
```

The following command sets the maximum header field size allowed in the HTTP header to *1000* bytes:

```
firewall mime-flood max-http-header-field-size 1000
```

# firewall policy

This command enables/disables Stateful Firewall support in a Firewall-and-NAT policy.



### Important

In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

---

**Product** PSF

---

**Privilege** Security Administrator, Administrator

---

**Command Modes** Exec > ACS Configuration > Firewall-and-NAT Policy Configuration  
**active-charging service** *service\_name* > **fw-and-nat policy** *policy\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

---

**Syntax Description** In 11.0 and earlier releases:

```
firewall policy firewall-required  
no firewall policy
```

In 12.0 and later releases:

```
firewall policy { ipv4-and-ipv6 | ipv4-only | ipv6-only }  
{ default | no } firewall policy
```

**default**

Disables IPv4 and IPv6 Stateful Firewall support in the Firewall-and-NAT policy.

**no**

Disables IPv4 and IPv6 Stateful Firewall support in the Firewall-and-NAT policy.

**firewall-required**

Enables Stateful Firewall support in the Firewall-and-NAT policy.




---

**Important** This keyword is available only in 11.0 and earlier releases.

---

**ipv4-and-ipv6**

Enables both IPv4 and IPv6 Stateful Firewall support in the Firewall-and-NAT policy.

**ipv4-only**

Enables IPv4 Stateful Firewall and disables IPv6 Stateful Firewall in the Firewall-and-NAT policy.

**ipv6-only**

Enables IPv6 Stateful Firewall and disables IPv4 Stateful Firewall support in the Firewall-and-NAT policy.

---

**Usage Guidelines** Use this command to enable/disable IPv4 and/or IPv6 Stateful Firewall support for all subscribers using a Firewall-and-NAT policy.



**Example**

The following command enables IPv4 and IPv6 Stateful Firewall support in a Firewall-and-NAT policy:

```
firewall policy ipv4-and-ipv6
```

The following command disables Stateful Firewall support in a Firewall-and-NAT policy:

```
no firewall policy
```

## firewall tcp-checksum-error

This command configures Stateful Firewall action on packets with TCP Checksum error.

<b>Product</b>	PSF
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > ACS Configuration > Firewall-and-NAT Policy Configuration <b>active-charging service</b> <i>service_name</i> > <b>fw-and-nat policy</b> <i>policy_name</i> Entering the above command sequence results in the following prompt: <pre>[local]host_name(config-fw-and-nat-policy) #</pre>
<b>Syntax Description</b>	<pre>firewall tcp-checksum-error { drop   permit } default firewall tcp-checksum-error</pre> <p><b>default</b> Configures the default setting. Default: <b>drop</b></p> <p><b>drop</b> Drops packets with TCP Checksum errors.</p> <p><b>permit</b> Permits packets with TCP Checksum errors.</p>
<b>Usage Guidelines</b>	Use this command to configure Stateful Firewall action on packets with TCP Checksum error. For NAT-only calls, packets with TCP Checksum errors are permitted.

**Example**

The following command specifies Stateful Firewall to drop packets with TCP Checksum errors:

```
firewall tcp-checksum-error drop
```

# firewall tcp-first-packet-non-syn

This command configures Stateful Firewall action on TCP flows starting with a non-SYN packet.



## Important

In release 9.0, this command is deprecated. This configuration is available as the **firewall tcp-fsm [ first-packet-non-syn { drop | permit | send-reset } ]** command.

## Product

PSF

## Privilege

Security Administrator, Administrator

## Command Modes

Exec > ACS Configuration > Firewall-and-NAT Policy Configuration  
**active-charging service** *service\_name* > **fw-and-nat policy** *policy\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

## Syntax Description

```
firewall tcp-first-packet-non-syn { drop | reset }  
default firewall tcp-first-packet-non-syn
```

### default

Configures the default setting.

Default: **drop**

### drop

Drops the non-SYN packet.

### reset

Sends reset.

## Usage Guidelines

Use this command to configure Stateful Firewall action on TCP flows starting with a non-SYN packet.

### Example

For flows starting with a non-SYN packet, the following command specifies Stateful Firewall to drop the non-SYN packet:

```
firewall tcp-first-packet-non-syn drop
```

# firewall tcp-fsm

This command enables/disables Stateful Firewall's TCP Finite State Machine (FSM).

<b>Product</b>	PSF
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > ACS Configuration > Firewall-and-NAT Policy Configuration <b>active-charging service</b> <i>service_name</i> > <b>fw-and-nat policy</b> <i>policy_name</i> Entering the above command sequence results in the following prompt: <pre>[local] host_name (config-fw-and-nat-policy) #</pre>
<b>Syntax Description</b>	<pre>firewall tcp-fsm [ first-packet-non-syn { drop   permit   send-reset } ] { default   no } firewall tcp-fsm</pre> <p><b>default</b></p> <p>Configures the default setting.</p> <p>Default: <b>drop</b></p> <p><b>no</b></p> <p>Disables Stateful Firewall's TCP FSM.</p> <p><b>first-packet-non-syn { drop   permit   send-reset }</b></p> <p>Specifies Stateful Firewall action on TCP flows starting with a non-SYN packet:</p> <ul style="list-style-type: none"> <li>• <b>drop</b>: Specifies to drop the packet.</li> <li>• <b>permit</b>: Specifies to permit the packet.</li> <li>• <b>send-reset</b>: Specifies to drop the packet and send TCP RST.</li> </ul> <p>Default: <b>drop</b></p>
<b>Usage Guidelines</b>	<p>Use this command to enable/disable Stateful Firewall's TCP FSM checks. When Stateful Firewall and TCP FSM are enabled, state of the TCP session is checked to decide whether to forward TCP packets.</p> <p><b>Example</b></p> <p>The following command enables TCP FSM, and configures action to take on TCP flows starting with a non-SYN packet to drop the packet:</p> <pre>firewall tcp-fsm first-packet-non-syn drop</pre>

## firewall tcp-idle-timeout-action

This command configures action on TCP idle timeout expiry.



### Important

In release 9.0 and later this command is also available to NAT.

<b>Product</b>	PSF NAT
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > ACS Configuration > Firewall-and-NAT Policy Configuration <b>active-charging service</b> <i>service_name</i> > <b>fw-and-nat policy</b> <i>policy_name</i> Entering the above command sequence results in the following prompt: <code>[local]host_name(config-fw-and-nat-policy)#</code>
<b>Syntax Description</b>	<b>firewall tcp-idle-timeout-action { drop   reset } { default   no } firewall tcp-idle-timeout-action</b>  <b>default</b> Configures the default setting. Default: <b>reset</b>  <b>no</b> Configures the TCP idle timeout expiry action to reset.  <b>drop</b> Drops the session on TCP idle timeout expiry.  <b>reset</b> Resends TCP RST on TCP idle timeout expiry. When configured to reset, the session is dropped, and the system can avoid packets arriving for the idle flow from getting dropped.
<b>Usage Guidelines</b>	Use this command to configure action to take on TCP idle timeout expiry.

**Example**

The following command configures action to take on TCP idle timeout expiry to drop:

```
firewall tcp-idle-timeout-action drop
```

## firewall tcp-options-error

This command configures Stateful Firewall action on packets with TCP Option errors.

<b>Product</b>	PSF
<b>Privileges</b>	Security Administrator, Administrator

---

**Command Modes** Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

**active-charging service** *service\_name* > **fw-and-nat policy** *policy\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

---

**Syntax Description** **firewall tcp-options-error { drop | permit }**  
**default firewall tcp-options-error**

**default**

Configures the default setting.

Default: **permit**

**drop**

Drops packets with TCP Option errors.

**permit**

Permits packets with TCP Option errors.

---

**Usage Guidelines** Use this command to configure Stateful Firewall action on packets with TCP Option errors.

**Example**

The following command configures Stateful Firewall to drop packets with TCP Option errors:

```
firewall tcp-options-error drop
```

## firewall tcp-partial-connection-timeout

This command configures action on idle timeout for partially open TCP connections.

---

**Product** PSF

---

**Privilege** Security Administrator, Administrator

---

**Command Modes** Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

**active-charging service** *service\_name* > **fw-and-nat policy** *policy\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

---

**Syntax Description** **firewall tcp-partial-connection-timeout** *timeout*  
**{ default | no } firewall tcp-partial-connection-timeout**

**default**

Configures the default setting.

**no**

Disables the idle timeout for partially open TCP connections.

**timeout**

Specifies the timeout in seconds.

*timeout* must be an integer from 0 through 86400.

Default: 30 seconds

**Usage Guidelines**

Use this command to configure idle timeout for TCP connections that are yet to be established (partially open) in the case of Firewall enabled calls.

**Example**

The following command sets the idle timeout setting to 30 seconds:

```
firewall tcp-partial-connection-timeout 30
```

## firewall tcp-reset-message-threshold

This command configures a threshold on the number of TCP reset messages sent by the subscriber for a particular data flow. After this threshold is reached, further downlink traffic to the subscriber on the unwanted flow is blocked.

**Product**

PSF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

```
active-charging service service_name > fw-and-nat policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax Description**

```
firewall tcp-reset-message-threshold messages then-block-server
{ default | no } firewall tcp-reset-message-threshold
```

**default**

Configures the default setting.

Default: Disabled

**no**

Disables the configuration.

**messages**

Specifies the threshold on the number of TCP reset messages sent by the subscriber for a particular data flow. *messages* must be an integer from 1 through 100.

**Usage Guidelines**

Use this command to configure a threshold on the number of TCP reset messages (TCP RST+ACK) sent by the subscriber for a particular data flow. After the threshold is reached, assuming the server is not reacting properly to the reset messages further downlink traffic to the subscriber on the unwanted flow is blocked. This configuration enables QCHAT noise suppression for TCP.

**Example**

The following command sets the threshold on the number of TCP reset messages to *10*:

```
firewall tcp-reset-message-threshold 10 then-block-server
```

## firewall tcp-syn-flood-intercept

This command configures TCP SYN intercept parameters for protection against TCP SYN flooding attacks.

**Important**

In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

**Product**

PSF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

```
active-charging service service_name > fw-and-nat policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-fw-and-nat-policy) #
```

**Syntax Description**

```
firewall tcp-syn-flood-intercept { mode { none | watch [ aggressive ] }
| watch-timeout intercept_watch_timeout }
default firewall tcp-syn-flood-intercept { mode | watch-timeout }
```

**default**

Configures the default settings for SYN Flood DoS protection.

**mode { none | watch [ aggressive ] }**

Specifies the TCP SYN flood intercept mode:

- **none**: Disables the TCP SYN Flood Intercept feature.
- **watch**: Configures TCP SYN flood intercept feature in watch mode. The Stateful Firewall passively watches to see if TCP connections become established within a configurable interval. If connections are not established within the timeout period, the Stateful Firewall clears the half-open connections by sending RST to TCP client and server. The default watch-timeout for connection establishment is 30 seconds.
- **aggressive**: Configures TCP SYN flood Intercept or Watch feature for aggressive behavior. Each new connection request causes the oldest incomplete connection to be deleted. When operating in watch mode, the watch timeout is reduced by half. If the watch-timeout is 30 seconds, under aggressive conditions it becomes 15 seconds. When operating in intercept mode, the retransmit timeout is reduced by half (i.e. if the timeout is 60 seconds, it is reduced to 30 seconds). Thus the amount of time waiting for connections to be established is reduced by half (i.e. it is reduced to 150 seconds from 300 seconds under aggressive conditions).

Default: **none**

**watch-timeout *intercept\_watch\_timeout***

Specifies the TCP intercept watch timeout, in seconds.

*intercept\_watch\_timeout* must be an integer from 5 through 30.

Default: 30

### Usage Guidelines

This TCP intercept functionality provides protection against TCP SYN Flooding attacks. This command enables and configures TCP intercept parameters to prevent TCP SYN flooding attacks by intercepting and validating TCP connection requests for DoS protection mechanism configured with the **dos-protection** command.

The system captures TCP SYN requests and responds with TCP SYN-ACKs. If a connection initiator completes the handshake with a TCP ACK, the TCP connection request is considered as valid by system and system forwards the initial TCP SYN to the valid target which triggers the target to send a TCP SYN-ACK. Now system intercepts with TCP SYN-ACK and sends the TCP ACK to complete the TCP handshake. Any TCP packet received before the handshake completion will be discarded.

### Example

The following command sets the intercept watch timeout setting to 15 seconds:

```
firewall tcp-syn-flood-intercept watch-timeout 15
```

## firewall tcp-syn-with-ecn-cwr

This command configures Stateful Firewall action on TCP SYN packets with either ECN or CWR flag set.

### Product

PSF



**Privileges**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Policy Configuration  
**active-charging service** *service\_name* > **fw-and-nat policy** *policy\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax Description**

```
firewall tcp-syn-with-ecn-cwr { drop | permit }  
default firewall tcp-syn-with-ecn-cwr
```

**default**

Configures the default setting.

Default: **permit**

**drop**

Drops TCP SYN packets with either ECN or CWR flag set.

**permit**

Permits TCP SYN packets with either ECN or CWR flag set.

**Usage Guidelines**

Use this command to configure Stateful Firewall action on receiving a TCP SYN packet with either ECN or CWR flag set.

**Example**

The following command configures Stateful Firewall to drop TCP SYN packets with ECN / CWR flag set:

```
firewall tcp-syn-with-ecn-cwr drop
```

## firewall udp-checksum-error

This command configures Stateful Firewall action on packets with UDP Checksum error.

**Product**

PSF

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Policy Configuration  
**active-charging service** *service\_name* > **fw-and-nat policy** *policy\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax Description** `firewall udp-checksum-error { drop | permit }`  
`default firewall udp-checksum-error`

**default**

Configures the default setting.

Default: **drop**

**drop**

Drops packets with UDP Checksum error.

**permit**

Permits packets with UDP Checksum error.

**Usage Guidelines** Use this command to configure Stateful Firewall action on packets with UDP Checksum error. For NAT-only calls, packets with UDP Checksum error are permitted.

**Example**

The following command specifies to drop packets with UDP Checksum error:

```
firewall udp-checksum-error drop
```

## firewall validate-ip-options

This command enables / disables the Stateful Firewall validation of IP options for errors.

**Product** PSF

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > ACS Configuration > Firewall-and-NAT Policy Configuration  
**active-charging service** *service\_name* > **fw-and-nat policy** *policy\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax Description** `[ default | no ] firewall validate-ip-options`

**default**

Configures the default setting.

Default: Disabled. Same as **no firewall validate-ip-options**

**no**

Disables validation of IP options.

**Usage Guidelines**

Use this command to enable / disable Stateful Firewall validation of IP options. When enabled, Stateful Firewall will drop packets with IP option errors.

For NAT calls, validation of IP Options is disabled.

**Example**

The following command enables validation of IP options:

```
firewall validate-ip-options
```

## nat binding-record

This command configures the generation of NAT Binding Records.

**Product**

NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

```
active-charging service service_name > fw-and-nat policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy) #
```

**Syntax Description**

```
nat binding-record edr-format edr_format [ port-chunk-allocation ] [ port-chunk-release ] { default | no } nat binding-record
```

**default**

Configures the default setting.

Default: **port-chunk-release**

**no**

Disables generating NAT Binding Records.

**edr-format edr\_format**

Specifies the Event Data Record (EDR) format name.

*edr\_format* must be an alphanumeric string of 1 through 63 characters.

**port-chunk-allocation**

Specifies generating NAT Binding Records when a port-chunk is allocated.

**port-chunk-release**

Specifies generating NAT Binding Record when a port-chunk is released.

**Usage Guidelines** Use this command to configure the generation of NAT Binding Records.

### Example

The following command configures an EDR format named *test123* and specifies generating NAT Binding Records when a port chunk is allocated:

```
nat binding-record edr-format test123 port-chunk-allocation
```

## nat check-point-info

This command enables or disables the checkpointing of basic NAT, H323 and SIP ALG recovery. ICSR recovery can also be enabled or disabled for basic NAT and SIP flows.

### Product

PSF  
NAT

### Privilege

Security Administrator, Administrator

### Command Modes

Exec > ACS Configuration > Firewall-and-NAT Policy Configuration  
**active-charging service** *service\_name* > **fw-and-nat policy** *policy\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

### Syntax Description

```
[ default | no ] nat check-point-info { basic [ icnr-also | limit-flows limit ] | h323-alg | sip-alg [ icnr-also ] }
```

#### default

Configures this command with its default setting.

Default: Disabled

#### no

Disables the basic NAT recovery and stand-alone H323 ALG and SIP ALG recovery. Also disables ICSR recovery for SIP ALG.

#### basic [ icnr-also | limit-flows *limit* ]

Configures the basic flow checkpointing information.

- **icnr-also**: Enables checkpointing for ICSR.
- **limit-flows**: Limits the specified flows for basic NAT checkpointing. *limit* must be an integer from 1 through 100.

Default: 100

**h323-alg**

Enables checkpointing of H323 ALG.

**sip-alg [ icsr-also ]**

Enables checkpointing of SIP ALG.

- **icsr-also**: Enables checkpointing for ICSR.

**Usage Guidelines**

Use this command to enable or disable the checkpointing of basic NAT, standalone H323 and SIP ALG recovery. ICSR recovery can also be enabled or disabled for basic NAT and SIP flows. The maximum basic flows that can be checkpointed is also configured. By default, 100 flows can be recovered in a standalone chassis and ICSR setup.

**Example**

The following command enables basic NAT recovery and ICSR recovery with flows limited to 10:

```
nat check-point info basic limit-flows 10 icsr-also
```

## nat icsr-flow-recovery

This command enables/disables the NAT ICSR Flow checkpointing support for subscribers in a Firewall-and-NAT policy. This command is deprecated in StarOS 14.0 and later releases, and is replaced by the **nat check-point-info** command.

**Product**

NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

```
active-charging service service_name > fw-and-nat policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax Description**

```
[ default | no ] nat icsr-flow-recovery
```

**default**

Configures the default setting.

Default: Disabled. Same as **no icsr-flow-recovery**.

**no**

Disables the NAT ICSR Flow checkpointing.

**Usage Guidelines**

Use this command to enable/disable all NAT ICSR Flow checkpointing for subscribers using this policy.

**Example**

The following command enables NAT ICSR Flow checkpointing:

```
nat icsr-flow-recovery
```

## nat max-chunk-per-realm

This command enables or disables the allocation of multiple NAT IP addresses for the same N:1 NAT realm for a subscriber.

---

**Product** NAT

---

**Privilege** Security Administrator, Administrator

---

**Command Modes** Exec > ACS Configuration > Firewall-and-NAT Policy Configuration  
**active-charging service** *service\_name* > **fw-and-nat policy** *policy\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

---

**Syntax Description** **nat max-chunk-per-realm { multiple-ip | single-ip }**  
**{ default | no } nat max-chunk-per-realm**

**default**

Configures the default setting.

Default: **nat max-chunk-per-realm single-ip**

**no**

Disables the allocation of multiple NAT IP addresses for the same NAT realm for a subscriber.

**multiple-ip**

Enables the feature, that is, allows allocation of multiple IP addresses per NAT realm.

**single-ip**

Allows allocation of only one IP address per NAT realm. If the port chunks get exhausted, packets will be dropped. This is the default behavior.

---

**Usage Guidelines** Use this command to enable or disable the allocation of multiple NAT IP addresses for the same N:1 NAT realm for a subscriber. This enhancement is applicable only for N:1 NAT realms and not for 1:1 NAT realms.

# nat pkts-drop

This command is used to configure the EDR format in which records for dropped NAT packets will be saved and the time interval for EDR generation.

**Product** NAT

**Privilege** Security Administrator, Administrator

**Command Modes** Exec > ACS Configuration > Firewall-and-NAT Policy Configuration  
**active-charging service** *service\_name* > **fw-and-nat policy** *policy\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax Description** **nat pkts-drop** { **edr-format** *edr\_format\_name* | **timeout** *timeout\_value* }  
 { **default** | **no** } **nat pkts-drop** { **edr-format** | **timeout** }

## default

Configures the default setting.

Default: Disables the configuration. Same as **no nat pkts-drop { edr-format | timeout }** command.

## no

Disables the configured EDR format in which records for dropped NAT packets will be saved and the time interval for EDR generation.

## edr-format *edr\_format\_name*

Specifies the Event Data Record (EDR) format name.

*edr\_format\_name* must be an alphanumeric string of 1 through 63 characters.

## timeout *timeout\_value*

Specifies the NAT packet drop EDR timeout in seconds.

*timeout\_value* must be an integer from 1 through 86400.

## Usage Guidelines

Use this command to configure the EDR format in which records for dropped NAT packets will be saved and the time interval for EDR generation.

## Example

The following command configures an EDR format named *test1* and specifies a packet drop timeout of 200 seconds:

```
nat pkts-drop edr-format test1 timeout 200
```

# nat policy

This command enables/disables Network Address Translation (NAT) support in a Firewall-and-NAT policy.



## Important

In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

## Product

NAT

## Privilege

Security Administrator, Administrator

## Command Modes

Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

**active-charging service** *service\_name* > **fw-and-nat policy** *policy\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

## Syntax Description

In 12.1 and earlier releases:

```
nat policy nat-required [ default-nat-realm nat_realm_name [ fw-and-nat-action
action_name ] ]
no nat policy
```

In 12.2 and later releases:

```
nat policy [ ipv4-and-ipv6 | ipv4-only | ipv6-only ] [ default-nat-realm
nat_realm_name [ fw-and-nat-action action_name ] ]
no nat policy
```

**no**

Disables both NAT44 and NAT64 support in the Firewall-and-NAT policy.

**nat-required**

Enables NAT support in the Firewall-and-NAT policy.



## Important

This keyword is available only in 12.1 and earlier releases, and is supported in release 12.2 for backward compatibility. The **nat policy nat-required** command enables only NAT44.

**ipv4-and-ipv6**

Enables NAT processing for both IPv4 and IPv6 in the Firewall-and-NAT policy.

**ipv4-only**

Enables NAT processing for IPv4 in the Firewall-and-NAT policy.



**ipv6-only**

Enables NAT processing for IPv6 in the Firewall-and-NAT policy.

**default-nat-realm *nat\_realm\_name***

Specifies the default NAT realm for the Firewall-and-NAT policy.

*nat\_realm\_name* must be the name of an existing NAT realm, and must be an alphanumeric string of 1 through 31 characters.

**fw-and-nat-action *action\_name***

Specifies the Firewall-and-NAT action name.

*action\_name* must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to enable/disable IPv4 and/or IPv6 NAT support for all subscribers using a Firewall-and-NAT policy.

In release 8.1, to enable NAT support for a subscriber, Stateful Firewall must also be enabled for that subscriber. See the **firewall policy** CLI command.

Once NAT is enabled for a subscriber, the NAT IP address to be used is chosen from the NAT realms specified in the rules. See the **access-rule** CLI command.

You can enable/disable NAT at any time, however the changed NAT status will not be applied to active calls. The new NAT status will only be applied to new calls.

**Example**

The following command enables NAT support in a Firewall-and-NAT policy:

```
nat policy nat-required
```

The following command disables NAT support in a Firewall-and-NAT policy:

```
no nat policy
```

The following command enables IPv4 and IPv6 NAT support in a Firewall-and-NAT policy:

```
nat policy ipv4-and-ipv6
```

## nat private-ip-flow-timeout

This command configures the Private IP NPU flow timeout setting.

**Product**

NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

**active-charging service *service\_name* > fw-and-nat policy *policy\_name***

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax Description**

```
nat private-ip-flow-timeout timeout
{ default | no } nat private-ip-flow-timeout
```

**default**

Configures the default setting.

Default: 180 seconds

**no**

Disables the Private IP NPU flow timeout configuration.

When disabled, the flow is installed at call setup and will be removed only when the subscriber disconnects.

**timeout**

Specifies the Private IP NPU flow timeout period in seconds.

*timeout* must be an integer from 180 through 86400.

**Usage Guidelines**

Use this command to configure the Private IP NPU flow timeout setting.

For NAT-enabled calls, by default, the downlink private IP NPU flow will not be installed at call setup for a subscriber session. The flow will only be installed on demand. When there is no traffic on the private flow, the private IP flow will be removed after the configurable timeout period.

**Example**

The following command configures the Private IP NPU flow timeout setting to *36000* seconds:

```
nat private-ip-flow-timeout 36000
```

## nat suppress-aaa-update

This command suppresses sending NAT Bind Update (NBU) to the AAA server when PPP disconnect happens.

**Important**

This command is customer-specific. For more information please contact your local service representative.

**Product**

NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

```
active-charging service service_name > fw-and-nat policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax Description**

```
nat suppress-aaa-update call-termination
default nat suppress-aaa-update
```

**default**

Configures the default setting.

Default: No suppression of AAA updates.

**Usage Guidelines**

Use this command to suppress sending of NBU to the AAA server when PPP disconnect happens, as these NBUs would be cleared at the AAA after receiving the accounting-stop. This enables to minimize the number of messages between the chassis and AAA server. When not configured, NBU are sent to the AAA server whenever a port chunk is allocated, de-allocated, or the call is cleared (PPP disconnect).

**Example**

The following command suppresses the sending of NBU to the AAA server:

```
nat suppress-aaa-update call-termination
```

**nat suppress-aaa-update**



## CHAPTER 30

# Firewall-and-NAT Access Ruledef Configuration Mode Commands

The Firewall-and-NAT Access Ruledef Configuration Mode is used to configure and manage Access rule definitions used by the Stateful Firewall (FW) and Network Address Translation (NAT) in-line services.

### Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```



### Important

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

- [bearer 3gpp apn](#), on page 1320
- [bearer 3gpp imsi](#), on page 1321
- [bearer username](#), on page 1322
- [create-log-record](#), on page 1323
- [end](#), on page 1324
- [exit](#), on page 1324
- [icmp any-match](#), on page 1325
- [icmp code](#), on page 1326
- [icmp type](#), on page 1327
- [icmpv6 any-match](#), on page 1328
- [icmpv6 code](#), on page 1329
- [icmpv6 type](#), on page 1330
- [ip any-match](#), on page 1331
- [ip downlink](#), on page 1332
- [ip dst-address](#), on page 1333
- [ip protocol](#), on page 1334
- [ip server-ip-address](#), on page 1335
- [ip server-ipv6-network-prefix](#), on page 1336
- [ip src-address](#), on page 1337

- [ip uplink](#), on page 1339
- [ip version](#), on page 1340
- [tcp any-match](#), on page 1340
- [tcp client-port](#), on page 1341
- [tcp dst-port](#), on page 1343
- [tcp either-port](#), on page 1344
- [tcp server-port](#), on page 1346
- [tcp src-port](#), on page 1347
- [udp any-match](#), on page 1348
- [udp client-port](#), on page 1349
- [udp dst-port](#), on page 1351
- [udp either-port](#), on page 1352
- [udp server-port](#), on page 1353
- [udp src-port](#), on page 1355

## bearer 3gpp apn

This command configures an access ruledef to analyze user traffic based on APN bearer.

---

### Product

PSF  
NAT

---

### Privilege

Security Administrator, Administrator

---

### Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

---

### Syntax Description

[ **no** ] **bearer 3gpp apn** [ **case-sensitive** ] *operator value*

#### **no**

Removes previously configured bearer ruledef.

#### **case-sensitive**

This keyword makes the rule case sensitive.

By default, ruledefs are not case sensitive.

Default: Disabled

#### **operator**

Specifies how to logically match the APN name.

*operator* 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

**value**

The APN name to match in bearer flow.

*value* must be an alphanumeric string of 1 through 63 characters that can include punctuation characters.

**Usage Guidelines**

Use this command to specify an access ruledef to analyze user traffic based on APN name.

**Example**

The following command creates an access ruledef for analyzing user traffic for an APN named *apn12*:

```
bearer 3gpp apn = apn12
```

## bearer 3gpp imsi

This command configures an access ruledef to analyze user traffic based on International Mobile Station Identification (IMSI) number in bearer flow.

**Product**

PSF  
NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

```
active-charging service service_name > access-ruledef access_ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

**Syntax Description**

```
[ no ] bearer 3gpp imsi { operator msid | { !range | range } imsi-pool imsi_pool }
```

**no**

Removes previously configured bearer ruledef.

**bearer username*****operator***

Specifies how to logically match the MSID.

*operator* must be one of the following:

- **! =**: Does not equal
- **=**: Equals

***msid***

Specifies the Mobile Station Identifier.

**{ !range | range } imsi-pool *imsi\_pool***

**{ !range | range }**: Specifies the range criteria:

- **!range**: Not in the range of
- **range**: In the range of

**imsi-pool *imsi\_pool***: Specifies the IMSI pool name. *imsi\_pool* must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to specify an access ruledef to analyze user traffic based on IMSI number of mobile station.

**Example**

The following command creates an access ruledef to analyze user traffic for the IMSI number 9198838330912:

```
bearer 3gpp imsi = 9198838330912
```

## bearer username

This command configures an access ruledef to analyze user traffic based on user name of the bearer flow.

**Product**

PSF  
NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

**active-charging service *service\_name* > access-ruledef *access\_ruledef\_name***

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

**Syntax Description**

**[ no ] bearer username [ case-sensitive ] operator value**



**no**

Removes previously configured bearer ruledef.

**case-sensitive**

This keyword makes the rule case sensitive.

By default, ruledefs are not case sensitive.

Default: Disabled

**operator**

Specifies how to logically match the MSID.

*operator* 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

**value**

Specifies the user name.

*value* must be an alphanumeric string of 1 through 127 characters.

---

**Usage Guidelines**

Use this command to specify a access ruledef to analyze user traffic based on user name of the bearer flow.

**Example**

The following command creates an access ruledef for analyzing user traffic for the user name *user12*:

```
bearer username = user12
```

## create-log-record

This command enables/disables access ruledef logging.

---

**Product**

PSF

NAT

**end**

<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration <b>active-charging service</b> <i>service_name</i> > <b>access-ruledef</b> <i>access_ruledef_name</i> Entering the above command sequence results in the following prompt: [local] <i>host_name</i> (config-acs-fw-ruledef) #
<b>Syntax Description</b>	[ <b>no</b> ] <b>create-log-record</b>  <b>no</b> Disables access ruledef logging.
<b>Usage Guidelines</b>	Use this command to enable/disable access ruledef logging.

**Example**

The following command enables access ruledef logging:

```
create-log-record
```

The following command disables access ruledef logging:

```
no create-log-record
```

## end

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

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Syntax Description</b>	<b>end</b>
<b>Usage Guidelines</b>	Use this command to return to the Exec mode.

## exit

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

<b>Product</b>	All
<b>Privilege</b>	Security Administrator, Administrator
<b>Syntax Description</b>	<b>exit</b>
<b>Usage Guidelines</b>	Use this command to return to the parent configuration mode.

# icmp any-match

This command configures an access ruledef to match any ICMPv4 traffic for the user.

---

**Product**

PSF  
NAT

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

---

**Syntax Description**

```
[ no ] icmp any-match operator condition
```

**no**

Removes previously configured ICMPv4 any-match ruledef.

**operator**

Specifies how to logically match the analyzed state.

*operator* must be one of the following:

- **! =**: Does not equal
- **=**: Equals

**condition**

Specifies the condition to be matched for the user traffic.

*condition* must be one of the following:

- **FALSE**: Specified condition is FALSE.
- **TRUE**: Specified condition is TRUE.

---

**Usage Guidelines**

Use this command to specify an access ruledef to match any ICMPv4 traffic of the user.

**Example**

The following command creates an access ruledef to match any non-ICMPv4 traffic of the user:

```
icmp any-match = FALSE
```

# icmp code

This command configures an access ruledef to analyze user traffic based on ICMPv4 code.

---

## Product

PSF  
NAT

---

## Privilege

Security Administrator, Administrator

---

## Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

---

## Syntax Description

[ **no** ] **icmp code** *operator code*

### **no**

Removes previously configured ICMPv4 code ruledef.

### **operator**

Specifies how to logically match the ICMPv4 code.

*operator* must be one of the following:

- **! =**: Does not equal
- **< =**: Less than or equals
- **=**: Equals
- **> =**: Greater than or equals

### **code**

Specifies the ICMPv4 code.

*code* must be an integer from 0 through 255.

---

## Usage Guidelines

Use this command to define an access ruledef to analyze user traffic based on the ICMPv4 code.

### **Example**

The following command creates an access ruledef for analyzing user traffic using the ICMPv4 code as 23:

```
icmp code = 23
```

# icmp type

This command configures an access ruledef to analyze user traffic based on ICMPv4 type.

---

**Product**

PSF  
NAT

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

---

**Syntax Description**

[ **no** ] **icmp type** *operator type*

**no**

Removes previously configured ICMPv4 type ruledef.

**operator**

Specifies how to logically match the ICMPv4 type.

*operator* must be one of the following:

- **! =**: Does not equal
- **< =**: Less than or equals
- **=**: Equals
- **> =**: Greater than or equals

**type**

Specifies the ICMPv4 type.

*type* must be an integer from 0 through 255.

For example, 0 for ECHO Reply, 3 for Dest. Unreachable, and 5 for Redirect.

---

**Usage Guidelines**

Use this command to define an access ruledef to analyze user traffic based on the ICMPv4 type.

**Example**

The following command creates an access ruledef for analyzing user traffic using an ICMPv4 type as *123*:

```
icmp type = 123
```

# icmpv6 any-match

This command configures an access ruledef to match any ICMPv6 traffic for the user.

---

## Product

PSF  
NAT

---

## Privilege

Security Administrator, Administrator

---

## Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

---

## Syntax Description

[ **no** ] **icmpv6 any-match** *operator condition*

### **no**

Removes previously configured ICMPv6 any-match ruledef.

### **operator**

Specifies how to logically match the analyzed state.

*operator* must be one of the following:

- **! =**: Does not equal
- **=**: Equals

### **condition**

Specifies the condition to be matched for the user traffic.

*condition* must be one of the following:

- **FALSE**: Specified condition is FALSE.
- **TRUE**: Specified condition is TRUE.

---

## Usage Guidelines

Use this command to specify an access ruledef to match any ICMPv6 traffic of the user.

### Example

The following command creates an access ruledef to match any non-ICMPv6 traffic of the user:

```
icmpv6 any-match = FALSE
```

# icmpv6 code

This command configures an access ruledef to analyze user traffic based on ICMPv6 code.

---

**Product**

PSF  
NAT

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

---

**Syntax Description**

[ **no** ] **icmpv6 code** *operator code*

**no**

Removes previously configured ICMPv6 code ruledef.

**operator**

Specifies how to logically match the ICMPv6 code.

*operator* must be one of the following:

- **! =**: Does not equal
- **< =**: Less than or equals
- **=**: Equals
- **> =**: Greater than or equals

**code**

Specifies the ICMPv6 code.

*code* must be an integer from 0 through 255.

---

**Usage Guidelines**

Use this command to define an access ruledef to analyze user traffic based on the ICMPv6 code.

**Example**

The following command creates an access ruledef for analyzing user traffic using the ICMPv6 code as 23:

```
icmpv6 code = 23
```

# icmpv6 type

This command configures an access ruledef to analyze user traffic based on ICMPv6 type.

---

## Product

PSF  
NAT

---

## Privilege

Security Administrator, Administrator

---

## Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

---

## Syntax Description

[ **no** ] **icmpv6 type** *operator type*

### **no**

Removes previously configured ICMPv6 type ruledef.

### **operator**

Specifies how to logically match the ICMPv6 type.

*operator* must be one of the following:

- !=: Does not equal
- <=: Less than or equals
- =: Equals
- >=: Greater than or equals

### **type**

Specifies the ICMPv6 type.

*type* must be an integer from 0 through 255.

For example, 0 for ECHO Reply, 3 for Dest. Unreachable, and 5 for Redirect.

---

## Usage Guidelines

Use this command to define an access ruledef to analyze user traffic based on the ICMPv6 type.

### **Example**

The following command creates an access ruledef for analyzing user traffic using an ICMPv6 type as 123:

```
icmpv6 type = 123
```



# ip any-match

This command configures an access ruledef to match any IP traffic for the user.

---

**Product**

PSF  
NAT

---

**Privilege**

Security Administrator, Administrator

---

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

---

**Syntax Description**

[ **no** ] **ip any-match** *operator condition*

**no**

Removes previously configured IP any-match ruledef.

**operator**

Specifies how to logically match the analyzed state.

*operator* must be one of the following:

- **! =**: Does not equal
- **=**: Equals

**condition**

Specifies the condition to be matched for the user traffic.

*condition* must be one of the following:

- **FALSE**: Specified condition is FALSE.
- **TRUE**: Specified condition is TRUE.

---

**Usage Guidelines**

Use this command to specify an access ruledef to match any IP traffic of the user.

**Example**

The following command creates an access ruledef to match any non-IP traffic of the user:

```
ip any-match = FALSE
```

# ip downlink

This command configures an access ruledef to analyze user traffic based on IP packet flow in downlink direction (to subscriber).

---

## Product

PSF  
NAT

---

## Privilege

Security Administrator, Administrator

---

## Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

---

## Syntax Description

[ **no** ] **ip downlink** *operator condition*

### **no**

Removes previously configured IP ruledef.

### **operator**

Specifies how to logically match the packet flow direction.

*operator* must be one of the following:

- **!=**: Does not equal
- **=**: Equals

### **condition**

Specifies the condition to match.

*condition* must be one of the following:

- **TRUE**: Analyzed
- **FALSE**: Not analyzed

---

## Usage Guidelines

Use this command to define an access ruledef to analyze user traffic based on the IP packet flow direction as downlink.

## Example

The following command creates access ruledef for analyzing user traffic using an IP packet direction to downlink (to subscriber):

```
ip downlink = TRUE
```

# ip dst-address

This command configures an access ruledef to analyze user traffic based on IP destination address.

---

## Product

PSF  
NAT

---

## Privilege

Security Administrator, Administrator

---

## Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

---

## Syntax Description

```
[ no ] ip dst-address { operator { ipv4/ipv6_address | ipv4/ipv6_address/mask } |
{ !range | range } host-pool host_pool }
```

### no

Removes previously configured IP destination address ruledef.

### **operator**{ *ipv4/ipv6\_address* | *ipv4/ipv6\_address/mask* }

*operator* specifies how to logically match the IP destination address.

*operator* must be one of the following:

- **!:=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

*ipv4/ipv6\_address*: Specifies the IP address of destination node for outgoing traffic. *ipv4/ipv6\_address* must be the IP address entered using IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.

*ipv4/ipv6\_address/mask*: Specifies the IP address of destination node for outgoing traffic.

*ipv4/ipv6\_address/mask* must be the IP address entered using IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation. The mask bit is a numeric value which is the number of bits in the subnet mask.

### **{ !range | range } host-pool** *host\_pool* }

**!range** | **range**: Specifies the range criteria:

- **!range**: Not in the range of
- **range**: In the range of

**host-pool** *host\_pool*: Specifies the host pool name. *host\_pool* must be an alphanumeric string of 1 through 63 characters.

### Usage Guidelines

Use this command to specify an access ruledef to analyze user traffic based on the IP destination address.

### Example

The following command creates IP ruledef for analyzing user traffic using an IP destination address of *10.1.1.1*:

```
ip dst-address = 10.1.1.1
```

## ip protocol

This command configures an access ruledef to analyze user traffic based on the protocol being transported by IP packets.

### Product

PSF  
NAT

### Privilege

Security Administrator, Administrator

### Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

### Syntax Description

```
[ no ] ip protocol { { operator { protocol | protocol_assignment } } | { operator  
protocol_assignment } }
```

#### no

Removes previously configured IP protocol address ruledef.

#### **operator{ protocol | protocol\_assignment }**

*operator*: Specifies how to logically match the IP protocol.

*operator* must be one of the following:

- !=: Does not equal
- =: Equals

*protocol*: Specifies the protocol by name.

*protocol* must be one of the following:

- ah
- esp

- gre
- icmp
- tcp
- udp

*protocol\_assignment*: Specifies the protocol by assignment number. *protocol\_assignment* must be an integer from 0 through 255 (for example, 1 for ICMP, 6 for TCP, and 17 for UDP).

#### ***operator protocol\_assignment***

*operator*: Specifies how to logically match the IP protocol.

*operator* must be one of the following:

- <=: Less than or equals
- >=: Greater than or equals

*protocol\_assignment*: Specifies the protocol by assignment number.

*protocol\_assignment* must be an integer from 0 through 255 (for example, 1 for ICMP, 6 for TCP, and 17 for UDP).

#### **Usage Guidelines**

Use this command to specify an access ruledef to analyze user traffic based on the IP protocol.

#### **Example**

The following command creates IP ruledef for analyzing user traffic using a protocol assignment of 1:

```
ip protocol = 1
```

## ip server-ip-address

This command configures an access ruledef to analyze user traffic based on IP server address.

#### **Product**

PSF  
NAT

#### **Privilege**

Security Administrator, Administrator

#### **Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

#### **Syntax Description**

```
[ no ] ip server-ip-address { operator { ipv4/ipv6_address | ipv4/ipv6_address/mask } | { !range | range } host-pool host_pool_name }
```

**no**

Removes previously configured IP server address.

**operator**{ *ipv4/ipv6\_address* | *ipv4/ipv6\_address/mask*}

*operator*: Specifies how to logically match the IP server address.

*operator* must be one of the following:

- **!=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

*ipv4/ipv6\_address*: Specifies the server IP address. For uplink packets (subscriber to network), this field matches the destination IP address in the IP header. For downlink packets (network to subscriber), this field matches the source IP address in the IP header. *ipv4/ipv6\_address* must be an IP address in IPv4-dotted decimal notation or IPv6 colon-separated hexadecimal notation.

*ipv4/ipv6\_address/mask*: Specifies the server IP address with subnet mask bit. For uplink packets (subscriber to network), this field matches the destination IP address in the IP header. For downlink packets (network to subscriber), this field matches the source IP address in the IP header. *ipv4/ipv6\_address/mask* must be an IP address in IPv4 dotted-decimal notation or IPv6 colon-separated hexadecimal notation with subnet mask bit. The mask bit is a numeric value which is the number of bits in the subnet mask.

**{ !range | range } host-pool *host\_pool\_name***

**{ !range | range }**: Specifies the range criteria.

- **!range**: Not in the range of
- **range**: In the range of

**host-pool *host\_pool\_name***: Specifies name of the host pool. *host\_pool\_name* must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to specify an access ruledef to analyze user traffic based on IPv4 or IPv6 server address. For uplink packets, this field matches the destination IP address in the IP header. For downlink packets, this field matches the source IP address in the IP header.

**Example**

The following command creates an IP ruledef for analyzing user traffic using IPv4 server address *10.1.1.1*:

```
ip server-ip-address = 10.1.1.1
```

## ip server-ipv6-network-prefix

This command configures an access ruledef to analyze user traffic based on IPv6 server prefix.

<b>Product</b>	PSF NAT
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration <b>active-charging service</b> <i>service_name</i> > <b>access-ruledef</b> <i>access_ruledef_name</i> Entering the above command sequence results in the following prompt: [local]host_name(config-acs-fw-ruledef)#
<b>Syntax Description</b>	<b>[ no ] ip server-ipv6-network-prefix</b> <i>operator ipv6_prefix/prefix_length</i>  <b>no</b> Removes previously configured IPv6 server prefix.  <b>operator ipv6_prefix/prefix_length</b> <i>operator</i> : Specifies how to logically match the IPv6 server prefix. <i>operator</i> must be one of the following: <ul style="list-style-type: none"> <li>• !=: Does not equal</li> <li>• =: Equals</li> </ul> <i>ipv6_prefix/prefix_length</i> : Specifies the server's IPv6 address with subnet mask bit. <i>ipv6_prefix/prefix_length</i> must be in IPv6 colon-separated-hexadecimal notation with subnet mask bit. The <i>prefix_length</i> is the number of bits to match. The configurable prefix length values are 32, 40, 48, 56, 64 and 96.
<b>Usage Guidelines</b>	Use this command to specify an access ruledef to analyze user traffic based on IPv6 server prefix. When a first packet for a flow is received, it is matched against a set of rules configured in the Firewall-and-NAT policy. If the incoming IPv6 packet matches a ruledef and configured prefix, then it indicates that NAT64 needs to be applied on the packet. If the packet did not match the prefix configured, then NAT64 will not be applied on the packet. If there is no rule matching the packet or if there is no rule configured, then the incoming IPv6 packet is matched against the well-known prefix. If the well-known prefix matches, then NAT64 is applied on the packet.

**Example**

The following command creates an IP ruledef to analyze user traffic using the IPv6 server prefix *abcd:dcba* with 32 bits of the server IPv6 address:

```
ip server-ipv6-network-prefix = abcd:dcba::/32
```

## ip src-address

This command configures an access ruledef to analyze user traffic based on IP source address.

<b>Product</b>	PSF NAT
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration <b>active-charging service</b> <i>service_name</i> > <b>access-ruledef</b> <i>access_ruledef_name</i> Entering the above command sequence results in the following prompt: [local] <i>host_name</i> (config-acs-fw-ruledef) #
<b>Syntax Description</b>	<pre>[ no ] ip src-address { operator { ipv4/ipv6_address   ipv4/ipv6_address/mask }   { !range   range } host-pool host_pool }</pre> <p><b>no</b> Removes previously configured IP destination address ruledef.</p> <p><b>operator{ ipv4/ipv6_address   ipv4/ipv6_address/mask }</b> <i>operator</i>: Specifies how to logically match the IP source address. <i>operator</i> must be one of the following:</p> <ul style="list-style-type: none"> <li>• !=: Does not equal</li> <li>• &lt;=: Less than or equals</li> <li>• =: Equals</li> <li>• &gt;=: Greater than or equals</li> </ul> <p><i>ipv4/ipv6_address</i>: Specifies the IP address using IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.</p> <p><i>ipv4/ipv6_address/mask</i>: Specifies the IP address using IPV4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation with subnet mask bit. The mask bit is a numeric value which is the number of bits in the subnet mask.</p> <p><b>{ !range   range } host-pool host_pool</b> <b>!range   range</b>: Specifies the range criteria:</p> <ul style="list-style-type: none"> <li>• <b>!range</b>: Not in the range of</li> <li>• <b>range</b>: In the range of</li> </ul> <p><b>host-pool host_pool</b>: Specifies the host pool name. <i>host_pool</i> must be an alphanumeric string of 1 through 63 characters.</p>
<b>Usage Guidelines</b>	Use this command to specify an access ruledef to analyze user traffic based on the IP source address.



**Example**

The following command creates IP ruledef for analyzing user traffic using an IP source address of *10.1.1.1*:

```
ip src-address = 10.1.1.1
```

# ip uplink

This command configures an access ruledef to analyze user traffic based on IP packet flow in the uplink direction (from subscriber).

**Product**

PSF  
NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

**Syntax Description**

```
[ no ] ip uplink operator condition
```

**no**

Removes previously configured IP uplink match ruledef.

**operator**

Specifies how to logically match the IP packet flow direction.

*operator* must be one of the following:

- **! =**: Does not equal
- **=**: Equals

**condition**

Specifies the condition to match.

*condition* must be one of the following:

- **TRUE**: Not analyzed
- **FALSE**: Analyzed

**Usage Guidelines**

Use this command to define an access ruledef to analyze user traffic based on the IP packet flow direction as uplink.

**Example**

The following command creates access ruledef for analyzing user traffic using an IP packet direction to uplink (from subscriber):

```
ip uplink = TRUE
```

## ip version

This command defines rule expressions to match version number in IP header.

**Product**

PSF  
NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

**Syntax Description**

```
[ no ] ip version = { ipv4 | ipv6 }
```

**no**

Deletes the specified rule expression.

**ipv4**

Specifies the rule expression for IP version 4.

**ipv6**

Specifies the rule expression for IP version 6.

**Usage Guidelines**

Use this command to define rule expressions to match IPv4/IPv6 version number in IP header.

**Example**

The following command defines a rule expression to match user traffic for the IP version **ipv6**:

```
ip version = ipv6
```

## tcp any-match

This command configures an access ruledef to match any TCP traffic for the user.

<b>Product</b>	PSF NAT
<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration <b>active-charging service</b> <i>service_name</i> > <b>access-ruledef</b> <i>access_ruledef_name</i> Entering the above command sequence results in the following prompt: [local] <i>host_name</i> (config-acs-fw-ruledef)#
<b>Syntax Description</b>	[ <b>no</b> ] <b>tcp any-match</b> <i>operator condition</i>  <b>no</b> Removes previously configured TCP any-match ruledef.  <b>operator</b> Specifies how to logically match the analyzed state. <i>operator</i> must be one of the following: <ul style="list-style-type: none"> <li>• <b>! =</b>: Does not equal</li> <li>• <b>=</b>: Equals</li> </ul> <b>condition</b> Specifies the condition to be matched for the user traffic. <i>condition</i> must be one of the following: <ul style="list-style-type: none"> <li>• <b>FALSE</b>: Specified condition is FALSE.</li> <li>• <b>TRUE</b>: Specified condition is TRUE.</li> </ul>
<b>Usage Guidelines</b>	Use this command to specify an access ruledef to match any TCP traffic of the user.

**Example**

The following command creates an access ruledef to match any non-TCP traffic of the user:

```
tcp any-match = FALSE
```

## tcp client-port

This command configures an access ruledef to analyze user traffic based on client TCP port.

<b>Product</b>	PSF
----------------	-----

<b>Privilege</b>	Security Administrator, Administrator
<b>Command Modes</b>	Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration <b>active-charging service</b> <i>service_name</i> > <b>access-ruledef</b> <i>access_ruledef_name</i> Entering the above command sequence results in the following prompt: <pre>[local]host_name(config-acs-fw-ruledef)#</pre>
<b>Syntax Description</b>	<pre>[ no ] tcp client-port { operator port_number   { !range   range } { start_range to end_range   port-map port_map } }</pre> <p><b>no</b> Removes the previously configured client TCP port ruledef.</p> <p><b>operator</b> Specifies how to logically match the port number. <i>operator</i> must be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>! =</b>: Does not equal</li> <li>• <b>&lt; =</b>: Less than or equals</li> <li>• <b>=</b>: Equals</li> <li>• <b>&gt; =</b>: Greater than or equals</li> </ul> <p><b>port_number</b> Specifies the port number to match. <i>port_number</i> must be an integer from 1 through 65535.</p> <p><b>range   !range</b> Specifies the range criteria:</p> <ul style="list-style-type: none"> <li>• <b>!range</b>: Not in the range</li> <li>• <b>range</b>: In the range</li> </ul> <p><b>start_range to end_range</b> Specifies the starting and ending port numbers for the range of destination TCP ports. <i>start_range</i> must be an integer from 1 through 65535. <i>end_range</i> must be an integer from 1 through 65535 that is greater than <i>start_range</i>.</p> <p><b>port-map port_map</b> Specifies name of the port-map for the port range. <i>port_map</i> must be an alphanumeric string of 1 through 63 characters.</p>

**Usage Guidelines** Use this command to specify an access ruledef to analyze user traffic based on client TCP port.

### Example

The following command creates an access ruledef for analyzing user traffic matching client port for TCP as 50:

```
tcp client-port = 50
```

## tcp dst-port

This command configures an access ruledef to analyze user traffic based on destination TCP port.

### Product

PSF  
NAT

### Privilege

Security Administrator, Administrator

### Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration  
**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

### Syntax Description

```
[ no ] tcp dst-port { operator port_number | { !range | range } { start_range  
to end_range | port-map port_map } }
```

#### no

Removes the previously configured destination TCP port ruledef.

#### operator

Specifies how to logically match the port number.

*operator* must be one of the following:

- !=: Does not equal
- <=: Less than or equals
- =: Equals
- >=: Greater than or equals

#### port\_number

Specifies the port number to match.

*port\_number* must be an integer from 1 through 65535.

**range | !range**

Specifies the range criteria:

- **!range**: Not in the range
- **range**: In the range

**start\_range to end\_range**

Specifies the starting and ending port numbers for the range of destination TCP ports.

*start\_range* must be an integer from 1 through 65535.

*end\_range* must be an integer from 1 through 65535 that is greater than *start\_range*.

**port-map port\_map**

Specifies name of the port-map for the port range.

*port\_map* must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to specify an access ruledef to analyze user traffic based on destination TCP port.

**Example**

The following command creates an access ruledef for analyzing user traffic matching destination port for TCP as *10*:

```
tcp dst-port = 10
```

## tcp either-port

This command configures an access ruledef to analyze user traffic based on either (destination or source) TCP ports.

**Product**

PSF  
NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

**Syntax Description**

```
[ no ] tcp either-port { operator port_number | { !range | range } { start_range  
to end_range | port-map port_map } }
```

**no**

Removes previously configured TCP either-port (destination or source) ruledef.

**operator**

Specifies how to logically match the port number.

*operator* must be one of the following:

- **!:=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

**port\_number**

Specifies the port number to match.

*port\_number* must be an integer from 1 through 65535.

**range | !range**

Specifies the range criteria:

- **!range**: Not in the range
- **range**: In the range

**start\_range to end\_range**

Specifies the starting and ending port numbers for the port range.

*start\_range* must be an integer from 1 through 65535.

*end\_range* must be an integer from 1 through 65535 that is greater than *start\_range*.

**port-map port\_map**

Specifies name of the port-map for the port range.

*port\_map* must be an alphanumeric string of 1 through 63 characters.

---

**Usage Guidelines**

Use this command to specify an access ruledef to analyze user traffic based on either TCP port.

**Example**

The following command creates an access ruledef for analyzing user traffic matching destination or source port for TCP as *10*:

```
tcp either-port = 10
```

## tcp server-port

This command configures an access ruledef to analyze user traffic based on server TCP port.

---

### Product

PSF

---

### Privilege

Security Administrator, Administrator

---

### Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

---

### Syntax Description

```
[ no ] tcp server-port { operator port_number | { !range | range } { start_range  
to end_range | port-map port_map } }
```

#### **no**

Removes the previously configured server TCP port ruledef.

#### **operator**

Specifies how to logically match the port number.

*operator* must be one of the following:

- **!=:** Does not equal
- **<=:** Less than or equals
- **=:** Equals
- **>=:** Greater than or equals

#### **port\_number**

Specifies the port number to match.

*port\_number* must be an integer from 1 through 65535.

#### **range** | **!range**

Specifies the range criteria:

- **!range:** Not in the range
- **range:** In the range

#### **start\_range** to **end\_range**

Specifies the starting and ending port numbers for the range of destination TCP ports.

*start\_range* must be an integer from 1 through 65535.



*end\_range* must be an integer from 1 through 65535 that is greater than *start\_range*.

**port-map** *port\_map*

Specifies name of the port-map for the port range.

*port\_map* must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to specify an access ruledef to analyze user traffic based on server TCP port.

**Example**

The following command creates an access ruledef for analyzing user traffic matching server port for TCP as *100*:

```
tcp server-port = 100
```

## tcp src-port

This command configures an access ruledef to analyze user traffic based on source TCP port.

**Product**

PSF  
NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration  
**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

**Syntax Description**

```
[ no ] tcp src-port { operator port_number | { !range | range } { start_range  
to end_range | port-map port_map } }
```

**no**

Removes previously configured source TCP port ruledef.

**operator**

Specifies how to logically match the port number.

*operator* must be one of the following:

- !=: Does not equal
- <=: Less than or equals
- =: Equals
- >=: Greater than or equals

***port\_number***

Specifies the port number to match.

*port\_number* must be an integer from 1 to 65535.

***range | !range***

Specifies the range criteria:

- **!range**: Not in the range
- **range**: In the range

***start\_range to end\_range***

Specifies the starting and ending port numbers for the port range.

*start\_range* must be an integer from 1 through 65535.

*end\_range* must be an integer from 1 through 65535 that is greater than *start\_range*.

***port-map port\_map***

Specifies name of the port-map for the port range.

*port\_map* must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to specify an access ruledef to analyze user traffic based on source TCP port.

**Example**

The following command creates an access ruledef for analyzing user traffic matching source port for TCP as *10*:

```
tcp src-port = 10
```

## udp any-match

This command configures an access ruledef to match any UDP traffic for the user.

**Product**

PSF  
NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration  
**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

**Syntax Description**    `[ no ] udp any-match operator condition`

**no**

Removes previously configured UDP any-match ruledef.

**operator**

Specifies how to logically match the analyzed state.

*operator* must be one of the following:

- **! =**: does not equal
- **=**: equals

**condition**

Specifies the condition to be matched for the user traffic.

*condition* must be one of the following:

- **FALSE**: Specified condition is FALSE.
- **TRUE**: Specified condition is TRUE.

**Usage Guidelines**

Use this command to specify an access ruledef to match any UDP traffic of the user.

**Example**

The following command creates an access ruledef to match any UDP traffic of the user:

```
udp any-match = TRUE
```

## udp client-port

This command configures an access ruledef to analyze user traffic based on client UDP port.

**Product**

PSF  
NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration  
**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

**Syntax Description**

```
[ no ] udp client-port { operator port_number | { !range | range } { start_range  
to end_range | port-map port_map } }
```

**no**

Removes previously configured client UDP port ruledef.

**operator**

Specifies how to logically match the port number.

*operator* must be one of the following:

- **!<=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

**port\_number**

Specifies the port number to match.

*port\_number* must be an integer from 1 through 65535.

**!range | range**

Specifies the range criteria.

- **!range**: Not in the range
- **range**: In the range

**start\_range to end\_range**

Specifies the starting and ending port numbers for the port range.

*start\_range* must be an integer from 1 through 65535.

*end\_range* must be an integer from 1 through 65535 that is greater than *start\_range*.

**port-map port\_map**

Specifies name of the port-map for the port range.

*port\_map* must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to specify an access ruledef to analyze user traffic based on client UDP port.

**Example**

The following command creates an access ruledef for analyzing user traffic matching client port for UDP as 10:

```
udp client-port = 10
```

## udp dst-port

This command configures an access ruledef to analyze user traffic based on destination UDP port.

---

### Product

PSF  
NAT

---

### Privilege

Security Administrator, Administrator

---

### Command Modes

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

---

### Syntax Description

```
[ no ] udp dst-port { operator port_number | { !range | range } { start_range  
to end_range | port-map port_map } }
```

#### **no**

Removes previously configured destination UDP ports ruledef.

#### ***operator***

Specifies how to logically match the port number.

*operator* must be one of the following:

- **!:=**: Does not equal
- **<=**: Less than or equals
- **=**: Equals
- **>=**: Greater than or equals

#### ***port\_number***

Specifies the port number to match.

*port\_number* must be an integer from 1 through 65535.

#### **!range | range**

Specifies the range criteria.

- **!range**: Not in the range
- **range**: In the range

#### ***start\_range to end\_range***

Specifies the starting and ending port numbers for the port range.

*start\_range* must be an integer from 1 through 65535.

*end\_range* must be an integer from 1 through 65535 that is greater than *start\_range*.

#### **port-map *port\_map***

Specifies name of the port-map for the port range.

*port\_map* must be an alphanumeric string of 1 through 63 characters.

#### **Usage Guidelines**

Use this command to specify an access ruledef to analyze user traffic based on destination UDP port.

#### **Example**

The following command creates an access ruledef for analyzing user traffic matching destination port for UDP as 10:

```
udp dst-port = 10
```

## udp either-port

This command configures an access ruledef to analyze user traffic based on either (destination or source) UDP port.

#### **Product**

PSF  
NAT

#### **Privilege**

Security Administrator, Administrator

#### **Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

**active-charging service *service\_name* > access-ruledef *access\_ruledef\_name***

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

#### **Syntax Description**

```
[ no ] udp either-port { operator port_number | { !range | range } { start_range  
to end_range | port-map port_map } }
```

#### **no**

Removes previously configured either-port (destination or source) UDP ruledef.

#### **operator**

Specifies how to logically match the port number.

*operator* must be one of the following:

- !=: Does not equal
- <=: Less than or equals

- =: Equals
- >=: Greater than or equals

***port\_number***

Specifies the port number to match.

*port\_number* must be an integer from 1 through 65535.

***!range | range***

Specifies the range criteria.

- ***!range***: Not in the range
- ***range***: In the range

***start\_range to end\_range***

Specifies the starting and ending port numbers for the port range.

*start\_range* must be an integer from 1 through 65535.

*end\_range* must be an integer from 1 through 65535 that is greater than *start\_range*.

***port-map port\_map***

Specifies name of the port-map for the port range.

*port\_map* must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to specify an access ruledef to analyze user traffic based on either UDP port.

**Example**

The following command creates an access ruledef for analyzing user traffic matching destination or source port for UDP as 10:

```
udp either-port = 10
```

## udp server-port

This command configures an access ruledef to analyze user traffic based on server UDP port.

**Product**

PSF  
NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration  
**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef) #
```

### Syntax Description

```
[ no ] udp server-port { operator port_number | { !range | range } { start_range
to end_range | port-map port_map } }
```

#### **no**

Removes previously configured server UDP port ruledef.

#### **operator**

Specifies how to logically match the port number.

*operator* must be one of the following:

- **! =**: Does not equal
- **< =**: Less than or equals
- **=**: Equals
- **> =**: Greater than or equals

#### **port\_number**

Specifies the port number to match.

*port\_number* must be an integer from 1 through 65535.

#### **!range | range**

Specifies the range criteria.

- **!range**: Not in the range
- **range**: In the range

#### **start\_range to end\_range**

Specifies the starting and ending port numbers for the port range.

*start\_range* must be an integer from 1 through 65535.

*end\_range* must be an integer from 1 through 65535 that is greater than *start\_range*.

#### **port-map port\_map**

Specifies name of the port-map for the port range.

*port\_map* must be an alphanumeric string of 1 through 63 characters.

### Usage Guidelines

Use this command to specify an access ruledef to analyze user traffic based on server UDP port.



**Example**

The following command creates an access ruledef for analyzing user traffic matching server port for UDP as 100:

```
udp server-port = 100
```

## udp src-port

This command configures an access ruledef to analyze user traffic based on source UDP port.

**Product**

PSF  
NAT

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

**active-charging service** *service\_name* > **access-ruledef** *access\_ruledef\_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

**Syntax Description**

```
[ no ] udp src-port { operator port_number | { !range | range } { start_range  
to end_range | port-map port_map } }
```

**no**

Removes previously configured source UDP port ruledef.

**operator**

Specifies how to logically match the port number.

*operator* must be one of the following:

- !=: Does not equal
- <=: Less than or equals
- =: Equals
- >=: Greater than or equals

**port\_number**

Specifies the port number to match.

*port\_number* must be an integer from 1 through 65535.

**!range | range**

Specifies the range criteria.

- **!range**: Not in the range
- **range**: In the range

**start\_range to end\_range**

Specifies the starting and ending port numbers for the port range.

*start\_range* must be an integer from 1 through 65535.

*end\_range* must be an integer from 1 through 65535 that is greater than *start\_range*.

**port-map port\_map**

Specifies name of the port-map for the port range.

*port\_map* must be an alphanumeric string of 1 through 63 characters.

---

**Usage Guidelines**

Use this command to specify an access ruledef to analyze user traffic based on source UDP port.

**Example**

The following command creates an access ruledef for analyzing user traffic matching source port for UDP as *10*:

```
udp src-port = 10
```